**University of Plymouth**

**PEARL** **https://pearl.plymouth.ac.uk**

04 University of Plymouth Research Theses 01 Research Theses Main Collection

2021

# A Framework for Understanding and Establishing an Effective Information Security Culture

Tolah, Alaa

http://hdl.handle.net/10026.1/17027

http://dx.doi.org/10.24382/684
University of Plymouth

*All content in PEARL is protected by copyright law. Author manuscripts are made available in accordance with publisher policies. Please cite only the published version using the details provided on the item record or document. In the absence of an open licence (e.g. Creative Commons), permissions for further reuse of content should be sought from the publisher or author.*

Copyright Statement

This copy of the thesis has been supplied on condition that anyone who consults it is understood to recognise that its copyright rests with its author and that no quotation from the thesis and no information derived from it may be published without the author's prior consent.

UNIVERSITY OF PLYMOUTH

# A Framework for Understanding and Establishing an Effective Information Security Culture

By

**Alaa Tolah**

A thesis submitted to the University of Plymouth in partial fulfilment for the degree

**DOCTOR OF PHILOSOPHY**

School of Engineering, Computing and Mathematics

**October 2020**

**Acknowledgments**

I would like to state my initial thanks and praise to God, who has enabled me to have the faith to be able to complete my research. It would have been impossible to fulfil all the requirements of this research without the aid of various individuals, who have assisted in many ways.

Firstly, to my Director of Studies, Professor Steven Furnell, I would like to declare my special appreciation and sincere gratitude for his continual motivation, cooperation, a wealth of help, and support throughout my research, as well as his professional guidance throughout this journey. This research would certainly not have been possible without his help and knowledge. Similarly, I wish to extend my gratitude to my second supervisor, Dr. Maria Papadaki, as she has provided invaluable insight and effort during my research; without these supervisors' team, this study would not have been possible.

It is imperative that my heartfelt thanks go to my family, who have continued to assist and motivate me on this journey. This is particularly relevant in regard to my husband and daughters, who have provided love, patience, encouragement, and perpetual comprehension of my efforts. It is my hope that these accomplishments will help to inspire my daughters in the future to pursue their own ambitions. Special thanks to my parents and siblings that have always provided love and continual support, and there is no doubt that their thoughts and prayers have helped enormously in all my achievements.

It is necessary to thank experts who helped to review the research, as their time and insight were vital to the overall development of the study. This is also true of the research participants and those who helped to distribute the questionnaire across social network sites. Additionally, my gratitude goes to the individuals who work anonymously and assisted in facilitating the research empirical work. Also, Plymouth University has helped to make this research a reality, as have my colleagues and friends at the Centre for Security, Communication and Network Research. Further, it would not have been possible to undertake this research without obtaining my scholarship by Saudi Electronic University, Saudi Arabia.

I will be eternally grateful to you all.

## Author's Declaration

At no time during the registration for the degree of Doctor of Philosophy has the author been registered for any other University award without prior agreement of the Doctoral College Quality Sub-Committee.

Work submitted for this research degree at the University of Plymouth has not formed part of any other degree either at the University of Plymouth or at another establishment.

This study was financed with the aid of a full scholarship from Saudi Electronic University, Saudi Arabia.

Relevant scientific seminars and conferences were regularly attended at which work was often presented and several papers prepared for publication.

Publications

1. Tolah, A., Furnell, S. and Papadaki, M., 2017. A comprehensive framework for cultivating and assessing Information Security Culture. In *HAISA* 2017 (pp. 52-64).
2. Tolah, A., Furnell, S.M. and Papadaki, M., 2019. A Comprehensive Framework for Understanding Security Culture in Organizations. In *IFIP World Conference on Information Security Education* (pp. 143-156). Springer.

Word count of main body of thesis: 90235

Signed: ... .....

Date: ...27/10/2020.....

## Abstract

### A Framework for Understanding and Establishing an Effective Information Security Culture

**Alaa Tolah**

A challenge facing organisations is information security, as security breaches pose a serious threat to sensitive information. Organisations face security risks in relation to their information assets, which also stems from their own employees. Individuals who work in organisations can cause serious risks, even though investments are generally provided to improve security control measures and other devices. Organisations need to focus on employee actions and behaviour to limit security failures, as they aim to establish effective security culture with employees acting as a natural safeguard for information assets. However, the literature review highlights the lack of prior research models that are able to direct organisations with effective security culture, which is why the current research was conducted to provide a comprehensive framework that demonstrates the key factors that affect security culture.

The main objective was to implement a reliable and valid framework capable of focusing on human behaviour and directing organisations in their assessment and improvement of security culture. The current research developed a comprehensive Information Security Culture and key Factors Framework (ISCFF) that correlates between human factors and security culture, which determined how information assets' security is enhanced. The framework provided a level of structured direction to enhance security management and security culture assessment controls. The development of framework is based on Alnatheer's (2012) model and a review of academic literature in a security culture. In the framework, a security culture comprised of various factors in three categories: influential factors, organisational behaviour factors that influence a security culture and reflection factors, which constitute a security culture. First category includes (top management, security policy, security education and training, security risk analysis and assessment, and ethical conduct); second category includes (personality traits and job satisfaction); and third category includes (security awareness, security ownership, and security compliance).

The framework was validated, using a pragmatic approach with mixed-methods that comprised qualitative and quantitative research, with the findings confirmed the significance of the research identified factors in the development of security culture. A semi-structure interview-based investigation was conducted with thirteen experienced security specialists from seven organisations. The findings of interviews concluded that the continuous guidance of employees towards relevant security training sessions and security awareness development to enhance security culture. Additionally, an exploratory survey with 266 valid responses demonstrated the framework levels of validity and reliability through the use of an exploratory factor analysis (EFA), and a confirmatory factor analysis (CFA). Different hypothetical correlations were analysed through the use of structural equation modelling (SEM), with indirect exploratory effect of the moderators achieved through a multi-group analysis (MGA).

This research has shown that the framework has validity and achieved an acceptable fit with the data, to initiate and maintain organisational security culture. This research fills an important gap on the significant relationship between personality traits and security culture. It also contributes to improve the knowledge of information security management through the introduction of a comprehensive information security culture and key factors framework in practice, which functions in the cultivation and maintenance of quality security culture. The framework factors are vital in justifying security culture acceptance. The framework is ultimately able to be used by organisations to construct their security culture through a process of enabling employees, directing their assumption and reducing the levels of insider threat. The framework can be used to improve the possibility to measure an organisational security culture and how to assess it. It helps in the design of employee security training for security awareness-advancement that will enhance the security culture.

## Table of Contents

Acknowledgments ..... ii

Author's Declaration ..... iii

Abstract ..... iv

List of Table ..... xi

List of Figures ..... xiii

Chapter One : Introduction and Overview ..... 1

1.1 Introduction ..... 2

1.2 Research Gap ..... 5

1.3 Research Aims and Objectives ..... 6

1.4 Structure of Thesis ..... 7

Chapter Two : An Overview of Information Security ..... 10

2.1 Introduction ..... 11

2.2 The Information Security Concept ..... 11

2.3 The Human Aspect of Information Security ..... 13

2.3.1 The Human Element and Insider Threat ..... 15

2.3.2 The Challenge of Insider Threats in Information Security ..... 16

2.3.3 The Common Insider Risks to Information Security ..... 17

2.3.4 The Human Element in Information Security International Standards and Guidelines ..... 20

2.4 Conclusion ..... 22

Chapter Three : Information Security Culture ..... 23

3.1 Introduction ..... 24

3.2 Culture within Organisations ..... 24

3.3 Culture of Information Security and the Organisational Culture ..... 25

3.3.1 Schein's Model of Organisational Culture ..... 26

3.4 Introduction to Information Security Culture ..... 28

3.4.1 Information Security Culture Definition ..... 29

3.4.2 An Overview of Existing Information Security Culture Approaches ..... 32

3.5 Discussion and Resulting Research Objectives....43
3.5.1 Summary of Literature Gap....49
3.6 Information Security Culture and The Key Factors....51
3.6.1 Top Management Support....53
3.6.2 Security Policy....54
3.6.3 Security Awareness....56
3.6.4 Security Education and Training....58
3.6.5 Security Ownership....59
3.6.6 Security Risk Analysis and Assessment....60
3.6.7 Security Compliance....61
3.6.8 Ethical conduct....62
3.7 The Interaction between the Key Factors Relating to The Information Security Culture....64
3.8 The Other Influencing Important Security Factors....67
3.9 Conclusion....69
Chapter Four : Research Methodology....72
4.1 Introduction....73
4.2 Methodology....73
4.2.1 Research Philosophy....74
4.2.2 Research Approach....76
4.2.3 Research Strategy and Design....77
4.3 Time Horizon: Cross-sectional....78
4.4 Data Collection Strategies....79
4.4.1 Literature Review....81
4.4.2 Interview Method....81
4.4.3 Survey Method....88
4.5 Data Analysis....96
4.5.1 Interviews Data Analysis....96
4.5.2 Survey Data Analysis Process....98
4.6 Ethical Considerations....99
4.7 Conclusion....100
Chapter Five : A Framework for Information Security Culture....101

5.1 Introduction ....102
5.2 Limitation of Current Studies Considering Information Security Culture Factors ....102
5.3 The Information Security Culture and key Factors Framework (ISCFF) ....103
5.3.1 The Development of the Proposed Framework ....104
5.3.2 The Interaction between Framework Components ....110
5.4 The Information Security Culture and key Factors Framework (ISCFF) Application Example ....111
5.5 Conclusion ....115
Chapter Six : Formulation of the ISCFF: Qualitative Interviews ....117
6.1 Introduction ....118
6.2 Overview ....118
6.3 Development of the Interview Guide ....118
6.4 Pilot Study Interview Guide ....120
6.4.1 Analysis and Results of the Pilot Study ....121
6.5 Interview Sampling ....122
6.6 Interview Process ....125
6.7 Qualitative Data Analysis - Interviews ....128
6.7.1 General Analytic Strategy ....129
6.7.2 Analytic and Coding Techniques ....130
6.8 Interview Findings ....132
6.8.1 Employment Details ....132
6.8.2 Information Security Culture Practices ....133
6.8.3 Employee Security Behaviour Patterns ....136
6.8.4 Perceptions for Improving the Information Security Culture ....145
6.9 Interview Discussion ....147
6.10 Hypothesis Development ....154
6.11 Conclusion ....166
Chapter Seven : Empirical Study Methodology- Survey Design and Development ....168
7.1 Introduction ....169

7.2 Survey Design .....169
7.2.1 The Questionnaire's Content Development and Operational Items .....170
7.2.2 Measurement Scale .....181
7.3 Questionnaire Pre-test .....183
7.3.1 Expert Review .....184
7.3.2 Pilot Study .....186
7.4 Population and Survey Sampling .....190
7.5 Questionnaire Process and Administration .....193
7.6 Conclusion .....195
Chapter Eight : Empirical Study Analysis and Quantitative Results .....196
8.1 Introduction .....197
8.2 Data Analysis .....197
8.2.1 Data Preparation and Screening .....198
8.3 Questionnaire Results .....208
8.3.1 Demographic Data .....208
8.3.2 Information Security Knowledge .....215
8.3.3 The Statistical Analysis of the Research's Framework Dimensions .....225
8.4 The Research Instrument Levels of Reliability and Validity .....229
8.4.1 Reliability of the Instrument .....229
8.4.2 Validity .....231
8.5 Factor Analysis (FA) .....232
8.5.1 Exploratory Factor Analysis (EFA) .....233
8.6 Assessment and Evaluation of the Model .....240
8.6.1 Structure Equation Modelling (SEM) Overview .....240
8.6.2 Measurement Model Assessment .....243
8.6.3 Final Measurement Model .....252
8.6.4 Structure Model Assessment .....254
8.6.5 Multi-group Analysis with Demographic .....264
8.7 Conclusion .....271
Chapter Nine : Discussion and Implications of Quantitative Results .....276

9.1 Introduction ....277
9.2 Reflecting upon The Results ....277
9.3 Influential Constructs/Factors ....280
9.4 Organisational Behaviour Construct/Factors ....286
9.5 The Constituting Constructs/Factors ....290
9.6 Conclusion ....294
Chapter Ten : Conclusions and Future Work ....297
10.1 Introduction ....298
10.2 General Overview of Research ....298
10.3 The Achievements and Contributions from the Research ....300
10.4 Implications ....304
10.4.1 Research Implication ....305
10.4.2 Practical Implications ....306
10.5 Research Limitations ....307
10.6 Future Research and Recommendation ....308
10.7 The Future for Information Security Culture ....310
References ....312
Appendices ....340
Appendix A. Summary Discussion of Fourteen Studies of The Current Perspective Offered by Each Study Reviewed in Chapter 3 ....341
Appendix B. Ethical Approval Letter -Interview ....352
Appendix C. Ethical Approval Letter -Survey ....353
Appendix D. Interview Invitation Flyer ....354
Appendix E. Interview Guide ....355
Appendix F. Interview - Code Book ....358
Appendix G. Interview- List of Category Codes ....360
Appendix H. Interview - Example of Category Codes ....361

Appendix I. Survey Invitation Flyer ..... 371

Appendix J. Survey ..... 372

Appendix K. Multivariate Normal P-P plot of Regression Standardised Residual ..... 384

Appendix L. Items Results Statistical Analysis ..... 391

Appendix M. Total-Item Correlation ..... 394

Appendix N. Items Cross Loading ..... 404

## List of Table

Table 3.1: A Summary of Currently Proposed Constructs Across Different Researches in Information Security Culture ..... 37
Table 3.2: Summary of Top Candidate Factors in the Information Security Culture Research ..... 52
Table 4.1: A Summary of Research Design and Process ..... 80
Table 6.1: The Interview Guide Questions and their Linkage to the Research Objectives ..... 120
Table 6.2: Interview Question (C-2) ..... 121
Table 6.3: Demographic Profile of Organisation ..... 125
Table 6.4: A Summary of the Interview Process ..... 126
Table 6.5: Interviews Details ..... 127
Table 6.6: Example of Data Categorisation ..... 131
Table 6.7: The Main Information Security Practices and Rules Used in Participating Organisations 133
Table 6.8: The Participants' Perceptions of Having an Effective Security culture ..... 138
Table 6.9: Respondents Recommendation for Improving the Information Security Culture ..... 145
Table 6.10: Five-Factors Traits as Described by John and Srivastava (1999) ..... 158
Table 6.11: Research Hypothesis to be Testing in a Subsequent Survey Phase ..... 164
Table 7.1: Knowledge Questions ..... 172
Table 7.2: Information Security Culture Questionnaire Operationalisation Statements ..... 175
Table 7.3: Survey-Demographic Section (Question 11) ..... 185
Table 7.4: Survey-Knowledge Section (Statement 3) ..... 185
Table 7.5: Survey-Knowledge Section (Statement 17) ..... 186
Table 7.6: Survey-Information Security Culture Practice and Behaviour Section (Statement 3.3) ..... 186
Table 7.7: The Shape of Data Distribution Based on Skewness and Kurtosis Values and Reliability ..... 189
Table 7.8: Survey-Knowledge Section (Question 14) ..... 190
Table 8.1: Data Distribution Shape Based on Skewness and Kurtosis Values ..... 200
Table 8.2: Data Outlier Screening ..... 204
Table 8.3: Collinearity Assessment ..... 207
Table 8.4: Correlations Among Components of Information Security Culture with Key Factors ..... 208
Table 8.5: The Industries of Organisations ..... 210
Table 8.6: Information Security Knowledge Statements ..... 216
Table 8.7: Analysis of the Correlation between Knowledge and Demographical Information ..... 221
Table 8.8: T-test Statistics Demonstrating Organisational Type Differences Regarding Knowledge 223
Table 8.9: T-test Statistics Showing Countries Differences in Knowledge ..... 223

Table 8.10: ANOVA Statistics Demonstrating Years of Experiences and Differences in Knowledge Levels....224
Table 8.11: T-test Statistics that Show Induction Training Differences in Knowledge....224
Table 8.12: T-test Statistics that Show Induction Training Differences in Levels of Knowledge....225
Table 8.13: Research Framework Constructs Results Statistical Analysis Summary....226
Table 8.14: Cronbach's Alpha Attribute Value and the Result of Analysis....230
Table 8.15: KMO and Bartlett's Test of Sphericity....234
Table 8.16: Factor Loading (Pattern Matrix)....238
Table 8.17: Measurement Model Fitting Criterions....244
Table 8.18: Convergent Validity and Reliability for the Constructs....246
Table 8.19: Discriminant Validity-Fornell Larcker Criterion....249
Table 8.20: Factors/Outer-Loading with Cross-Loading....250
Table 8.21: Model Fit Indices....252
Table 8.22: Structure Model Assessment Criteria....255
Table 8.23: Hypothesised Paths' Coefficients, Observed T-Statistics, Significant Level P-value....257
Table 8.24: Results of the Research Hypotheses....259
Table 8.25: Correlations Among Components of Security Culture with the Key Factors....261
Table 8.26: The Constructs' Coefficient Determinations....262
Table 8.27: Differences of Organisation Type in PLS-MGA and Path Coefficients....268
Table 8.28: Differences of Gender in PLS-MGA and Path Coefficients....269
Table 8.29: Differences of Country in PLS-MGA and Path Coefficients....270
Table 8.30: Difference of Background Education in IT in PLS-MGA and Path Coefficients....271
Table 9.1: Results of the Research Hypotheses....280

## List of Figures

Figure 3.1: Schein's Three Level Model....27
Figure 4.1: Generic Research Onion Process (Saunders et al. 2003)....74
Figure 4.2: Three Phases of Data Collection Process....80
Figure 5.1: The Information Security Culture and Key Factors Framework (ISCFF)....106
Figure 6.1: Interview Data Analysis Process....130
Figure 6.2: Years of Work Experience for Participants....133
Figure 6.3: Information Security Level in Organisations....136
Figure 6.4: Employee's General Security Behaviour....137
Figure 6.5: The Most Effective Information Security Practices on Employee Security Behaviour....137
Figure 6.6: The Main Contributory Factors for Establishing an Effective Information Security Culture ....140
Figure 6.7: The Main Obstacles to Achieving Improved Security Compliance....143
Figure 7.1: Example of Statements Related to the Major Five Dimensions in the Questionnaire....181
Figure 7.2: Measurement Scale Example....182
Figure 7.3: Measurement Scale (Yes/No) Example....183
Figure 7.4: Measurement Scale (Multiple choice) Example....183
Figure 8.1: An Example of Multivariate Normal P-P plot of Regression Standardised Residual for Top Management....202
Figure 8.2: Organisational Types....209
Figure 8.3: Number of Employees in Organisations....211
Figure 8.4: Participants' Genders....212
Figure 8.5: Participants' Ages....212
Figure 8.6: Different Nations....213
Figure 8.7: Length of Employment in the Organisation....214
Figure 8.8: Respondents' Employment Level....215
Figure 8.9: Reports in Organisations of Information Security Incidents....219
Figure 8.10: Training Session Type Provided in Organisations....219
Figure 8.11: Preference of How to Receive Information Regarding Security Awareness and Training Messages....220
Figure 8.12: Scree Plot....236
Figure 8.13:Measurement Model for Information Security Culture....254
Figure 8.14: Evaluation of the Information Security Culture Structure Model....257

## List of Abbreviations

| | |
|---|---|
| ACM | Association for Computing Machinery |
| AGFI | Adjusted-Goodness-of-Fit-Index |
| AMOS | Analysis of Moment Structure |
| ANOVA | Analysis of Variances |
| AVE | Average Variance Extracted |
| CBSEM | Covariance-Based SEM |
| CERT | Computer Emergency Response Team |
| CFA | Confirmatory Factor Analysis |
| CFI | Comparative-Fit Index |
| C.I.A. | Confidentiality, Integrity, Availability |
| CISF | Comprehensive Information Security Framework |
| CMB | Common Method Bias |
| COBIT | Control Objectives for Information and Related Technology |
| CORAS | Conducting Security Risk Analysis |
| CPNI | Centre for the Protection of National Infrastructure |
| CR | Composite Reliability |
| CRAMM | Central Computer and Telecommunication Agency Risk Analysis and Management Method |
| CSV | Comma Separated Values |
| EFA | Exploratory Factor Analysis |

| | |
|---|---|
| EBSCO | Elton Bryson Stephens Company |
| ENISA | European Network and Information Security Agency |
| EQS | Equations |
| FBI | Federal Bureau of Investigation |
| FFM | Five Factor Model |
| GFI | Goodness-of-Fit Index |
| GLS | Generalised Least Squares |
| HAISA | Human Aspects of Information Security and Assurance |
| IBM | International Business Machines |
| ICT | Information and Communication Technology |
| IEEE | Institute of Electrical and Electronic Engineers |
| IFIP | International Federation for Information Processing |
| IP | Internet Protocol |
| IS | Information Systems |
| IEC | International Electrotechnical Committee |
| ISC | Information Security Culture |
| ISCF | Information Security Culture Framework |
| ISCFF | Information Security Culture and key Factors Framework |
| ISF | Information Security Forum |
| ISM | Information Security Management |

| | |
|---|---|
| ISO | International Organisation for Standardization |
| ISMS | Information Security Management System |
| ISSA | Information Systems Security Association |
| IT | Information Technology |
| ITIL | Information Technology Infrastructure Library |
| KMO | Kaiser-Meyer-Olkin measure of sampling adequacy |
| LISREL | Linear Structural Relations |
| LV | Latent Variables |
| MANOVA | Multivariate Analysis of Variance |
| MGA | Multiple Group Analysis |
| ML | Maximum Likelihood |
| NATO | North Atlantic Treaty Organisation |
| NFI | Normed-Fit Index |
| OCTAVE | Operationally Critical Threat, Asset, and Vulnerability Evaluation |
| OLS | Ordinary Least Squares |
| PAF | Principal Axis Factors |
| PCA | Principal Component Analysis |
| PLS | Partial Least Squares |
| PwC | Price waterhouse Coopers |
| RMR | Root Mean Square Residual |

| | |
|---|---|
| RMSEA | Root Mean Square Error of Approximation |
| ROI | Return on Investment |
| RSA | Rivest, Shamir, and Adleman company |
| SANS | System Administration, Networking, and Security Institute |
| SD | Standard Deviation |
| SE | Standard Error |
| SEM | Structural Equation Modelling |
| SMEs | Small and Medium Enterprise |
| SMS | Short Message Service |
| SPSS | Statistical Package for the Social Sciences |
| SRMR | Standardised Root Mean Square Residual |
| SSW | Secure South West |
| STOPE | Strategy, Technology, Organisation, People and Environment |
| ULS | Unweighted Least Squares |
| USB | Universal Serial Bus |
| VIF | Variance Inflation Factors |
| WINS | World Institute for Nuclear Security |
| WLS | Weighted Least Squares |

# Chapter One :

# Introduction and Overview

## 1.1 Introduction

Currently, the knowledge-based economy has become more dynamic than any time in the past and is still progressing. Indeed, technology enables all business operations and information technology (IT) to develop into a central concept for the majority of aspects of life whilst geographical boundaries are reducing. Consequently, there has been a change in the conduct of commerce, the structure of government, the delivery of public services, as well as the provision of education and health care. In this changing international environment, it is important that the relationship between the business environment and technology is fully understood. This relationship is incorporated into everyday organisational tasks, provides data, which is transformed into decipherable information which can be stored, transferred or used to inform strategic decision-making.

However, the inflated use of software and different technologies have increased potential for breaches in security (Reid & van Niekerk 2014). The technological environment and advanced business possibilities have created challenges and security risks to data and information used by a wide range of businesses, governments, and organisations. Breaches of security are exacerbated by various common technological traits and behaviours. For example, wireless access in public areas, failure to disconnect from the Internet, and leaving access to private data open. As a result, organisations must recognise and adapt to the challenges and risks of security breaches. Organisational information security requires continuous assessment and improvement if a competitive edge is to be maintained. Reliable information is a vital asset to all organisations (Van Niekerk & Von Solms 2009). It is crucial that this information is protected in order to create not only a competitive and stable business, but also reflects on the stability of national economies.

Many organisations are affected by breaches in data. These attacks are highly detrimental and can cost billions of pounds in data cleanup, loss of data and customer confidence (Ponemon 2015). Breaches of information security can cost a single organisation approximately £1m annually (Ponemon 2019). Furthermore, data breaches can only be managed correctly by 32% of organisations. Consequently, current information security programs need to be advanced and understood more widely and at a deeper level. Future technology needs to be designed to combat existing and potential concerns to security (IBM 2016).

Over the past few years, various technical approaches have been developed in relation to security, control and potential countermeasures. Additionally, organisations have introduced safeguards that have been practised, understood and developed. Information security has evolved into fundamental component of security systems in the majority of organisations. Yet, simultaneously there has been an acceleration of breaches, due to the sophistication of malware, which unfortunately creates added pressures to the professionals working within IT (Trustwave 2014). A greater level of vulnerable components in information systems exists due to the individuals who use information technology. Staff members can activate viruses and have access to personal data theft, which includes attacks through social engineering (ENISA 2010; Cybersecurity Insiders 2019). A delay in detection of such breached may be due to the fact that users often remain unaware of security risks, and their connection to them. Users may only become aware of breaches a long time after the incident. The possibility of accumulated costs to an organisation due to this delay in detection is often increased (Ernst & Young 2015).

It is believed therefore, that security is not only a 'technical issue' but also a 'people issue' (Alhogail 2016; Connolly et al. 2017; Furnell & Clarke 2012). There are different type of threats that have recorded to security of information from all different sectors but the actions of employees when managing information are one of the major threats to the secure information environment within an organisation (Cybersecurity Insiders 2019; Renaud & Goucher 2014; Parsons et al. 2017). It has been concluded that users inside an organisation often create the most prominent threat to information protection, even if it is unintentional (Da Veiga & Eloff 2010; Furnell & Thomson 2009; Verizon 2017). Unfortunately, the users who interact with the information and data on a daily basis directly affect the efficiency of countermeasures for information security. The human 'person' component has been deemed to be vital in the formation and challenges to information security (Karyda 2017; McCormac et al. 2018). Therefore, making employees aware of information security is imperative. Information security can only be effective when employees are knowledgeable, aware and able to take the relevant precautions when using information technology (McCormac et al. 2018). Information security needs to function together with technical aspects to achieve an environment that is successfully secure. In addition, employees need to take responsibility for individual actions when working with sensitive information.

Human interaction with information security must be considered when processing the life cycle of information security management, although this has not been the focus of much research in this field (Furnell & Clarke 2012; Metalidou et al. 2014). The majority of investigations state that employees are potentially one of the most significant contributors to breaches in security (Ponemon 2019; Verizon 2017). The United States of America Federal Bureau of Investigation (FBI) stated that more risks are posed by insiders within organisations in comparison to hackers or other security risks. This was based on case investigations from the previous 20 years. As early as 2015, the indication was that technology was less likely to cause problems than human error. Human error was identified as the cause of the majority of breaches in security (Verizon 2017). As 75% of large organisations and 31% of SMEs organisations were revealed to suffer security breaches by insider employees (PwC 2015). It was confirmed that the human element remains a concern to the information security of organisations (PwC 2018; Ponemon 2019). The Data Breach Investigations Report of Verizon (2017) revealed that at least 15% of security breaches come from insider employees and 14% of security breaches caused from error made by insider employees that was unintentional.

It is imperative that employees comprehend information security practices and develop a cultural and social understanding of the information activities committed by their employees (Da Veiga & Martins 2015; Karyda 2017). One particular approach that an organisation could take to manage the changing security landscape would be to develop strategies for security that enhance security cultures of information (Karyda 2017; Martins & Martins 2016). As a result, organisations would place more emphasis on creating more IT cultural awareness (Wiley et al. 2020). Also, the creation of an information security culture would demonstrate an organisation's commitment to the employees. Increased user commitment to information security requires increasing trust between an organisation and its employees together with positive changes in behaviour patterns both personally and professionally (Martins & Eloff 2002; Parsons et al. 2014).

A sufficient information security culture is necessary within an organisation to cope with a range of behavioural issues that might contradict security requirements (Alnatheer et al. 2012). The development of an information security culture would allow employees to become more aware of risks and personal security responsibilities (Alhogail 2016; Da Veiga & Eloff 2010; Parsons et al. 2015). A raised level of awareness should reduce potential risks of harmful

information interaction by employees. Employees need support to develop knowledge, understanding and comprehension of risk, and to advance their own skill levels correctly (Da Veiga & Martins 2015; Emma W 2017; Van Niekerk & Von Solms 2010). In addition, the development of the information security culture, must include all employees and not remain exclusive to IT team. The enforcement of security policy is more effective and beneficial when all individuals are aware and knowledgeable (Alhogail 2016; Alnatheer et al. 2012).

## 1.2 Research Gap

It is evident from studies Bell et al. (2019) and Mehan (2016), that employees within organisations can create security risks in relation to their knowledge of information, which can be either intentional or unintentional. The development of an effective information security culture within an organisation helps to minimise risks created by employees. It can safeguard levels of confidentiality, integrity and reduce information assets' availability. The information security culture is still an emerging area of research (Karlsson et al. 2014; Karyda 2017). Organisational culture alongside human behaviour in information security has been analysed by researchers such as Dojkovski et al. (2007) and Van Niekerk and Von Solms (2010). Nevertheless, there is minimal available evidence with regard to how the knowledge of security risks and personal responsibilities is applied and integrated into security development. Researchers are forced to utilise a variety of models and approaches that attempt to offer a complete practice and comprehension (Karlsson et al. 2014; Nasir et al. 2019; Mahfuth et al. 2017; Pevchikh 2015; Sas et al. 2020).

Accordingly, previous analysis has determined that the understanding of the information security culture and its measurements are still lacking. In particular, further research needs to provide a comprehensive view that guides and integrates all important factors that shape or have an impact on the information security culture (Karlsson et al. 2014; Nasir et al. 2019; Sas et al. 2020). There is a gap in knowledge regarding the development of a theoretical framework of constructs that influence the effectiveness of the information security culture in organisations. Consequently, it is imperative that a more reliable and valid theoretical model framework, which would improve levels of security compliance, is needed. This model needs to be part of the overall security culture of the organisation.

However, organisations are not homogenous, situational contexts differ (Cazemier et al. 2010). This research attempts to provide an information security framework that can be tailored to specific security needs. It will propose a reference framework (whilst offering more than one solution) to be used as a process for problem-solving in regard to information security. The focus is on creating structures that influence and measure the information security culture, which minimise risks caused by human behaviour.

## 1.3 Research Aims and Objectives

This research aims to design and develop a comprehensive Information Security Culture and key Factors framework (ISCFF), which is reliable and valid in order to cultivate and measure the level of the information security culture in an organisation. This will assist researchers and practitioners to understand the complexity and challenges of the information security culture inside organisations. Since there is a still lack of consideration of factors and issues in the current adoption studies and frameworks, are explained in Chapters 3 and 5. The framework will be developed by considering existing research and by determining which further problems exist in the security management of organisations. The main objectives that will be achieved in this research are the following:

1. To explore and evaluate the conceptualisation of information security culture and the importance of implementation in an organisation.

2. To present a summary of previous studies aimed at establishing and managing information security culture and various factors that could influence the effectiveness of information security culture and the behaviour of employees.

3. To identify the critical success factors that have a direct influence or constitute information security culture components.

4. To understand the relevance of these identified factors and their relationship with each other in order to inform the design of an information security culture framework.

5. To identify any other security factors that could have a direct influence on the information security culture.

6. To develop a comprehensive framework that integrates all important factors that can be used for the implementation of an effective information security culture.

7. To assess the validity of the proposed Information Security Culture and key Factors framework (ISCFF) through a structural equation modelling (SEM) technique by gathering data from real-world situations.

## 1.4 Structure of Thesis

The thesis consists of ten chapters and following on from this introduction,

Chapter 1 introduces the research problem, provides a background to the overall context of the current research, outlines the core research gap and problems, and describes the research objectives and process.

Chapter 2 provides a brief background of information security and a discussion of why human elements represent a challenge to the security of information assets in organisations with a specific focus on insider threats. The next section presents the types of insider threats and risks that might pose to the organisational information assets. The final part discusses some widely used international standards and guidelines that support the information security management and the protection of organisational information assets.

Chapter 3 presents a review of the literature that focus in the area of relevance to the research problem. It explores the literature in order to formulate an understanding of information security culture and discusses current information security culture issues and research perspectives. It outlines the current available information security culture definitions that serve as a reference for understanding. It also presents various frameworks and models that explore different factors that have an effect on the information security culture field. The next section highlights the gaps in the literature and further research required in the information security culture field. The final section presents the main critical success factors that strongly assist the cultivation of information security culture within an organisation. It provides an evidence for each factor presented in previous studies and research in the information security culture field. This evidence will provide the basis of a comprehensive framework, which is the main aim of the current research.

Chapter 4 provides the methodological pragmatic philosophical approach with mixed methods of data collection, and data analytical techniques applied to examine the research framework established in Chapter 5. There is a description of the research strategy and design; with the application of a mixed-methods' approach, that are explained in order to justify the research method selection. The chapter then describes the qualitative phase, including data collection procedures, sampling, pilot study and data analysis techniques. It also illustrates the quantitative phase, including data collection method, survey sampling, questionnaire development, sampling, pre-testing, analysis technique and data validation. The last section of this chapter is the ethical considerations.

Chapter 5 presents the initial comprehensive framework developed based on the integration of the contribution made in Chapters 2 and 3 in order to achieve the research objectives. First the limitation of previous studies that identified the information security culture factors and issues is noted with the need for a new framework. The second section presents and discusses the proposed new framework and its main components that should influence the information security culture in an organisation.

Chapter 6 provides the findings and analysis of the qualitative data. It begins with an overview of the interview objectives. Second, it presents the interview guide design and development, pilot study results and interview procedure. Third, it outlines the data analysis and technique used to form a view of the information security culture and influencing factors. Fourth, it provides the main findings of the qualitative interviews, which include specific factors constituting information security culture; and factors that influence the information security culture. Final section presents the development of research hypothesis associated with relationships between the framework constructs that will be examined in Chapter 8.

Chapter 7 presents the survey design and development for this research. It provides a description of the questionnaire design and measurement scale. The following section describes the survey sample and population. The next section provides the result of questionnaire pre-test results including the expert panel feedback and the findings from the pilot study. The final section provides the administration of the questionnaires.

Chapter 8 presents the analysis of quantitative exploratory survey. It presents detailed results of the data analysis and tools used in the current research. In this section, it discusses the

screening of the data; and output including missing data treatment, normality, and common method bias. It continues by providing the results of the descriptive findings of the respondents' characteristics. Then, it discusses the results of information security knowledge questions, descriptive statistics for the variables of factors influencing information security culture and factors reflecting information security culture in the theoretical framework. It presents the inferential analysis with partial least squares (PLS) including the reliability of the internal consistency and item-total correlations and validity of the instrument. The exploratory factor analysis (EFA) is presented to determine the structures that demonstrate the framework's constructs. This is followed by a section that presents the two-step process to analysis; the proposed framework, including the measurement model using confirmatory factor analysis, (CFA) in order to improve the structure of the constructs; and the structural equation model (SEM), in order to test the relation between research model constructs and the research hypotheses. The chapter concludes with an overview of the multiple group analysis (MGA) and the findings from testing the research framework.

Chapter 9 presents the detailed discussion about the main survey findings obtained in Chapter 8. The following section provides a discussion of the findings from testing the research hypotheses and findings that complemented with the previous literature to rationalise the objectives proposed in the current research.

Chapter 10 provides a summary of the thesis results and main findings in terms of contributions and limitations. Specifically, it describes the most notable conclusions and the research objectives that have been accomplished. Finally, it provides some recommendations for future research.

# Chapter Two：An Overview of Information Security

## 2.1 Introduction

The purpose of this chapter is to provide an understanding of how human elements impact on information security with a specific focus on insider threat. It begins by providing a brief background and an overview of information security in general. Next, it provides a discussion of why the human factors effect represents a challenge to information security, and how individuals interact with it. Then, it presents the risks that insiders might pose to the information assets of organisations which result in security breaches. Finally, some widely used standards and guideline that support the information security management and protect the information assets of organisations are presented.

## 2.2 The Information Security Concept

The application of technology enables business operations in the global economy in the modern era. Through all remits and stages of business operations, deals are made, goods and services are provided, clients' accounts are tracked, and strategic/financial decisions are made. These transactions are undertaken through systems of information technology. This allows information in the capacity of storage and transportation to be made between businesses. Systems of information technology are generally perceived as the most valuable resource of a company, alongside protecting its individual needs.

Advancements in technology have increased the scope of computing systems, as well as the overall environments. It is believed that IT personnel are able to handle technological problems with the systems. This concept may have been correct during the initial stages of computing when mainframe computers were using a single processor, and no databases were shared as only a single program was executed at one time (Thomson & Von Solms 1998). Consequently, the set environment was easier to define and control. Nowadays, the concept of computer security has developed into the concept of information security, as businesses have gained more fluidity. Security of information is a central issue in the majority of organisations, as the advancements in distributed processing have enabled better information access, and thus, organisations want to assure the protection of their information (Von Solms et al. 1998). The requirement of information security is vital, due to the risks created by applied technology in information acquisition (Blakley et al. 2001). The securitisation of information related to the implementation of sufficient controls need to be aligned with the clarified objectives of the

organisation, in order to reduce the potential risks exposed (ISO/IEC 27002 2005). This increases trust in the business transactions of the organisation. It also ensures IT services can adequately resist, and recover from error induced failures, provoked attacks and to ensure the protection of confidential information (COBIT 2004).

Security in IT, which has been defined by various sources as the form of protection against unauthorised access, as well as disruption, modification or disclosure (ISO/IEC 27002 2005; Killmeyer 2006), has also gained importance in relation to academic communities and practitioners. This is in direct reference to confidentiality protection and the maintenance of computerised data integrity, which helps to continuously report the data and occurs during the output stages of processing, storage and dissemination (Kaur & Mustafa 2013; Kruger 2006); referred to as the CIA triad. Likewise, security information's basic components are defined as follows:

1. Confidentiality: when data is disclosed purely to authorised individuals, it is confidential. Similarly, unauthorised employees are unable for example to check payroll data. Security aims to deter potential attackers from accessing customer databases in order to protect personal details and secure information such as credit card details (Goh 2003).

2. Integrity: when data is accurate and complete then it has measured integrity. Integrity can be lost when an unauthorised entity has modified or destroyed the data. For instance, this may occur following the modification of a file due to a malware infection or transmitted e-mails being altered (Goh 2003).

3. Availability: when information is ensured, and important services become accessible then availability becomes apparent for those individuals who are authorised. When the data or a system becomes unavailable when required then the availability is lost. For instance, when a customer aims to purchase a product and the online shop is not operational then availability is lost (Goh 2003).

The industry standard for computer security has been structured by the themes of C.I.A. since the original mainframe development. From this, organisations are able to use these security standards of information in order to display security mechanisms that create protection for

information (Von Solms 1999). In order for organisations to manage and respond to the elevated levels of threat, information security measures have been deployed with three important components (Korovessis 2015). Firstly, the physical, incorporates various security related activities, such as specific buildings, cameras and guards. Secondly, the technical incorporates electronic devices that are used to protect system monitors, firewalls and access control systems. Thirdly, the administrative incorporates different policies and procedures, as well as guidelines that help to define the used technology in a secure manner of operation (Korovessis 2015).

The Internet has spread exponentially in relation to the number of users and computing devices. For example, there has been the advancement of the cloud in securing information for the business environment, which has helped to improve levels of cyber security. Physical and technical security controls have been developed, whilst innovative security tools are continuously created and advanced. Nevertheless, due to the increased dependency upon the electronic information, security threats are of more concern than in the past. It is necessary to combat these threats in order to achieve a sufficient security level. However, the 'human factor' in the field of information security does not have the emphasis that it deserves. At present, technology is designed to function without considering the human factor, which leaves security systems at risk, even though it is managed and used by them (Mahfuth et al. 2019; Schultz 2005).

## 2.3 The Human Aspect of Information Security

Business environments depend on, and benefit from information systems, whether this is mobile computing, using the cloud or the Internet. These practices have led to parallel changes in security threats and attacks (Mahfuth et al. 2019; PwC 2018; Symantec Corporation 2014). Every organisation needs to protect its information assets against hostile acts and prevent information from falling into the wrong hands. The organisational information assets, therefore, need to be protected, particularly since they contain sensitive data which needs to remain secure (Okere et al. 2012).

There are a series of shared security risks and threats to information assets. However, most organisations tend to concentrate on managing technology and processes and ignore people (Connolly & Lang 2013; Mahfuth et al. 2019). Norman and Yasin (2010), concluded that

traditional technical alterations and revisions are inadequate solutions to the security risks facing today's business community. Several studies have pointed out that technology is totally dependent on the people who operate it, use, administer and store information (Eloff & Eloff 2005; Mahfuth 2019; Joshi et al. 2019). Also, Moag et al (2011) illustrated that despite organisations spending millions on technology, approximately 70% of the security breaches came from individuals, rather than the technology itself. Consequently, information security is not solely a matter of taking a series of technical steps and introducing controls; the human factor is crucial (Connolly et al. 2017; Karlsson et al. 2015; Mahfuth et al. 2019). In 2015, IBM's Security Services produced a Cyber Security Intelligence Index Report revealed that 95 % of security issues stemmed from human factors. Given the fact that people play a main role in the information security process (Van Niekerk & Von Solms 2010), this is of major concern, for security controls cannot exclude human involvement. Additionally, many researchers such as Alhogail (2016), Martins and Eloff (2002), Schlienger and Teufel (2003) and Da Veiga et al (2007) concluded that the majority of security breaches are caused by people, not technological faults.

Therefore, the human factor can be considered as one of the most significant vulnerability; but it is often left unaddressed (Alfawaz et al. 2011; Walton 2015). The organisation often attempts to solve breaches by spending budgets on updating technology and revising processes and do not address the problem of the human factor (Bulgurcu et al. 2010; Mahfuth et al. 2019). Organisations will not be able to preserve the confidentiality, integrity and availability of information assets if they do not understand and resolve the issues surrounding human factors.

Additionally, Colwell (2009) indicated the reasons behind not focusing on human factor in the organisation. First, organisations do not understand the risks posed by insider. Second, fear negative publicity. If such an incident takes place, it is normally denied or hidden. There is evidence that the human factor is a cause of security breaches, but people could be part of the solution. It must be acknowledged that people are not just problems – they could repair, report and learn from every security incident (Bell et al. 2019; Walton 2015). Every organisation includes a range of people from different backgrounds. It is important to examine their differences and their behaviours (Lacey 2009; McCormac et al. 2016). The human factor is a significant factor in both the problem and the solution.

### 2.3.1 The Human Element and Insider Threat

Human security threats in information security could be classified into internal and external threats (Goh 2003; Warkentin & Wilson 2009). External threats include viruses, hacker attack, technological failures and acts of nature, spam or fraud attacks (Loch et al. 1992). The external threats have, for a long time attracted media interest and coverage which prompts organisations into quickly responding and efficiently to a perceived and actual threat. In contrast, the internal threats could be accidental actions which breach security caused by an employee. The reason for these accidents may be due to lack of employees' security knowledge and awareness (Bell et al. 2019; Mehan 2016). It could also be non-compliance with procedures and ignoring of policies (Mehan 2016; Warkentin & Wilson 2009). One approach that organisations could take is focusing on human factor and establishing an effective information security culture.

According to the survey findings of McCue (2008), it appears that insiders are responsible for 70% of all frauds rather than external attacks, yet 90% of security measures are still focused on external threats. Similarly, in 2014 a survey of the Global State of Information Security concluded that the vast majority of security incidents were caused by insiders or former insiders as 31 % of current employee and 27% of a former employee. Also, a security breach survey by Price Waterhouse Coopers showed that 44% of data security breaches were caused by insiders (PwC 2018). These figures suggest that insider threats are more significant than external threats (CERT 2014; Schulze 2018). Therefore, this research focuses on insider threats in general, as well as how the behaviour of employees could pose a threat, whether mild or severe, to information assets.

Insider threat could be defined as an intentional act or behaviour, which is disruptive, unethical or illegal, that is carried out by someone who has internal access to the information assets of an organisation (Mehan 2016). Insider threats could also include unintentionally disruptive acts from these individuals (Mehan 2016; Warkentin et al. 2012). The insider data breach survey Egress (2020) demonstrated that 75% of employees have put the organisation’ data at risk intentionally, and 78% of employees put organisation’ data at risk unintentionally. The human factor includes everyone who has access to information from top level managers to clerical staff whether the past or present employees and irrespective of rank.

Various researchers, such as Mehan (2016), Schultz (2005), and Joshi et al. (2019) have all conducted research studies on human factors and insider threats. Studies of Bell et al. (2019) and Hu et al. (2012) concluded that employees are a significant threat to information assets and security. Similarly, according to the work of Hu et al (2012) and Stanton et al (2005), found that the human insider threat poses a huge problem for information technology security in organisations and one of the hardest to protect against. Failing to deal with this issue could end up costing organisations many lost employee's hours, negative publicity and substantial financial losses.

The most significant incident of 2013 was the security breach of Edward Snowden. Snowden was a government contractor who breached security systems and leaked classified information of the National Security Agency's surveillance programs via WikiLeaks. Snowden accessed files by using other employee accounts. He removed hundreds of thousands of politically sensitive files, which were then put in the public domain through WikiLeaks. This was the most significant leak in a history of the United States of America and attracted a great deal of interest in academic circles (Westervelt 2013). Consequently, organisations and security experts started to pay more attention to the dangers posed by insider threats and how to prevent them.

In 2015, Price Waterhouse Coopers released the results of a security breach survey, which found that 28% of large organisations asserted that the security breaches were caused by employees; 57% of small organisations had experienced insider-related security breaches; and 36% of the worst security breaches resulted from unintentional human error. This highlighted the importance to adopt security solutions that address the human factors in organisations.

### 2.3.2 The Challenge of Insider Threats in Information Security

The human challenge lies in accepting that individuals have to be viewed as whole beings, that is, people with personal attitudes, beliefs and social traits, rather than as merely the personification of their job role (Alhogail et al. 2015; Da Veiga & Eloff 2010). The challenge that faces organisations is how to manage this and maintain a good balance between managing individuals and meeting business aims by using resources in the most efficient way (Schlienger & Teufel 2003; Ashenden 2009).

Researchers such as Ashenden (2009), Da Veiga and Eloff (2010) and Alhogail (2016) have agreed that, to have a successful information security management, it has to include and understand the social features (human element) of the organisation. Since human beliefs and emotions change constantly, they are difficult to manage optimally in the context of information security. So, it will be difficult to manage or predict behaviour with any degree of accuracy. Another challenge of insider threat was highlighted by Dhillon and Backhouse (2000), who point out that a lack of skills and knowledge could impact negatively when it comes to employee behaviour. For instance, while individuals might know how to protect the contents of a physical filing cabinet, this does not mean that they recognise the importance of protecting the information assets of organisation (Bell et al. 2019; Mahfuth 2019). Lack of awareness is one of a major challenge that confront the security of organisation's information because the employees might not see this as a vital task (Bell et al. 2019; Thomson et al. 2006).

Moreover, Dhillon and Backhouse (2000) argued that the expansion of information technology (IT) in organisations has led to employees developing what they call security blindness when using information technology on a daily basis. The prevailing attitude appears to be that protecting the security of the information is a task entrusted to the IT department only and has nothing to do with anyone else (Dhillon & Backhouse 2000; Egress 2020). According to Egress (2020), employees get confused about data ownership and their security responsibility in organisations. Thomson et al. (2006) acknowledge that individual attitudes and core values could be changed by giving the right training. The behaviour of employees could be positive with a raised level of awareness and the correct training. Employees could form a strong bulwark for the organisation and prevent breaches of its security infrastructure (Bell et al. 2019; Thomson et al. 2006).

### 2.3.3 The Common Insider Risks to Information Security

One of the common insider threats to information security in an organisation is the employees' erroneous behaviour (Thomson et al. 2006). The ignorant or careless behaviour on the part of employees poses a serious and widespread threat to organisations' information assets and overall security (Kaspersky 2018; PwC 2018). The study of Dojkovski et al. (2007) listed a number of actions which could unintentionally create security risks. These include opening spam emails, opening an email attachment which contains a virus, or ignoring the security rules and policy on the use of external devices. The negligence of an employee could put the entire

organisation network at risk by allowing viruses, malware, and Trojans to spread across the system and expose the whole organisation's communication structure inserted to infection (Egress 2020; Mahfuth 2019). In addition, employees who do not consider security rules and measures when using personal mobile device, personal USBs and hard drives could also expose the organisational network to infection and malfunction –as well as security threats.

The State of Cybercrime Survey - CERT (2014), revealed that 34% of insider cyber incidents revolved around the unintentional leaking of private or sensitive data, and this shows how employees' negligence could cause a problem of security breaches. Also, the security breaches survey by Price Waterhouse Coopers in 2015 showed that 36% of the worst breaches were caused by unintentional human mistake (PwC 2015). Most employees frequently carry mobile devices outside their organisation, which contain sensitive data, and if the mobile device is stolen or lost, this work-related information could be lost or fall into the wrong hands (Egress 2020; Kaspersky 2018). Similarly, if either family or friends are permitted to use organisation networks or computers, this opens the door to outsiders having access to organisational information of a sensitive nature they should not be able to see (Goh 2003). Also, 30% of surveyed insider cyber incidents comprised unauthorised individuals' access to and use of networks, equipment or information that should have stayed within the organisation (CERT 2014).

21% of surveyed employees admitted that they allowed outsiders such as family or friends to use their work laptops to go on the Internet or look at the corporate network (Information Systems Security Association 2013). In addition, Renaud and Goucher (2014) study underscored a further issue. They noted that personal records are frequently not disposed of in a proper way and documents are occasionally sent to the wrong person that could be noted as a cause of many security breaches.

In general, employees have limited knowledge about security (Mahfuth 2019; Bell et al. 2019). In 2013, a survey was conducted by information Security Breaches Survey; found that 62% of employees stated that they had very limited knowledge of information security. In addition, 8% of employees believed that the accidental data breaches happen due to the inadequate security system have in their organisation and 5% of employees report insufficient security training in organisations (Egress 2020).

The majority of information security breaches is related to the fact that employees' failures to comply with the information security guidelines and policies (Da Veiga 2015; Parsons et al. 2010). For instance, employees could plug personal devices such as USBs into the organisation network. This type of action facilitates for copying large amounts of sensitive data, information and programs from the network and all sensitive information which should not leave the workplace, thereby risking information assets (Goh 2003).

Some employees may also use the organisation network for their personal activities, such as playing games, downloading music, documents and applications, accessing or storing films. This is not a malicious, but the use of organisation network will increase pressures placed on electronic storage and resources. This might risk the whole system and be infected by opening the door to viruses which attach themselves to download and could finish by being stored on the system (Goh 2003; Mahfuth et al. 2019). 60% of employee respondents stated that they did store personal materials on work computers, but 12% of employees downloaded non-work-related content (Information Systems Security Association 2013). Furthermore, the non-work-related issue such as downloading is particularly sensitive, as an employee could place a whole organisation at risk of breaching government regulations, for example accessing a banned site or illegal content and the use of browsers and torrents blocked by the government.

Some employees may deliberately hack into the organisation's information technology system, either to steal information or to disrupt the organisation's activities (McAfee 2012). In 2018, a survey conducted by Price Waterhouse Coopers, found that 26% of insider threats committed were for financial gain or revenge. Any theft of sensitive or commercially useful data, if leaked on to competitors, could impact negatively on the organisation and lead to financial losses. Unlike hackers, who are on the outside, and therefore need to both break into the network and find the data they are looking for, insider employees have easy access to the information (Joshi et al. 2019; Mehan 2016).

Given all the potential risks created by the insider-related human factor, many organisations have implemented a number of administrative and technical measures. These measures become part of their overall information security management that is based on a number of policies, procedures and best practices (Alhogail 2016; Mahfuth et al. 2019).

### 2.3.4 The Human Element in Information Security International Standards and Guidelines

A number of various information security international standards and guidelines have been designed, and placed in order, to support the information security management requirements and protect organisations information assets in the term of confidentially, integrity and availability (Von Solms 1999). The standards and guidelines present principles and recommendations that focus on the human factor in information security. The following are some of the information security international standards and guidelines that have been developed and published:

1. **Information technology – Security techniques – Information security management systems – Requirements (ISO/IEC 27001:2018):** is the internationally accepted standard for good practice for information security management. It provides how to establish, implement, operate, monitor, review, maintain and improve an Information Security Management System (ISMS) (Da Veiga & Eloff 2007; Ismail et al. 2010). This standard mentioned several human behaviour issues, such as human resource security, compliance issues, registering users, the management of passwords, how to control user access and the need for a clear work environment. It also highlights the importance of staff training to raise awareness and understanding of security issues (Alhogail 2016).

2. **Control Objectives for Information and Related Technology (COBIT 5):** is a framework that was developed by Information System Audit and Control Association. It provides and demonstrates the best way of communicating the right information security culture to various groups, including stakeholders and employees (COBIT 2000). In addition, it outlines the acceptable information security behaviour between the members of the organisation (Ismail et al. 2010; Alhogail 2016).

3. **The Information Technology Infrastructure Library (ITIL):** is a collection of best practices for IT management. The ITIL contains a four-P model (People, Processes, Products and Partners) that illustrates how management needs to incorporate these elements in an efficient and workable combination. ITIL supports organisations to be aware of the business value that their IT services provide to both internal and external

stakeholders. ITIL states that management has to define information security principles, taking account all local laws and regulations in the process, then ensure that they are followed in the organisation. Any planned controls which are introduced and impact on daily activities must be regularly monitored with various inspections to ensure they are effective (Alhogail & Mirza 2015). ITIL thus takes the human factor into account when offering guidelines on how to promote security awareness.

The above standards and guidelines are intended to guide the organisation how to control and deal with human-related risks. Many organisations use these international standards and practices as guidance and as part of their initial step towards selecting convenient controls and process in order to manage their information security.

However, the previous standards and practices provide general guidance and describe different process and control needed for successful security implementation, not the solution for managing information security (Hone & Eloff 2002). According to Siponen (2006) and Baker and Wallace (2007) studies, indicate that these standards do not provide how well the process is implemented or how effective they are in practice. In addition, information security cannot be solved alone by just implementing these standards, because of the complexities of human interaction with information security systems (Bess 2012). The above standard and practices do not provide a clear reference guide on how to deal with the challenge of insider threats by tackling the human factors which are the source of these risks.

Furthermore, Von Solms (2000) discussed the evaluation of information security approach by dividing its development into four waves. Each wave presented a comprehensive set of elements that should be considered in order to ensure the protection of information in the organisation. In his third wave, the researcher has highlighted the importance of having incorporate standardisation of information security, best practices, and security certification and cultivates an information security culture in order to support the security policies, procedures and responsibilities of the organisation (Von Solms 2000).

It is evident from the above that the human factor is considered as a major cause for security breaches, whilst at the same time, could be is a significant, positive asset to organisational information. So, it is important to examine relationship between all security issues and the human factor in order to establish the information security culture of an organisation.

Therefore, in order to achieve the effective information security and manage security risks, the organisation should understand the information security culture, and this will be a significant step towards addressing the human element (Alhogail 2016; Da Veiga & Eloff 2010; Mahfuth et al. 2019).

## 2.4 Conclusion

The growth of the technological environment has created challenges to information security and increased the potential for breaches in security. Several studies, surveys and reports have indicated that information security can no longer be achieved or improved by technological issue alone but also is associated with people who actually operate these systems. The interactions between human and information security have increased the possibility of security risks and breaches. There is evidence from research that the human factor is a risk in relation to information security. Therefore, an understanding of the human factor is required in order to determine the reason behind unacceptable behaviour leading to security data breaches and to make information security effective in organisations.

# Chapter Three :

# Information Security Culture

## 3.1 Introduction

The first objective of this chapter is to provide a literature review that formulates an understanding the concept of information security culture by investigating and critical analysing of current studies and practice in the information security culture field. The second objective is to provide a theoretical perspective, through a review of the relevant literature regarding identified key factors that strongly assist the creation of information security culture in the organisation. The first section presents the concept of culture, an introduction to the organisational culture and its links to information security culture. The second section focuses on currently available information security culture definitions in order to serve it as a reference to understanding. The third section discusses various issues related to information security culture. Then, it explores current frameworks with identified factors, which have an impact on information security culture. This is followed by a summary of the literature and a discussion leading to the identification of a literature gap and further research required in the information security culture field. The next section provides a literature background for each factor or constructs that were presented in previous studies in the information security culture field. After that, a section illustrates the interaction and relationship between the identified factors. The final section in this chapter explores other factors that have not been considered in the information security culture research, in order to integrate important factors into a comprehensive framework for this research.

## 3.2 Culture within Organisations

The concept of culture has been defined by several researchers. For instance, Plog and Bates (1976) defined the culture as “a system of shared beliefs, values, customs, behaviours, and artefacts which the members of a society use to adapt with their world and with one another, and that are transmitted from generation to generation through learning”. The concept of culture relates to collective understanding that distinguishes individuals from different countries in accordance with anthropological social theories (Hofstede 2001). Thus, it is possible to comprehend an organisational culture that defines employees’ perceptions of their organisation, which develops with time through the influence of management and the individuals themselves (Schein 1999).

Culture has been presented as a factor affecting the performance of individuals, adoption of information technology, integration process of information systems, information security management, knowledge transfer and change management (Hofstede 2001). Culture is often believed to be vital in the determination of organisational success or failure (Deal & Kennedy 1982). Yet, a mere 5% of total organisations have actually set a definition of their culture, as the design of the corporate culture has been structured by senior management (Atkinson 1997). Indeed, it can prove highly detrimental to the organisation when the management staff members do not have cultural awareness (Hagberg & Heifetz 2000). The corporate or organisational culture helps to determine different employees' behaviour (Schein 1999; Thomson & Von Solms 1998), as well as influencing what is determined to be acceptable within the organisation (Beach 1993). It has also been stated that a potential negative side stems from oversimplifying cultural awareness, as it is often necessary to develop the understanding of various levels and remits of culture (Schein 1999).

## 3.3 Culture of Information Security and the Organisational Culture

Advancement in the awareness of culture in regard to information security would help to minimise employee misbehaviour and the risk imposed by interacting with information (Da Veiga & Martins 2015; Wiley et al. 2020). When a more comprehensive corporate or organisational culture of information security is developed and maintained, it becomes possible to manage information security more rigorously (Von Solms 2000). As information security has become a function within organisations, the information security culture has developed to become a part of the organisation, as the maintenance of information security is now a stable part of any employee's daily activities (Schlienger & Teufel 2003). The study of Dojkovski et al. (2007) stated that the culture of local organisations highly affects the information security culture formation. The practice of information security must develop into a set part of corporate culture, in order to achieve a secure environment for the information assets.

Corporate culture helps to guide an organisation's activities, as well as its employees through the implementation of activity constraints and influence upon employee behaviour by determining what the employees are able to do (Thomson et al. 2006). Consequently, this should be utilised in order to establish the employees' information security behaviour (Lopes & Oliveira 2014). In particular, various research studies have analysed the correlation that

exists between organisational and information security cultures. For instance, the specific challenges that information security culture faces in relation to organisations have been detailed (Ashenden 2008). Meanwhile, a model of the relationship that exists between the culture within organisations and information security management (ISM) was investigated, which quantified organisational traits and how they affected the culture of information security (Chang & Lin 2007). A framework was presented by Lim et al. (2009; 2010) that would assist to determine whether the culture of information security is integral to the overall structure of organisational culture. Likewise, a different study analysed eight different dimensions of organisational culture and their effects on information security (Ruighaver et al. 2007). Organisations and the role of information security culture were discussed by Connolly and Lang (2015), in order to achieve greater levels of security of information systems. As a result of these aforementioned studies, it can be determined that organisational culture impacts greatly upon both the management of information security and its performance.

However, each individual within an organisation is expected to play their role in the process of information security, and their varied attitudes and assumptions in regard to the implementation of information systems and security can benefit positively to the organisation. Also, new and improved technical advances increase the applicability of utilised tools to help control and redefine unauthorised behaviour by employees. Therefore, it is vital that the assumptions, beliefs and values that define the behaviour of users are understood. Although this can become challenging due to rapid changes in the environment of information systems and the threats to their security, individual knowledge and skills must be understood to potentially alter (Da Veiga & Martins 2015; Parsons et al. 2014).

One of the most common models of organisational culture within the information security field resulting from the literature review, is that corporate culture can be best represented by Schein's model of organisational culture. This model has been used as a basis for developing a number of information security culture frameworks (Karyda 2017; Van Niekerk & Von Solms 2010).

### 3.3.1 Schein's Model of Organisational Culture

The organisation or corporate culture as represented by Schein (1999) is an arrangement of commonly inferred assumptions, which a group learns during the problem-solving process regarding the external adaptation and internal integration. The corporate culture should be used

to educate new members in how they should perceive, think, and feel regarding these problems. The Schein's model of corporate culture contains three levels which are artefacts, espoused values, and shared tacit assumptions.

1. ***Artefacts*** are connected to the visible layer and concern the normal behaviour in the organisation which can be seen and quantified (Van Niekerk & Von Solms 2006). Also, Okere et al. (2012) noted that artefacts are made up of behaviour patterns, security handbooks, awareness courses, language and technology.
2. ***Espoused values*** correspond to the 'reasons' which the insiders of an organisation give in relation to the perceived artefacts (Van Niekerk & Von Solms 2006). Schein (1999) stated that these adopted values incorporated strategies, goals, policy statements and a range of other transcribed records, which represent the official values, principles and vision of the organisation.
3. ***Shared tacit assumptions*** concern employees' beliefs and values (Van Niekerk &Von Solms 2006). Schein (1999) stated that they are brought about by prior integrated learning experiences linked to previous successful behaviour. Van Niekerk and Von Solms (2006) also mentioned that on continued organisation success, the beliefs and values evolve would become communal and accepted by everyone. As a result, begin to constitute the organisation's cultural core. The Schein's corporate cultural model is presented in Figure 3.1.

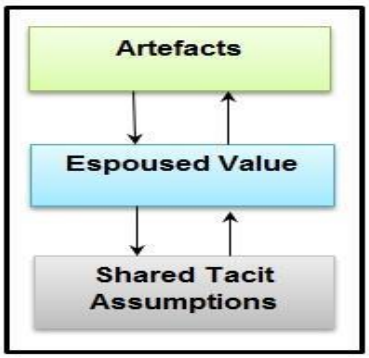



**Figure 3.1: Schein's Three Level Model**

Van Niekerk and Von Solms (2006), confirmed Schein's model and included a fourth level-information security knowledge, that supports other three levels. They argued that it is not feasible to expect all employees to have the requisite knowledge regarding information

security. It is incumbent on the management to ensure that all employees have the necessary information security knowledge so they could be empowered to behave in a secure manner.

Information security knowledge supports the other three levels. With artefacts, it is necessary that employees have sufficient information regarding security, which continues to allow them to carry out their job role safely and securely. In terms of espoused values, the employees need to have adequate knowledge and information regarding information security, which can then be included in relevant policy documents and organisation security requirements. For shared tacit assumptions, it is important that an employee's beliefs do not conflict with an espoused value. For instance, if an employee was not aware of why a specific control is needed, the employee may purposely ignore the security control (Van Niekerk & Von Solms 2006). In addition, Schlienger and Teufel (2003) concluded that having the requisite information and knowledge would contribute to a greater understanding and lead to greater compliance.

## 3.4 Introduction to Information Security Culture

In order to improve the security of information assets, an understanding of the human behaviour aspects is required to reduce information security breaches (Karyda 2017; Straub & Welke 1998). Various approaches have been used in order to provide guidance and describe the implementation of security controls that touch human components such as awareness, education and training, but they do not focus on how to direct, measure and change the employee behaviour (Da Veiga & Eloff 2010; Mahfuth et al. 2017). Recently, one of the approaches that has been used and considered as a way to reduce the risks posed by employees is that establishing a security-aware culture inside the organisation (Da Veiga & Martins 2015; Karyda 2017).

Since human behaviour is considered as one of the main threats to the protection of information that could lead to information security incidents, organisations need guidance to establish a strong information security culture inside the organisation (PwC 2018, Ponemon 2019). Similarly, Von Solms (2000) suggested that information security could be managed more properly if a comprehensive organisational security culture was in place. It is vital to creating an information security culture to protect the information assets of organisations since users frequently pose threats to the information assets (Alnatheer et al. 2012; Da Veiga 2008; Tessem & Skaraas 2005). By having an effective security culture, the security risks will reduce, the

user will tend to behave in a more secure manner and the security level in the organisation will improve (Alhogail 2016; Ruighaver et al. 2006).

The concept of information security culture within an organisation has been one of the most important issues that guide organisations on how to operate, protects assets and exerts an influence on the employee's behaviour with regard to security (Nasir et al. 2019; Walton 2015). The creation and establishment of information security culture are necessary for having an effective information security inside organisations (Alnatheer et al. 2012; Eloff & Eloff 2005). However, the information security culture is a new and emerging area of research (Karlesson et al. 2015; Sas et al. 2020; Walton 2015). Researchers began to recognise that the information security culture could be an important factor in maintaining an adequate level of information security in organisations (Mahfuth et al. 2017; Ruighaver et al. 2007). Some organisations have started to focus on culture and have required a comprehensive framework and guidelines to establish a security aware culture (Alhogail & Mirza 2014; Da Veiga & Martins 2015). Numerous studies have attempted to confirm the need to create and establish information security culture in the organisation in order to manage security in an effective way (Mahfuth et al. 2017; Nasir et al. 2019). Creating an information security culture in an organisation is about guiding employees to respect, accept the values, standard and policies regarding security and behave in a certain manner in their working environment to protect its information assets (Da Veiga & Martins 2015; Walton 2015).

### 3.4.1 Information Security Culture Definition

Most of the researchers attempted to define the concept of information security culture in order to cultivate it inside the organisation and manage security in an effective way. They defined information security culture in many different ways by using a mixture of theories and principles from other research areas (Mahfuth et al. 2017). Some of these definitions are very cleared and detailed, whereas others are much shorter. According to Chia et al. (2002) and Malcolmson (2009), they indicated that the definition of information security culture is the subject of argument and several researchers have proposed a variety of different definitions.

One of the earlier definitions of information security culture was provided by Dhillon (1995), who described it, as "a totality of patterns of behaviour in an organisation that contribute to the protection of information of all kinds". He found that the information security culture is derived

from the behaviours such as attitudes, values and beliefs of employee and their behaviour could affect the security of the organisation.

Another definition of information security culture was presented by the Information Security Forum (2000). It discussed the definition of information security culture and identified factors in order to measure the information security culture in the organisation. In this report, the information security culture relates to the common values and beliefs that organisational members have it regarding information security with the interaction between them and the information assets of the organisation causing a particular set of behaviour and incidents (Information Security Forum 2000). However, the integrity, availability and confidentiality of information might be affected by a number of situations which occur due to information security incidents in the organisation. The causes of these events could be linked back to employees' behaviour and their interactions with information. Also, the system will be affected by the values and beliefs of employees with respect to information security and the organisation's policies (Information Security Forum 2000). Consequently, employee behaviour and the number of incidents, which occur in an organisation are reflective of the information security culture of the organisation (Information Security Forum 2000). Additionally, according to Information Security Forum (2000), they concluded that there is still a lack of a strong information security culture in organisations and literature.

Some researchers linked their definition of information security culture to theories. Indeed, most studies used Schein's model of organisation culture in defining the concept of information security cultures, for example, Martins and Eloff (2002), Schlienger and Teufel (2003), Vroom and Von Solms (2004), Da Veiga and Eloff (2010) and Alhogail and Mirza (2014). Schlienger and Teufel (2003) and Vroom and Von Solms (2004) indicated that the information security culture is a subset of organisation culture and concerned with three main areas, which are artefacts and creations; collective values, norms and knowledge; and basic assumptions and beliefs. They concluded that an information security culture should be incorporated into all activities to become a natural aspect of every employee's daily activities.

There are some researchers such as Martins and Eloff (2002) and Ngo et al. (2005) have similar perspective regarding the information security culture. They see the information security culture as a way of how things are done and held by employees in the organisation. They

believed that the information security culture is derived from presumptions regarding perceived acceptable behaviour and characteristics, which has an effect on how people deal with information security in the organisation. Moreover, Malcomson (2009) argued that the information security culture is derived from the assumptions, attitudes, values, beliefs and behaviour of employees and these could have an impact on the information security of an organisation.

Furthermore, studies of Da Veiga and Eloff (2010) and Alhogail and Mirza (2014) concluded that information security culture is associated with employees' assumptions, attitudes, beliefs, values, knowledge and behaviour that used as a guidance of doing activities inside the organisation in order to preserve the information assets and impacting the behaviour of employee in an acceptable way by considering information security as a natural part of employee's daily activities. In addition, Da Veiga and Eloff (2010) also believed that this information security culture changes over time because over time people gain more experience and work after experiencing various life situations and as a result, their perceptions change.

The previous studies have defined the information security culture as a reflection of the beliefs and values of organisation members. They recognised the importance of creating the information security culture in order to manage security effectively within the organisation. Therefore, this research defines the concept of information security culture as a collection that related to artefacts, perceptions, attitudes, values, assumptions and knowledge which hold by an employee for doing daily activities toward the information security in the organisation.

It is important to clearly define what is meant by the two terms "security "and "culture" (Alnatheer et al. 2012). The complexity of defining and understanding both elements "security" and "culture" makes the information security culture more challenging (Schlienger & Teufel 2003). According to Schlienger and Teufel (2003), a security culture includes the social, cultural and ethical measures which are put in place to make sure the organisational members improve their security behaviour. Additionally, Schlienger and Teufel (2003) argued that measuring security and culture will be a complex task, time consuming and any results will not be easily turned into generalisations. So, it is difficult to precisely define or measure the "culture". Thus, it is necessary to quantify and analyses the most important elements and

factors which shape and measure the information security culture (Alnatheer et al. 2012; Nasir et al. 2019; Walton 2015).

In general, all the above definitions have focused on the manifestation and explanation of information security culture and its role within organisations. Ruighaver et al. (2007) and Alnatheer et al. (2012), believed that some researchers did not clearly define the term of information security culture because some of these definitions only focus on the manifestation of information security culture within organisations.

### 3.4.2 An Overview of Existing Information Security Culture Approaches

A comprehensive review of information security culture has been conducted in order to identify the key literature that relating to the information security culture and gain an understanding of the information security culture frameworks, models and factors which have been proposed to cultivate an information security culture inside the organisation. This review will lead to the identification of the gaps in the information security culture research. The review based on a number of information systems and information security journals, articles, textbooks, conference proceedings retrieved from various academic databases, (such as ACM Digital Library, Elsevier Science Direct, Emerald digital library, online publications, IEEE electronic library, EBSCO, Wiley online library, Springer publication, etc.) and the reports of several information security institutes, (such as Egress, Price Waterhouse Coopers, Ponemon, and Verizon).

Since information security cultures is still an emerging area of research, many researchers have been conducted different topics of studies in the information security culture field. There are several literature reviews that offered an overview of existing research that focused on the information security culture such as Connolly and Lange (2013), Alhogail and Mirza (2014), Karlsson et al. (2015), Pevchikh (2015), Mahfuth et al. (2017), Nasir et al. (2019) and Sas et al. (2020) studies. Their literature analysis concluded that most issues that been investigated in the information security culture is related to one of the following:

1. Conceptualisation of information security culture in order to define, understand the concept and identify factors that affect or affected by the information security culture.

2. Cultivation and establishment of information security culture in order to assist organisations, to observe the behaviour of people and change the current culture to a more secure one. It is concerned with the examination of the current security culture in the organisation to determine the weakness area that requires more attention for change (Ngo et al. 2005). Also, it assists of how to develop a security culture to be an acceptable level in the organisation (Da Veiga & Eloff 2010).
3. Assessment of information security culture in order to measure and assess the level of the information security culture and identify if it is on the adequate level to provide quality protection to information assets (Da Veiga & Eloff 2010; Nasir et al. 2019; Walton 2015).

Recently, there has been a large volume of published studies that presented different approaches and frameworks that guide the researchers and the implementation of the information security culture (Karlsson et al. 2015; Pevchikh 2015; Nasir et al. 2019; Sas et al. 2020). Each study differs in depth of research regarding the information security culture. For instance, some researchers focus only on developing an understanding the concept of information security culture (OECD 2005; Tessem & Skaraas 2005), on defining the information security culture (Information Security Forum 2000; Martins & Eloff 2002; Kuusisto & Illoven 2003) or providing a set of principles, guidelines or checklist (Zakaria & Gani 2003; OECD 2005; Kraemer & Carayon 2005; Ruighaver et al. 2006; Detert et al. 2000).

Some researchers performed in-depth studies to illustrate a way to cultivate an information security culture by developing a framework (Dojkovski et al. 2006; Da Veiga & Eloff 2010; Alfawaz et al. 2010; Alnatheer et al. 2012; Alhogail & Mirza 2014; Sherif et al. 2015; Masrek et al. 2017; Nasir et al. 2017) or to assess an information security culture (Martins & Eloff 2002; Schlienger & Teufel 2005; Da Veiga & Eloff 2010). Other researchers investigated the mechanisms or components that could influence the information security culture and employee behaviour (Schlienger & Teufel 2005; Thomson et al. 2006; Kraemer et al. 2009; Ruighaver et al. 2007; Van Niekerk & Von Solms 2010; Alnatheer et al. 2012; Martin & Da Veiga 2015; Sherif et al. 2015). In addition, some researchers such as Robbins (2001), Kreitner and Kinicki (1995) and Schein (1999) focused on the field of organisational behaviour and the way in which the organisational culture could be developed in order to understand how to cultivate an information security culture in organisation settings.

However, most of the researchers used other theories and explained by using different theories and established principles from other previous research areas (Connolly & Lang 2012; Karlsson et al. 2015; Nasir et al. 2019). For instance, most of researchers in the information security culture field used theories from different perspectives which belong to organisation behaviour (Leach 2003; Stanton et al. 2005; Vroom & Van Solms 2004; Van Niekerk & Von Solms 2005), to communication (Schlienger & Teufel 2003), to organisational culture (Chang & Lin 2007; Alfawaz et al. 2010), to national culture (Chaula 2006; Alfawaz et al. 2010), to total quality management (Chia et al. 2002) or to principles of psychology (Schein 1999). One of the most commonly used theories within the information security field and resulting from the literature review is that the information security culture can be best represented by adopting Schein's model of organisational culture. This has been used as a basis for establishing various information security culture frameworks and models (Van Niekerk & Van Solms 2010; Karlsson et al. 2015; Nasir et al. 2019).

A wide range of useful models and approaches that highlight the importance of creating the information security culture have been created (Alhogail & Mirza 2014; Karlsson et al. 2015; Nasir et al. 2019; Pevchikh 2015). The majority of studies in this field have promoted the benefits of information security culture and provides recommendations and guidelines for creating and assessing the information security culture (Nasir et al. 2019; Sas et al. 2020). However, the importance of creating the information security culture within organisation resulted from the fact that the human dimension in information security is always considered to be the weakest link (Karyda 2017; Schlienger & Teufel 2003). Several researchers such as Furnell and Thomson (2009), Da Veiga and Martins (2015), Karlsson and Hedström 2014 recommend that there must be a real investment in people and in information security culture in order to achieve the required protection in organisation setting. Similarly, according to Dojkovski et al. (2007) and Alhogail (2016), there is evidence the strong information security culture might deal with many of the behavioural issues that cause information security breaches inside organisations.

#### *3.4.2.1 Review of the Factors and Issues Relating to Information Security Culture*

Since the information security culture has been assigned to control the human factor in order to improve information security in organisations, it is important to understand how employees should behave, to keep the organisation's information secure and to understand the factors

behind their behaviours to support the security of information assets and avoid insider threats (Alhogail & Mirza 2014; Da Veiga & Martins 2015; Wiley et al. 2020). Researchers believe that there are a number of factors that affect the individual behaviour should be considered in order to improve the security of information assets and measure the information security culture within organisations (Alnatheer et al. 2012; Nasir et al. 2019).

The literature analysis revealed that most available studies concluded that there are different factors or components that could shape or change the information security culture in order to protect the information security in the organisation (Nasir et al. 2019; Sas et al. 2020; Walton 2015). Additionally, some studies stated that cultivating an information security culture could be influenced by different factors or constructs (Alnatheer et al. 2012; Alhogail & Mirza 2014).

It is essential to gain an overview of the information security culture models and structures, which already exist by conducting a comprehensive review. This was the starting point for this research. Therefore, the first aim of the comprehensive review is to recognise and investigate the conceptualisation of the information security culture. This will help to create a conceptual framework which will assist and improve organisations' security management. The second aim is to list and analyse the constructs or components that were provided in each study in the information security culture field in order to explore the relationship between constructs and design the framework for this research. The review will also focus on studies that assess the information security culture to determine which studies provide the most comprehensive perspective. A focus on studies that included questionnaires would help to develop a reliable and a valid information security culture framework.

Numerous researchers have examined the information security culture and factors that could possibly influence the culture and behaviour of employees (Alnatheer et al. 2012; Alhogail 2016; Da Veiga & Eloff 2007; Schlienger & Teufel 2005; Zakaria 2004). Some of these studies have defined principles that could be followed, whereas others developed a comprehensive framework that offer different human issues that need to be identified and included in order to establish and assess the information security culture. Their work differs in terms of comprehensiveness and in term of the research field that information security culture is combined with. They presented various components and factors that influence employee behaviour toward information security.

Table 3.1 summarises the current researcher perspectives on information security culture. It provides a list of the information security culture research components or factors identified across different studies. More specifically the table recaps the different research perspectives that have been evaluated according to the following criteria: development of the assessment instrument, content validity, construct validity and reliability. These criteria assist in determining which study provides the most comprehensive perspective, identifying the existing gap in the information security culture research literature and what constitutes a valid and a reliable information security culture questionnaire.

The first column represents different information security culture research frameworks which are listed in chronological order according to the year in which the research work was published. The second column represents the identified constructs and findings for each study. The third columns indicate whether the study has conducted survey methods to assess and measure the information security culture. The fourth and fifth columns represent the content and construct validity in order to ensure whether the researcher used the theoretical perspective as a foundation (input) for developing the questionnaire and to ensure that the results are accurate when using the assessment instrument or measurement - thereby providing a valid result. The sixth column represents whether the frameworks constructs are reliable. The seventh column shows whether the study provides a statistical analysis of the data for determining the reliability of the assessment instrument.

**Table 3.1: A Summary of Currently Proposed Constructs Across Different Researches in Information Security Culture**

| # | Research | Constructs/Findings | Assess | | | | |
|---|---|---|---|---|---|---|---|
| | | | **Assessment Instrument (Questionnaire)** | **Content Validity** | **Construct Validity** | **Reliability** | **Statistical Analysis** |
| 1 | Martin & Eloff (2002) | Policy, benchmark, risk analysis, budget, management, trust, awareness, ethical conduct, change. | Yes | Yes | - | - | - |
| 2 | Chia et al. (2002) | Security budget, security expenditure, employee security awareness, security risk of staff, implementing security policy, making security suggestions, security ownership, audits. | - | - | - | - | - |
| 3 | Helokunnas & Kuusisto (2003); Kuusisto & Ilvonen (2003) | **Security culture framework:** Standardization, Certification, Measurement of information security.<br>**Content components:** People's attitude, Motivation, Knowledge, Communication, Compliance. | Yes | - | - | - | - |

| # | Research | Constructs/Findings | Assess | | | | |
|---|---|---|---|---|---|---|---|
| | | | **Assessment Instrument (Questionnaire)** | **Content Validity** | **Construct Validity** | **Reliability** | **Statistical Analysis** |
| 4 | Schlienger & Teufel (2002,2003, 2005) | Schein organisational culture model that has 3 layers:<br>**Corporate policies** (policy, organisation structure, resources).<br>**Management** (implementation of security policy, responsibility, qualification and training, awards and prosecutions, audits, benchmarks).<br>**Individual** (attitude, communication, compliance). | Yes | Yes | Yes | Yes | - |
| 5 | OECD (2005) | Awareness, responsibility, response, ethics, democracy, risk assessment, security design and implementation, security management and reassessment. | - | - | - | - | - |
| 6 | Tessem & Skaraas (2005) | Long term plan, change management, top management, participation, branding, organisation culture. | - | - | - | - | - |

| # | Research | Constructs/Findings | Assess | | | | |
|---|---|---|---|---|---|---|---|
| | | | **Assessment Instrument (Questionnaire)** | **Content Validity** | **Construct Validity** | **Reliability** | **Statistical Analysis** |
| 7 | Ruighaver et al. (2005, 2006) | **Security governance framework**: structural mechanism, functional mechanisms, social participation **Influences on security culture framework dimension:** control, coordination, ownership, responsibility. | - | - | - | - | - |
| 8 | Dojkovski et al. (2006) | Individual and organisational e-learning. Ethical, national and organisational culture. **Managerial:** Policies and procedures, benchmarking, risk analysis, budget, management, response, training, education, awareness, change management.<br><br>**Behavioural:** Responsibility, integrity, trust, ethnicity, values, motivation, orientation personal growth. | - | - | - | - | - |
| 9 | Kraemer & Carayon (2005,2007) | Employee participation, training, hiring practices, reward system, management commitment, communication and feedback. | - | - | - | - | - |

| # | Research | Constructs/Findings | Assess | | | | |
|---|---|---|---|---|---|---|---|
| | | | **Assessment Instrument (Questionnaire)** | **Content Validity** | **Construct Validity** | **Reliability** | **Statistical Analysis** |
| 10 | Da Veiga & Eloff&Martin (2007, 2010, 2015) | **Leadership and governance** (sponsorship, strategy, IT governance, risk assessment, ROI/metrics/measurement);<br><br>**Security management and organisation** (legal and regulatory, program organisation);<br><br>**Policy** (policies, standard, procedure, guidelines, best practice, certification, certification); **security program management** (monitor, audit, compliance); **user security management** (awareness, training, trust, privacy, ethical conduct); **technology protection and operations** (sys development, technical operation, physical and environment, asset management, incident management, business continuity); **change.** | Yes | Yes | Yes | Yes | Yes |
| 11 | Alnatheer (2012) | **Factors influence Security Culture:** Top management, policy enforcement, IS training. | Yes | Yes | Yes | Yes | Yes |

| # | Research | Constructs/Findings | Assess | | | | |
|---|---|---|---|---|---|---|---|
| | | | **Assessment Instrument (Questionnaire)** | **Content Validity** | **Construct Validity** | **Reliability** | **Statistical Analysis** |
| | | **Factors reflect Security Culture:** Security awareness, security ownership. | | | | | |
| 12 | Alhogail & Mirza (2014, 2015); Alhogail (2016) | **Organisation dimension:** Management (policy, practice, communication); environment (national culture, standards and regulations, organisational culture);<br><br>**Employee dimension:** preparedness (awareness and training, change); responsibility (reward, monitoring and control, acceptance). | Yes | Yes | Yes | Yes | Yes |
| 13 | Sherif, Furnell &Clarke (2015) | **National culture, organisational culture, Security compliance** (IS behavior, management support, policy, awareness and education, acceptance). | - | - | - | - | - |

| # | Research | Constructs/Findings | Assess | | | | |
|---|---|---|---|---|---|---|---|
| | | | **Assessment Instrument (Questionnaire)** | **Content Validity** | **Construct Validity** | **Reliability** | **Statistical Analysis** |
| 14 | Masrek, Harun & Zaini (2017) | **Management support** (information security commitment, information security importance)**, Policy and procedures** (information security policy effectives, information security detective), **Compliance** (information security monitoring compliance, information security consequences), **Awareness** (information security responsibility, information security training), **Technology** (information technology capability, information technology compatibility), **Budget** (information security budget practice, information security investment). | Yes | Yes | Yes | Yes | Yes |

The fourteen studies in Table 3.1, were reviewed and show an essential knowledge for the current study in terms of identifying factors that assist in establishing the information security culture in order to design a conceptual framework. The summary discussion of the current perspective offered by each study listed in Table 3.1 is provided in Appendix A.

## 3.5 Discussion and Resulting Research Objectives

Based on the literature review, most of the available studies indicate that information security is relevant to people's motivation, societal and cultural aspects. Since the human element of information security cannot be solved by technical and management measures, many studies such as Furnell and Thomson (2009) and Da Veiga and Martins (2015) have agreed that managing an individual's behaviour is best achieved through establishing an information security culture in the organisation. The literature analysis has revealed that the information security culture is considered as one of the main ingredients in the success or failure of security implementation in the organisation as it affects security practices and human behaviour. The information security culture must be seen as an asset in order to ensure security and reduce breaches in organisations. Developing an effective security culture is an essential step for having an adequate level of information security in organisations. As consequence, the information security culture contribution is highly important for the organisation.

The literature confirms that the concept of information security culture has been established and its importance has been investigated and explored. Many different standards, guidelines and relevant frameworks have been developed for establishing and assessing the information security culture in order to manage security in an effective way. Furthermore, there are studies that demonstrates the importance of understanding factors and issues that could possibly influence the information security culture (Alhogail 2016; Alnatheer et al. 2012; Da Veiga & Martin 2010).

Most of the available research perspectives discussed above focus on providing principles (Helokunnas & Kuusisto 2003; Kraemer & Carayon 2005; Kuusisto & Ilvonen 2003; Tessem & Skaraas 2005; OECD 2005), that could be followed, or on developing comprehensive frameworks (Alhogail 2016; Alnatheer et al. 2012; Chia et al. 2002; Da Veiga & Martin 2010; Dojkovski et al. 2006; Ruighaver et al. 2006; Masrek et al. 2017; Martins & Eloff 2002; Sherif et al. 2015; Schlienger & Teufel 2003), that involved in identifying various components and factors that should be included in order to establish and assess the information security culture.

These studies have developed a comprehensive information security culture model and contribute a good understanding of how organisations could create and maintain an acceptable level of information security culture. They concluded that the information security culture is a product of various elements or factors such as top management, security policy, security awareness, security education and training that determines individual behaviour within an organisation. For instance, some of the studies such as Martins and Eloff (2002) present various information security components on a different level of organisation behaviour that could be used as a guidance to cultivate an adequate level of information security culture. Another study by Schlienger and Teufel (2003) has used the Schein organisational culture model to study and evaluate the information security culture. Their study argued that every information security issues, or elements could be allocated a place in the organisation's cultural model and could represent the three levels which are an artefact, a value and an assumption.

The study by Da Veiga and Eloff (2007) provides a complete list of information security components that deal with the human, process and technical issues that are used to compile a comprehensive information security governance framework, that will help in establishing an acceptable level of information security culture. In addition, the study of Alhogail and Mirza (2014) develop the human diamond framework. Their framework provides a comprehensive view of various human issues that influence employees' behaviour based on a social cognitive theory of Bandura (1999) and previous studies.

Unfortunately, most of the previous studies show different factors or elements that could affect the information security culture inside the organisation. Some of these studies did not discuss what specific factors or elements might be conceptualised or shape the information security culture itself. They ignored the factors that constitute the information security culture itself (Alnatheer et al. 2012). Also, they stated that an information security culture could be created without determining what factors those constitute the information security culture.

However, Alnatheer's approach is the only research work that specified what factors conceptualise an information security culture. Alnatheer et al. (2012) study developed a conceptual model that identified and examine a range of factors that constitute or influence the information security culture in the Saudi Arabia settings. But this study was unable to develop a valid scale for some identified factors such as ethical conduct, risk assessment and security compliance due to its low validity.

Since it is important to assess the information security culture to identify whether the culture is on an adequate level and prepare plans for improvements in order to provide a protection of information assets, the developed model or framework should supply a validated information security culture assessment instrument (Da Veiga & Eloff 2010; Walton 2015). The developed information security culture framework should be used to create the security culture and at the same time should be served as the foundation for the assessment approach. The designed framework could provide direction for formulating a security culture assessment instrument. For instance, the designed frameworks should contribute towards identifying all the requirements components that organisations have to consider when establishing the security culture. Thus, the developed framework could be used as a practical reference and ensure that the approach is comprehensive in the creation of the security culture. Additionally, this will contribute to the effectiveness of the approach, whereby the same framework could be used for cultivating and assessing the information security culture. Therefore, it is important to design a reliable and valid instrument for assessing the information security culture (Straub 1990; Da Veiga & Eloff 2010).

The review of the literature has indicated that there is a growing interest in security culture assessment research, which includes developing and validating assessment instruments. A few frameworks and models had provided a validated security culture assessment instrument. Some studies such as Da Veiga and Eloff (2010) and Schlienger and Teufel (2005) highlighted the importance to measure the information security culture in order to diagnosis of security issues and improve the level of a protection of information assets. Only four of the above studies perspectives in Table 3.1(Da Veiga and Eloff 2010; Kuusisto and Ilvonen 2003; Martins and Eloff 2002; Schlienger and Teufel 2005) focus on the assessment of the information security culture. Martins and Eloff (2002) study were the first study that provides an assessment instrument for information security culture. They developed a theoretical information security culture framework that assessed the information security culture. But their designed information security culture questionnaire was not validated in the real world. The second study was Kuusisto and Ilvonen (2003) study. They used ISO/IEC (17799:2000) and BS7799-2:2002 (BS7799 2002) standards to perform assessments in SMEs to determine the state of information system security but did not assess the content components of their approach.

Schlienger and Teufel (2005) provided a validated information security culture assessment instrument. They created a questionnaire designed to investigate how official rules impact on

employee security behaviour. They developed assessment instrument for analysing the information security culture of an organisation based on internal marketing, in order to create and maintain the information security culture. They proposed a model consists of five phases, which are pre-evaluation, strategic planning, operative planning, implementation and post-evaluation for assessing the information security culture. They designed the assessment tool based on the three levels of organisational behaviour of Robbins (2001), and on Schein (1999) study. They perform a survey with interview employees in a private bank and the working group (Information Security Society) in Switzerland to ensure the practicability of the process and used the data to validate the assessment instrument. This study contributed towards the effective development of an assessment instrument that could be used by the organisation and that has been tested for reliability and validity. They argued that in order to create and maintain the information security culture continuously, there has to be an ongoing measurement and analysis of the culture. This could be achieved by use of an ongoing survey during the lifetime of the organisation.

Another study developed by Da Veiga and Eloff (2009) created an information security culture assessment tool. They used their proposed model as the basis of the instrument for assessing an information security culture and help organisations to identify the developmental areas. The designed assessment tool included five major components: leadership and governance, security management and organisations, security policies, security program management and user security management. Their model established on the basis of the quantitative method to collect data. They collected data in a South African firm that performs advisory assignments with 3000 employees through questionnaires from their developing the information security culture assessment tool. This work is generally considered to provide the most comprehensive method of assessing information security culture. These studies have contributed positively to the information security culture research particularly with regard to quantitative findings.

In addition to the above-mentioned studies, there are numerous model and assessment tools that may be used to measure the current state of the information security culture in an organisation. For instance, Alnatheer et al. (2012) developed a reliable and valid measurement model that present various factors that comprise and influence the information security culture, that can be measured in order to diagnoses the current state of the organisation’s security culture and employee risk.

Moreover, some security tools such as the World Institute for Nuclear Security (WINS) and Centre for the Protection of National Infrastructure (CPNI) have produced an effective checklist or survey that could be used to measure security culture. First, the World Institute for Nuclear Security (WINS) has developed a security culture checklist assessment that could be used to assign the current level of the information security culture in an organisation. It consists of a number of yes/no questions which help employees to determine whether specific factors are in place or not. The checklist is a simple diagnostic tool that does not usually provide enough information for determining which actions would be important to form the sort of information security culture the organisation required. The World Institute for Nuclear Security also developed a survey, that contains sixteen questions, to evaluate and assess factors that need to be considered, for establishing or improving a healthy security culture (World Institute for Nuclear Security 2011; Walton 2015).

Second, the UK's Centre for the Protection of National Infrastructure (CPNI) developed two versions of a tool called the Security Culture Review and Evaluation tool (SeCuRE). This is a survey and evaluation tool that provide a view of the organisation's performance in relation to its information security culture. These tools could be used to measure the information security culture and security behaviour change in order to help organisations understand their current and target security culture and identify what they need to improve (Walton 2015). Hence, measuring information security culture is an important part in assisting the organisation in cultivating the information security culture. Also, once the information security culture is created and understood, it must be measured and monitored in order to be managed in an effective way.

Although other information security culture researchers had proposed constructs and factors to develop an information security culture framework, they did not develop an assessment instrument to measure the information security culture (Nasir et al. 2019; Sas et al. 2020). Hence, it is clear from the current overview that there is a lack of empirically validated research in this field.

Analysis of methods used to apply and validate proposed model of frameworks indicated that most studies in information security culture have implemented a quantitative approach. There were only a few studies such as Alhogail and Mirza 2015, Alnatheer et al. (2012), Da Veiga and Eloff (2010), Masrek et al. (2017) and Martins and Eloff (2002) that used pragmatic, mixed method approach to address the information security culture measurement instrument.

It is important to understand the influence of the variously identified factors in order to understand the critical mechanisms that positively influence the information security culture (Alnatheer et al. 2012; Martins & Da Veiga 2015). Limited studies have developed and empirically tested theoretical models that apply identified constructs to information security culture (Alnatheer et al. 2012; Martins & Da Veiga 2015; Nasire et al. 2019). Most of the studies discussed above have investigated what factors could influence the information security culture but some of these studies did not provide an empirical analysis with the relationships and the interactions between identified factors such as Helokunnas and Kuusisto (2003), Kuusisto and Ilvonen (2003), Tessem and Skaraas (2005) and OECD (2005). For instance, some studies did not test the model to identify the relationship between identified components. Also, they did not provide the relationship between their measurements constructs by using various validation techniques such as exploratory factor analysis and confirmatory factor analysis. Using these techniques would help in producing a reliable factor structure and validating the developed frameworks or measurement models.

In addition, there is a limited empirical research where a validated and reliable information security culture instrument has been deployed using advanced statistical instruments such as Structural Equation Modelling (SEM) techniques to ensure the nomological validity of the research framework for information security culture (Alnatheer et al. 2012; Martin & Da Veiga 2015). The Structural Equation Modelling (SEM) has been defined as a collection of statistical techniques that allows examination of a set of relationships between the independent variables and dependent variables, either discrete or continuous in both independent and dependent cases (Tabachnick & Fidell 1983). The benefits of using the Structural Equation Modelling (SEM) methodology are that enabled the researchers to test and confirm the identified factors or components that influence information security culture. Also, it provides a comprehensive statistical approach to test hypotheses about relations between latent variables (Hoyle 1995).

Few of research perspectives such as Alnatheer et al. (2012) study that used different validation techniques such as conducting Exploratory Factor Analysis (EFA) as a preliminary analysis using Principal Components Analysis (PCA) as factor extraction to illustrate the relationship between constructs. Confirmatory Factor Analysis (CFA) was conducted to validate information security culture measurement and used SEM to test and ensure the validity of their proposed model. This study was one of the earliest in the security culture area that developed a reliable and valid information security culture model. The results of SEM model confirm five

of the identified factors in the model (security awareness, security ownership, top management, policy enforcement, education and training). However, the study was unable to develop a valid scale for some identified factors, such as ethical conduct policies, policy maintenance, and security compliance.

Also, Masrek et al. (2017) study used just two quantitative validation techniques. First, EFA was conducted using factor extraction Principal Axis Factoring (PAF). Then, CFA was applied to test and validate their developed framework. The study showed that all of the identified dimensions are significant and should be considered to develop the information security culture. Similarly, the study of Martins and Da Veiga (2015) proposed a theoretical information security culture model with the aim of identifying mechanisms that could positively influence the information security culture. They validated the theoretical model by using SEM in order to prove the hypothesis and to produce a sound theoretical information security culture model, which was supported by the empirical study. First, they performed EFA to reduce the dimensionality of data using PAF method. Then, conducted CFA to specify the measurement model using the nine factors identified during the PAF. SEM was performed to test the hypotheses and identify the relationships between main dimensions. The SEM enabled the researchers to test the main dimensions and sub-dimensions influencing information security culture. The results of SEM model confirm the existence of the four main dimensions along with its sub-dimensions (policies, management, awareness and compliance).

### 3.5.1 Summary of Literature Gap

Based on the literature analysis of current research perspectives on information security culture, there is still much to be developed in the field of information security culture concepts and practices. A direction of this research has been identified as a result of the literature review and has guided the formation of the research objectives. The areas worthy of further research are:

- The review of the literature has indicated that the available models and frameworks are lacking a comprehensive view that guides and integrate all important human factors that should be considered in the information security culture. Further research is needed to investigate factors or constructs that shape or have an impact in information security culture creation (Alhogail & Mirza 2014; Karlsson et al. 2015; Nasir et al. 2019). Only one study in the literature that examines factors that constitutes information security

culture (Alnatheer et al. 2012; Karyda 2017; Nasir et al. 2019). There is a clear gap in the existing literature of what constitutes a security culture in terms of identifying factors or components necessary for the creation of information security culture. Most previous studies have identified various elements which should be considered in the creation of information security culture. However, it is essential for the developed information security culture framework to provide and clarify the interaction and influence between identified factors or components (Alnatheer et al. 2012; Nasir et al. 2019).

So far, there has been little discussion about confirming the theoretical model by means of an empirical model (Alnatheer et al. 2012, Martins & Da Veiga 2015; Nasir et al. 2019; Sas et al. 2020). Few studies have developed and an empirically tested theoretical model applying identified constructs to the information security culture that could serve as guidance for organisations to positively influence the information security culture. There is a lack of a theoretical model that substantially combines all important factors that shape or have an impact on the information security culture. Since there is no mutual agreement on factors that have to be considered for cultivating the information security culture, this research aims to fill this gap by providing an understanding of the key factors that either influence or constitute the information security culture inside organisations and clarifying the relationship and interactions between the key factors. Also, since there is a lack of theoretical frameworks that guide and integrate all main factors that should be included in order to have an effective information security culture, this research aims to fill this gap by developing a comprehensive framework of main human factors that could serve as guidance for the organisation to influence the information security culture positively.

- The comprehensive review revealed that there have been relatively few recent studies that developed a measurement model or assessment instruments for information security culture (Karlsson et al. 2015; Nasir et al. 2019; Sas et al. 2020; Van Nunen et al. 2018). There remains a lack of studies on empirical measurement in the information security culture field, and thus a parallel absence of instruments for the information security culture measurement models. However, Da Veiga and Eloff (2010) recommend that the information security culture assessment instrument, which is based on the information security culture framework, must be developed in order to ensure the effectiveness of the approach and ensure content validity. Thus, the information security culture approach is required to both cultivate and assess an information security

culture. Nevertheless, few studies have developed framework that could be used for both cultivating and assessing the information security culture. Based on this, the second aim of this research is to propose a reference framework that could be used by researchers and practitioners, as the basis to cultivate and measure the information security culture in organisations.

- Furthermore, few studies used a mixed method approach to address the information security culture measurement instrument. According to the International Atomic Energy Agency (2017), Van Nunen et al. (2018) and Sas et al. (2020), a mixed method approach is needed and should be used to measure the information security culture in order to have depth details regarding the information security culture in the organisation. Thus, there is a gap of knowledge in terms of adopting a mixed approach in the information security culture studies. Also, very few studies have compiled the statistical analysis in their designed information security culture assessment instrument. Statistical analysis should be conducted in order to confirm the validity and reliability of the study (Alnatheer et al. 2012; Da Veiga & Eloff 2010). There is a lack of studies that validate their proposed frameworks or measurement models that use different validation techniques. For example, EFA in order to produce a reliable construct structure and illustrate the relationship between factors. CFA and SEM in order to test the nomological validity in information security culture field. In order to ease the existing limitation of current literature, this research will use a mixed method (qualitative and quantitative approach) in order to develop a reliable and valid framework. It will also validate the proposed framework by using various validation techniques, such as EFA, CFA and SEM.

## 3.6 Information Security Culture and The Key Factors

Several studies conclude that it is important to understand the underlying factors and components which make up an information security culture contributes towards the successful information security practice in the organisation (Alnatheer et al. 2012; Alhogail & Mirza 2014; Hassan et al. 2015). Many research studies have explored and examined various factors that could positively influence the information security culture and behaviour of employees (Martins & Da Veiga 2015; Schlienger & Teufel 2005; Zakaria 2004). The literature analysis also revealed there is no mutual agreement on what factors have to be considered for the

information security culture to be created and measured in an organisation (Karlsson et al. 2015; Nasir et al. 2019; Walton 2015).

Therefore, it is important to consider human components that could influence the employee behaviour to ultimately aid in cultivating the information security culture. One of this research objectives is to fill this gap, by identifying and providing an understanding of the key factors that either influence or constitute organisational security culture. It aims to clarify the relationship and interactions between the key factors in order to develop a comprehensive framework of relevant human factors. This framework could serve as guidance for an organisation to positively influence the information security culture. A comprehensive review has been conducted, in order to investigate and better understand the main critical factors that influence the successful adoption of the information security culture in an organisation. Fourteen studies were retrieved that presented essential knowledge and identified various factors and components, which should be presented when creating and assessing the information security culture in an organisation. For each study, all the identified factors/constructs were extracted and counted in Table **3.2**. The purpose of counting these constructs is to identify the top critical factors as potential candidates for the conceptualising an information security culture.

**Table 3.2: Summary of Top Candidate Factors in the Information Security Culture Research**

| Construct (Factor) | No. of Times Cited/ 14 | Ranking |
|---|---|---|
| Top Management Support | 9 | 1 |
| Information Security Policy | 9 | 1 |
| Security Awareness | 9 | 1 |
| Security Education and Training | 8 | 1 |
| Security Ownership | 7 | 5 |
| Security Risk Analysis & Assessment | 6 | 6 |
| Security Compliance | 6 | 6 |
| Ethical Conduct | 5 | 7 |

Note: No of Times Cited: Number of Times Cited

The literature review revealed several factors have been explored by many researchers such as Schlienger and Teufel (2005), Da Veiga and Eloff (2010) and Alhogail and Mirza (2014) and reported to have an impact on the information security culture. Most of the previous studies demonstrated that the information security culture is a product of various components or factors that determine the employee's behaviours in an organisation. These studies also found that there are a number of factors, such as top management support, information security policy, security awareness and security education and training, which have a direct effect on individual behaviours in relation to the information security culture. These factors should be considered in order to improve the security of information assets and measure the information security culture within organisations.

Based the literature review analysis, the top important factors that might have impact on the effectiveness of the information security culture are top management support, security policy, security education and training, security awareness, security ownership, security risk assessment and analysis, security compliance and ethical conduct. The following section presents these factors.

### 3.6.1 Top Management Support

Top management support has been identified as a major construct that significantly influences secure compliance. Top management support is an effective component of establishing a conducive environment for successful information security implementation (Knapp et al. 2007; Da Veiga & Eloff 2007). Many of the existing studies demonstrate that executive involvement leads to information security success and effectiveness in organisations. As stated by Fourie (2003) that top management support is one of the most defining factors that affect an organisation's security management. It was shown that support from the level of top management was deemed to be the most important issue from twenty-five potential information security issues (Knapp et al. 2007).

The support by management determines the level of understanding that senior management figures have towards the function of the information security, together with the extent that they are involved in the activities relating to the information security (Ragu-Nathan et al. 2004; Knapp et al. 2007). Top management support often involves the communication and definition of defining security policies, which allocates particular responsibilities to entrusted individuals (Fourie 2003). Moreover, it was stated that top management should make resources available

that help to progress the information control and security, as well as perpetually enabling the review and maintenance to the effectiveness of the information security (Brady 2010).

For instance, when management clearly presents a commitment to the issue and shows quality comprehension of security needs, then the success of the information security is duly increased (British Standards Institute 1999). Nonetheless, when senior management individuals lack this commitment and knowledge, then the organisation can be faced with major issues in operations on a day-to-day basis, as occurs in many organisations that encounter information security management difficulties (Von Solms 1996).

The promotion of an effective program of information security can be helped by executive support. Management support includes more than the management of information security, as it helps to establish and support the overall information security culture. In particular, top management has been shown to be imperative in the establishment of a security culture in the organisation (D'Arcy & Greene 2009; Masrek et al. 2017; Martins & Da Veiga 2015).

The organisational commitment from management, alongside strong leadership, is vital at the initiation of the information security culture, in order for success in the long term (Gaunt 2000; Nasir et al. 2018). The support from top management could help to predict the quality of the information security culture and security policy. The low levels of executive support have been shown to develop a culture within an organisation with worse information security (Knapp et al. 2006). Moreover, it was demonstrated within the same study that user training can be advanced by top management support, whilst also promoting a culture of security awareness, which implements the relevance and continuation of security (Knapp et al. 2004). As a consequence, a failure of top management and inconsistent support within an organisation would result in a badly constructed security culture. Therefore, top management support would have a strong effect on the cultivation of information security culture.

### 3.6.2 Security Policy

The importance of the security policy has been emphasised by many studies, international standards and guidelines. Most researchers concluded that having an effective policy of security helps to influence the understanding of what is deemed responsible and acceptable behaviours, that ensures a safe environment inside the organisation (Da Veiga 2015; Hedström et al. 2013; Knapp et al. 2005). The security policy creates a consensus for the organisation's

vision that combines with added knowledge of how data and information become protected (Dhillon 2006).

The security policy has been defined as a written document which specifies the organisation's strategies and requirements of information security approach and with a connection to the general policies (Fulford & Doherty 2003; Höne & Eloff 2002). The principal objective of security policy is to establish the rights and responsibilities of the users (Blacharski 1998; Ward & Smith 2002). It has also been argued that the security policy of an organisation needs to incorporate responsibilities that are clearly defined, in order to increase success rates. The policies should deal with what can protect the confidentiality, integrity and availability of information as well as different assets of worth that approve corporate objectives and strategy for the security (British Standards Institute 1999).

In addition, a security policy enables the direction for management support in relation to information security (Da Veiga 2015; Thomson & Von Solms 2004). The system for information security management is also enhanced by a security policy's formulation and utilisation (Fulford & Doherty 2003). The organisation will fail to achieve a system of effective information security management without the implementation and continuous development of the security policy (Hong et al. 2003). Therefore, the structure and organisation of a policy must be constructed effectively (Von Solms & Von Solms 2004).

Various empirical investigations have analysed the security policies in large organisations where they have been implemented (Da Veiga 2015; Hong et al. 2006). Some organisations still remain unaware of the importance of security policy establishment. It was noted that security practices will start to be developed with no clearly defined objectives and responsibilities when a policy is not in place. Yet, it could never be guaranteed that the employees will follow these policies (Von Solms & Von Solms 2004).

A security policy is vital for the establishing an information security culture, as well as information security management effectiveness. It is clear that, security awareness needs a foundation of security policies in order for it to succeed (Da Veiga 2015; Hovav & D'Arcy 2012). Security policies are imperative and need to become a set part of the information security program within any organisation. However, the information security culture should be cultivated and comprehended in relation to how it will be integrated with policy (Knapp et al. 2005). Indeed, the aim of information security culture is to provide progress influence towards

employee's behaviour that will comply with the defined official policy of security (Box & Pottas 2013; Masrek et al. 2017; Schlienger & Teufel 2003). Moreover, the culture of information security needs to be integrated into the routines of daily work that will develop a security environment that employees understand and adhere to and be adaptable when organisations create consistent security policy enforcement (Alhogail 2016; Da Veiga 2015). Based on this discussion, the security policy would have an influence on the creation of the information security culture.

### 3.6.3 Security Awareness

Several studies have concluded that levels of awareness are critical within the information security management for the organisation (Furnell et al. 2007; Parsons et al. 2014; Wiley et al. 2020). Security awareness was defined as user understanding of potential information security-related issues and awareness of their security mission, which often leads to the commitment to the ideal (Bulgurcu et al. 2010; Siponen 2000).

Since the techniques and procedures within security can often be badly utilised or misinterpreted by employees, the awareness of security within all specifics of its management is vitally important to embed compliance behaviour in line with the information security requirements in the organisation (Dhillion & Torlzadeh 2006; Parsons et al. 2017; Von Solms 2006). Many statistical analyses from organisations have demonstrated a lack of awareness of information security in organisations. According to the Ernst and Young's 2015 Global Information Security Survey, the necessity to enhance the awareness of security is not adhered to by most organisations. Moreover, awareness by employees has been shown to be the main obstacle towards information security (Johnson 2006; Parsons et al. 2017).

As a result, a large percentage of breaches within information security are undertaken by the actual employees (Magklaras & Furnell 2005; Schlienger & Teufel 2005; Ponemon 2019). Additionally, the greater risks will be incurred when the manager fails to be aware of the user effect upon security (Straub & Welke 1998). At times, this awareness is only directed to the IT department, and thus, fails to include the entirety of the organisation (Mitchell et al. 1999). As consequence, the potential for additional problems could occur as not all the employees are placed on the same awareness (Von Solms & Von Solms 2004). Indeed, the levels of employee awareness in relation to the information security have been found to be low in many organisations, which are enhanced by a failure to address the issue (Von Solms & Von Solms

2004; Wiley et al. 2020). This is why the employees within an organisation have been identified as vital to information security enablement, as incidents of security stem from the particular lack of awareness regarding policies of information procedures and security (Chan & Mubarak 2012; Wiley et al. 2020).

Therefore, it is vital for programs of security awareness to be established as a form of information technology environment control development that ensures a sufficient level of awareness in the organisation (ISO/IEC 27002 2005). This importance can be seen through the adaptations by the international information security standards such as BS7799 and ISO/IEC TR 13335 (ISO/IEC 27002 2005). Security awareness programs need to be developed through the entirety of an organisation, which includes all management and employees, while a requirement of awareness training is imperative in accordance with the specific roles in the organisation (Masrek et al 2017; Parsons et al. 2017). Nonetheless, management is essential in ensuring the policies of security awareness are set up correctly (Kritzinger & Smith 2008).

The importance of security awareness, as highlighted above, is a necessary part of information security protection. It is acknowledged in the literature as a vital part of improving the culture of security. In particular, the 'institutionalisation wave', which is the term given to the third wave of information security, is discussed in study of Von Solms's (2000) 'information security awareness' and in the more recent "information security culture". Prior to this information security culture was described as a security awareness by organisations in advanced stages, which is achieved through the awareness, knowledge and skills of security (Information Security Forum 2000; Tarimo 2006). Moreover, the importance of security awareness for the establishment of security culture has been acknowledged by different researchers, as the culture of security is directly related to its behaviour, while the analysis contributes directly to the culture's development and maintenance (Da Veiga 2015; Hassan & Ismail 2012, Parsons et al. 2017).

All employees need to be security aware. This is essential for effective security, and this awareness has a positive effect on the culture of security (Da Veiga 2015; Wiley et al. 2020). In addition, the security awareness needs to be implemented within new organisations, as the managers will be able to construct a foundation of compliance (Eloff & Eloff 2005). Accordingly, it then becomes natural for individual responsibility to develop in relation to what is deemed acceptable in respect to information security, as employees are able to comprehend the importance of the security culture (Alhogail 2016; Da Veiga & Eloff 2010). Specifically,

breaches of the information security are caused by employees of an organisation, and so it becomes a crucial issue for the organisation (PwC 2018). Often, these employees lack adequate knowledge in the area of information security (Thomson & Von Sloms 1998). Indeed, the behaviour and control of employees can be seen as the greatest failure of operational awareness regarding information security (Van Niekerk & Von Solms 2005; Parsons et al. 2017). Consequently, by improving the understanding of security culture, the awareness of employees will automatically be increased. Security awareness is must become a priority in order to create effective management and control of information security, whilst also improving the culture of security (Alhogail 2016; Da Veiga 2015). Thus, security awareness has a strong impact on the information security culture of organisations.

### 3.6.4 Security Education and Training

Security education and training are considered as the most effective offsets to reduce the human risk posed to the information security (Hovav & D'Arcy 2012; Parsons et al. 2014). The security education and training have been defined as "instructions that provide users with the general knowledge of a certain subject which relate to the information security environment, along with the skills necessary to perform any required security procedures" (D'Arcy & Greene 2009). Recently, there have been a significant volume of published studies, international standards and guidelines that highlighted the importance of security education and training in order to encourage the employee secure practices in the organisations (Hovav & D'Arcy 2012; Parsons et al. 2014).

The education and training for information security culture are vital to the development of awareness. It had been stated that Return On Investment (ROI) through security education and training are the most beneficial enhancement (Schultz 2004). This training has to remain continuous, as there is an evolution of policies (Dojkovski et al. 2006). Security problems are a major issue, and thus, training needs to be provided that will help to advance awareness levels (Straub & Welke 1998). The correct application and levels of training can develop behavioural traits in relation to the security understanding (Information Security Forum 2000; Johnson 2006). It is also believed that employees will remain the most potentially detrimental factor towards an organisation's security if they have not received adequate training (Kraemer et al. 2009; Ponemon 2019; PwC 2018).

Security education and training should become a requirement, as it will improve awareness and develop the levels of information security culture (Alnatheer et al. 2012; Kelly 2006). In order to reduce risks to information assets, organisations must try to develop a culture of the information security through advanced education and training (Da Veiga & Eloff 2010; Hassan and Ismail 2012; OECD 2005). Therefore, it has been determined that effective information security culture is the main foundation for the development of information security management, which becomes impossible without universal organisational security education and training (Nasir et al. 2018; Tarimo 2006).

The information security culture can be assisted in its establishment through the implementation of a variety of techniques based on specific policy and education (Furnell et al. 2001; Lim et al. 2010). The information security culture cannot be improved without the correct training of employees for their roles and responsibilities (Da Veiga 2015; Von Solms & Von Solms 2004). It was also shown that initial awareness development of issues in relation to security is the main cost-effective form of control (Dhillion 1995; Wiley et al. 2020). Therefore, the education and training programs for employees are shown to help define achievable roles within the process and development of security culture (Van Niekerk & Von Solms 2005). The education and training of employees must be centred on the information security culture within an organisation (Da Veiga 2015; Van Niekerk & Von Solms 2005). As a result, it could be determined that in order to ensure an effective information security culture, the awareness, education and organisational leadership must be integrated simultaneously (Martins & Da Veiga 2015; Zakaria 2004). Therefore, the security education and training effect the cultivation of information security culture.

### 3.6.5 Security Ownership

Since employee perceptions, norms, values, beliefs and security knowledge affect willingness to act according to the organisation information security requirements, it is important for employees to understand their roles and responsibilities toward security of information assets inside the organisation (Alhogail & Mirza 2014; Chia et al. 2002; Goh 2003). Employees should view security as an essential aspect when interacting with information assets in the organization (OECD 2005). When employees understand their responsibilities and the importance of protecting the information security, they will be able to act in a supportive manner to prevent, detect and respond to any security incidents. Hence, the employees' security performance will improve, and their security awareness level will increase which will increase

the compliance with the security policy and thus the organisation's securely performance (Connolly et al. 2017; Ramachandran et al. 2008).

It has been stated that when the employees have a sense of ownership and be a responsible for the security practice, the employees will behave in more a secure manner with appreciation to protecting the information assets and thus, lead to the creation of information security culture (Ruighaver et al. 2006; Sas et al. 2020). In addition, a strong correlation was found between the information security culture and employee ownership (Alnatheer et al. 2012). Therefore, the employee ownership is a vital aspect and could influence the cultivation of a culture of information security (Alnatheer et al. 2012; Walton 2015).

### 3.6.6 Security Risk Analysis and Assessment

The risk is often an unavoidable fact, which means that organisations must accept it, and thus, attempt to minimise the potential threat (Turban et al. 1996). The potential sum of threats that could cause harm, vulnerability and asset valuation damage defines the level of risk. When any of these factors are raised, it increases the chance of risk (Smith 1993). Therefore, the risk analysis helps to determine the level of risk in the organisation through the application of security measures against potential threats, the value of resources and vulnerabilities. The risk analysis enables the ability to correspond expenditure incurred through organisational protection against a number of assets. The assessment of risk is also an essential step in defining an organisation's overall information security risk (Da Veiga & Eloff 2007). The risk assessment has been defined as when "countermeasures are adequate to reduce the probability of loss or the impact of loss to an acceptable level" (Caelli et al. 1989).

Due to the increase in the information security breaches and the security requirements of business partners, the pressure to implement risk management has increased (ISO/IEC 27002 2005). For instance, organisations in developed countries are pressured to implement methods of risk management by both their governments and national industry (Institute of Chartered Accountants in England and Wales 1999; Sarbanes-Oxley Act 2002). Nonetheless, the level to which the security organisations maintain safety within their systems is almost impossible to determine. In many instances, more additional questions are raised by the risk analysis studies, instead of answering them (Kwok & Longley 1999).

However, there are numerous studies and international standards that indicated that the risk analysis should always be seen to offer future benefits, as it increases knowledge and

comprehension in regard to how security failure induces loss (Gerber et al. 2001). Organisations have been helped in managing their security exposure through using the information security risk management methods such as Methodology for Model-Based Risk Assessment (CORAS), Central Computer and Telecommunication Agency Risk Analysis and Management Method (CRAMM), Threat, Asset, Vulnerability and Evaluation (OCTAVE). Each of these methods has a specific approach in the process of providing identification, measurement, control and analysis to the risks involved with the information security (Bornman & Labuschagne 2004). The information security risk methodology must correspond to what is recognised as the best practice internationally, and adapted correctly to a particular environment, recognising privacy regulations by governments (King Committee on Corporate Governance 2002).

The organisation and its employees need to become capable of understanding potential damage to security, which helps to create awareness in a security culture that is achieved by implementing analysis and assessment of security risk. The security risk influences overall understanding and potential acceptance of beliefs in security that subsequently influence the culture of information security (Alnatheer et al. 2012; Martins & Eloff 2002; Nasir et al. 2018). Consequently, security risk analysis and assessment could assist an organisation to develop loss and damage awareness, as the increased security knowledge and reduction of misbehaviour by employees improve practices of information security. Hence, the security risk analysis and assessment will have an impact on the information security culture of organisations.

### 3.6.7 Security Compliance

Human behaviour has caused the most security incidents (Beautement et al. 2008; Schneier 2000). An insider data breach survey by the Egress (2020) stated that 78% of employees put organisation' data at risk accidentally, through ignorance or negligence in relation to the policies of security in an organisation. Organisation employees are often unaware of the consequences to security caused by their actions and fail to comprehend how their decisions affect security (Khan et al. 2011; Zurko et al. 2002). However, this could be rectified when senior management attempts to influence the behaviour of employees with security policy compliance, which consequently protects information assets of an organisation (Von Solms & Von Solms 2004). The security compliance refers to ensuring that organisations and its

employees follow the regulations, international and national laws that related to the protection of information (Da Veiga & Eloff 2008).

Accordingly, various organisations have tried to redefine security behaviour exercised by employees in order to comply with security policies, as effective information security management and security culture is reliant on employees complying with security policies (Beautement et al. 2008). This was shown to be challenging, specifically the costs anticipated, as well as the negative effects counteracted against the benefits (Beautement et al. 2008). Separately, the information security compliance has failed in its establishment within operations of IT security (Von Solms 2005).

A method is required in order to ensure that employees' compliant behaviour continues to be monitored and measured in relation to the compliance program's effectiveness (Vroom & Von Solms 2004). It has also been argued that security compliance quality may be potentially augmented through the application of additional programs of security awareness, as well as involvement by management that will increase awareness and levels of education, together with security issue understanding (Lane & May 2006). This increase in awareness from training programs will increase the comprehension of potential risks (Denning 1999); which will redefine the applicability to specific laws and regulations (Luthy & Forcht 2006).

Policy compliance is also influenced by continual monitoring and enforcement behaviour (Weirich & Sasse 2001). It has been suggested that a user's behaviour can be influenced by adapting the information security culture, which advances decision making in security through compliance with policies (Brady 2010; Von Solms & Von Solms 2004). It was also noted that an organisation's security will be increased through security policy compliance (Eloff & Eloff 2005). Additionally, a strong correlation was found between the culture of information security, compliance, and the behavioural role of employees (D'Arcy & Greene 2009). As a result, it could be seen that security policy compliance is imperative towards establishing an organisation's security culture and improving its entire security level, which is vital as the security culture influences employees' behaviour in relation to official security policy compliance (Alnatheer et al. 2012; Da Veiga & Eloff 2010; Masrek et al. 2017).

### 3.6.8 Ethical conduct

Organisational security is debilitated by its weakest or most vulnerable section, which is often the employees. This can place the organisation at risk and there is a need to apply the correct

management and monitoring (Mears & Von Solms 2004). In order to control the employees' behaviour and create the establishment of 'moral' codes, the policies of ethical conduct can be used (Hinde 2002). The rules that help to distinguish what is right are often used as the definition of ethics (Hellriegal et al. 1998). The ethical codes could "facilitate responsible security awareness, as users are held personally responsible for ensuring sound security practices are implemented, reducing the security risks" (Mears & Von Solms, 2004). Subsequently, employees adhere to security policies, as the information security behaviour is instilled in a progressive manner that protects assets of information as determined by the security policies and ethical codes of the organisation (Hinde 2002). Hence, in the process of addressing security problems, the security ethics are vital.

Ethical codes are required to define the actions that are deemed to be ethical (Mears & Von Solms 2004). From this, the employees will help to integrate ethical behaviour that relates to the security of information into their common working day (Martins & Eloff 2002). It is the responsibility of the board and managers to develop and implement policies of ethical conduct (Baggett 2003). However, specific examples of unethical conduct have been defined as the installation of organisational software in the home place or Internet usage for private purposes while at work (Da Veiga & Eloff 2010). These examples need to be strongly shown to be unacceptable and as an unethical practice, as an organisation must address the ethical conduct in order to minimise invasion of privacy risks, threats to customer information and potential to altered private data.

Despite prior evidence, the majority of current models for security have not focused or analysed ethical conduct, as well as different academic and researcher approaches, even though the ethical conduct has been signified as important (Alnatheer et al. 2012; Flowerday & Von Solms 2006; Martins & Eloff 2002). Furthermore, the corporate codes of ethical conduct are presented by both the management and the board develops in an organisation as one of the central foundations of information security culture (Martins & Eloff 2002; OECD 2005). Yet, these standards of ethics and policies often alter between different countries (Dojkovski et al. 2007). It was shown by Helokunnas and Kuusisto (2003) and Alnatheer et al. (2012), that previous research on the ethical code of organisations has remained unexplored. It was also shown that individual values and cultures differ between nations and organisations while still sharing important knowledge, which may increase the culture of information security. Therefore, this

needs to be investigated and analysed to enhance the policies of ethical conduct for the advancement of information security culture.

## 3.7 The Interaction between the Key Factors Relating to The Information Security Culture

It is evident that there are many factors found to be the most critical success elements of the information security culture. Important factors have been identified concerning the information security culture. Addressing these factors could help to instill an adequate level of information security culture. Most researchers such as Alnatheer et al. (2012), Da Veiga and Eloff (2010) and Alhogail (2016) stress that these factors have to be considered when creating or assessing the information security culture. Some of the mentioned above factors have been proven to have a positive impact on the information security culture such as the top management support, security policy, security awareness, security compliance and security education and training (Alnatheer et al. 2012; Masrek et al. 2017; Martins & Da Veiga 2015; Nasir et al. 2019). For instance, the top management support has been identified as the most frequently hypothesised variable (Knapp et al. 2006). The commitment and involvement of top management support in security are considered as one of the most contributing to information security culture implementation success (Alnatheer et al. 2012; Da Veiga & Eloff 2010; Sas et al. 2020). The top management support is a major factor that can influence other factors to bring about an effective information security program. The managerial leadership and support of practices can enforce and communicate the security policy, promote employee training by developing and maintaining processes that sustain a trained workforce and advance a security-minded culture that could have significant positive effects on the overall security effectiveness of organisations.

Security policy is able to enforce changes in the attitudes and behaviours of employees through security education and training and security awareness that encourages security compliance (Masrek et al. 2017; Walton 2015). For example, the clean desk policy is a generally employed security roles in the organisation. This type of policy illustrates some information that cannot be left on the display and the employees should clean their desks at the end of their working day. Security education and training are inclined to increase the employee security awareness by communicating the security policy, requirements and achievable roles and educate

employees on how to protect vital organisational assets in order to influence the employee behaviour, encourage compliant behaviour and thus create the information security culture.

Additionally, some of the studies such as Alnatheer et al. (2012) and Connolly et al. (2017) stated that security awareness is the outcome of security policy and security education and training that tends to promote the security compliance behaviour. Security awareness can improve employees' behaviour directly by influencing them to contribute a compliant behaviour that promotes the information security culture. For example, when the employee is aware of security policy, the compliance with the security policy is achieved and thus the information security culture will be created (Schlienger & Teufel 2003; Wiley et al. 2020). As consequence, it could be seen the presence of these factors positively affects the cultivation of information security culture.

Nevertheless, there are other factors such as ethical conduct, security ownership, security risk analysis has been not proven its impact on the information security culture. These three factors have been signified its importance and benefits in establishing the information security culture in the organisation (Alnatheer et al. 2012; Martins & Eloff 2002). These factors tend to lead to compliant behaviour. For example, the security risk analysis and assessment could help the organisation on understanding the risks and the potential damage to the security, reducing misbehaviour by continually reviewing, updating and improving the security policy based on the risk reduction. Also, it will support the employee by increasing their knowledge regarding the security failures, as it increases their awareness which in turn has a tendency to encourage the compliance behaviour and cultivate the information security culture (Nasir et al. 2018; Walton 2015).

The ethical conduct factor could assist employees in understanding and be aware of their responsibilities, how to integrate ethical behaviour and adhering the security policy in order to reduce any risk associated with their behaviour. Thus, the awareness of employee will increase and will have a sense of security ownership and then promote compliance behaviour that leading to the creation of information security culture. The security ownership could enhance the organisation performance by assisting employees in understanding their responsibilities, their security roles and the importance of protecting the information assets. This will increase the employee awareness levels that will increase the compliance with security policy and have a sense of ownership. Consequently, the employee behaviour will change with respect to protecting the information assets of the organisation, which in turn lead to cultivating the

information security culture. However, these factors have been received a little attention and very few studies such as Alnatheer et al. (2012), Helokunnas and Kuusisto (2003) and Nasir et al. (2018) have tried to prove and validate the impact of these factors on the information security culture. Therefore, more research is needed to examine and analyse these factors in order to clarify and prove the influence of these factors on the information security culture.

However, it is important to understand the influence of the variously identified factors in order to understand the critical mechanisms that influence the information security culture positively (Karyda 2017; Sas et al. 2020). Based on the analysis of the literature review, the previous factors have interactions and relationships between each other that lead to creating the information security culture. Unfortunately, most of the previous studies have investigated what factors could affect information security culture but some of these studies did not provide an empirical analysis with the relationships and the interactions between identified factors. For example, some studies did not test their model to identify the relationship between identified components. Also, they did not provide the relationship between their measurements constructs by using different validation techniques to produce a reliable factor structure and indicate the relationship between factors. The relationships and the interactions between constructs of information security culture have not been investigated from an empirical standpoint. There is still a limited study have developed and empirically tested theoretical models that apply their identified constructs to the information security culture (Martins & Da Veiga 2015; Nasir et al. 2019; Sas et al. 2020). Therefore, this research will take this initiative and develop an information security culture framework that clearly determines the relationships between the factors and will be tested statistically.

Alnatheer et al. (2012) stated the importance to distinguish between the factors constitutes the information security culture and factors affect the information security culture in order to assist the organisation in directing the interaction of humans with information security. Yet, there is little clarification as to what exact factors constitute the information security culture and as to what factors affect the cultivation of information security culture (Karyda 2017; Nasir et al. 2019). Thus, there is a clear gap in the existing literature of what constitutes a security culture in terms of identifying factors or components that are necessary for the cultivation of an information security culture. Therefore, this research will propose an information security culture framework that distinguishes between what factors constitute the information security culture and what factors influence the information security culture.

## 3.8 The Other Influencing Important Security Factors

There are other influencing security factors that relate to the organisational behaviour that received little attention from researchers in the information security culture domain. The literature provides a rich source of knowledge on factors that motivate the employee behaviour toward the information security. However, several studies have found that there are other security factors that have a direct effect on individual behaviour and these factors could help to improve the security of information assets of organisations. These studies have proved the positive impact of these factors and its contribution to a variety of workplace behaviour including adhere to organisations policies and regulations (D'Arcy & Greene 2014).

An example of an efficient factor that most widely investigated and examined in the organisational behaviour literature is job satisfaction (D'Arcy & Greene 2014; Judge et al. 2001). The construct of job satisfaction is rather broad, as it encompasses the feelings of employees in relation to various intrinsic and extrinsic job elements. The job satisfaction refers to a positive or pleasant emotional condition that is derived from the employee's appreciation for his occupation or work experience (Locke 1976). In general, job satisfaction refers to the overall sentiment of 'well-being' in the workplace (Ang et al. 2003). Employees who report positive feelings are more likely to work well with the policies of their organisation, as their improved engagement allows them to interact directly with their individual and collective responsibilities (Farokhi et al. 2016). This could help to determine how the employee may adapt to situational factors, such as remaining committed and not opting for easier options, which could prove detrimental to the organisation (Greene & D'Arcy 2010).

A variety of empirical studies has examined the job satisfaction variable and its impact on user's information security policy compliance decisions. It is evident that a correlation exists between employee compliance behaviour and job satisfaction, and that job satisfaction acts positively upon security policy compliance. For instance, the influence of job satisfaction upon security policy compliance by users was researched through the hypothesis that satisfaction positively affects compliance (Greene & D'Arcy 2010). Greene and D'Arcy (2010) model was tested and validated on 223 participants. The results suggested that security compliance is affected by job satisfaction, whilst a strong relationship was noted to exist between job satisfaction and the intentions of users in compliance. There is an evidence that there is a strong correlation between the information security culture, security compliance and the behavioural role of employees and that higher job satisfaction could motivate employees to comply with

security requirements (D'Arcy & Greene 2009). This research postulates that there is a potential link between job satisfaction and the information security culture.

Another factor that has been investigated and considered in several studies such as Gabriel and Furnell (2011) and McCormac et al. (2017) studies is the individual difference variables such as personality traits. Gabriel and Furnell (2011), explored the relation between personality characteristics and good security behaviours. They concluded that personality test results might possess a predictive value for security behaviour in the organisation. Another study performed by McCormac et al. (2017) investigated and empirically evaluated the nature of the relationship between the personality traits and individuals' security awareness. Their main contribution has been the consideration of individual differences, including personality, in relation to the security awareness. These findings could benefit the organisations to identify areas that require improvement or to facilitate the development of training programs.

There are five specific personality traits commonly used within psychology to describe, understand the human personality and predict numerous factors in diverse and complex environments (Shropshire et al. 2006). The Five-Factor Model (FFM) of personality usually referred to as *The Big Five* is considered the leading theoretical model for understanding and measuring personality (Shropshire et al. 2006). The five factors are: openness, agreeableness, extraversion, conscientiousness and neuroticism (Costa & McCrae 1992; John & Srivastava 1999). The dynamics and extent of the relationship between these personality traits were analysed by Shropshire et al. (2006) through 120 respondents, as well as user behaviour upon information security compliance. Their model was based on the five specific personality traits, and as a result, conscientiousness and agreeableness were shown to have the highest impact on information policy towards user compliance. Likewise, Mcbride et al. (2012) undertook a study with 481 participants to develop levels of comprehension into individual personality traits that hold behavioural patterns and can have an impact on the intentions of users to comply with the policies of information security. Mcbride et al. (2012) empirically validated a theoretical model that attempted to assess personality factors and their potential factors and effects. The results indicated that compliance with security policy was more likely with participants who are more open, conscientious and agreeable, as violations of security policy were generally committed by the extrovert and neurotic.

Shropshire et al. (2015), investigated self-reported intentions and personality to adopt a web-based security software program. The results suggest that potential to use security software was

related with high levels of agreeableness (Shropshire et al. 2015). Participants who obtained high agreeableness are often worried in relation to the opinion of others, and subsequently become more concerned with security issues (Korzaan & Boswell 2008; Shropshire et al. 2015). In addition, certain traits were positively associated with conscientiousness and agreeableness, such as 'rule following', even though they would not have known that their behaviour was being monitored (Organ & Paine 1999). A separate study Pattinson et al. (2015) detailed and evaluated the computer-based behaviour of a non-malicious nature, together with individual factors that included the individual's age, connection with computers and their level of education. From this research, it was found that accidental-naïve behaviour of employees is potentially at lower risk when their personalities are defined as conscientious, agreeable, not very impulsive, and with less experience working with computers.

The study of McCormac et al. (2017) investigated and examined the relationship between individual differences, which include personality test and the security awareness. The research sample was 505 participants. The authors found that conscientiousness, agreeableness and emotional stability significantly explained variance in individuals' security awareness. This study suggested the need for future research to examine individual differences and their impact on the information security culture. Based on the previous studies such as Alnatheer et al. (2012) and Martins and Da Veiga (2015) concluded that there is a strong correlation between the information security culture and the security awareness and on the study of McCormac et al. (2017) revealed and considered the impact of personality on the security awareness. Hence, this research predicts that there is a potential link between the personality traits and the information security culture.

Based on the previous discussion and on the literature review analysis, these two factors have not been examined and considered in most previous adoption frameworks and models that relate to the information security culture. Thus, there is still limited coverage of other influencing security factors. As a result, this research will also investigate these two factors that could have impact on the information security culture.

## 3.9 Conclusion

This chapter has presented an overview of literature relevant to the field of information security culture. The discussion highlighted the importance of information security culture and discussed its conceptualisation and practices. This chapter also addressed the issue of

formulating an understanding of the concept of information security culture and provided a summary of the current literature to assist the researcher identifying the gap in knowledge that this research is aims to fill.

A considerable amount of literature has been published in the information security culture field. These studies have been conducted different aspects of the studies. In general, the concept of information security culture and its importance has been explored. The literature review demonstrated that most of studies applied existing social or organisational theories to develop a framework or model that guide their investigation and had been accepted by the research community. Furthermore, a comprehensive review of existing literature demonstrated that there are various important factors, have an impact on the information security culture, which should be considered in order to have an effective information security culture in organisations.

Therefore, fourteen research perspectives that focus on terms of identifying factors which aid in establishing the information security culture were presented. The available studies were evaluated in terms of assessing the information security culture. Most of these studies provide a comprehensive security culture model and contribute a good understanding of how to create and assess an acceptable level of information security culture in the organisation. Fourteen of the research perspectives relate to the cultivation a security culture and five of them incorporate the assessment of information security culture.

However, far too little attention has been paid to specify factors that shape the information security culture. Only one study in the literature that specifies factors constitutes the information security culture. Yet very few studies have used the same framework to create and assess the information security culture in an organisation. Two of research perspectives provide an approach that uses the same framework for cultivating and assessing the information security culture. Also, there is only three research perspective that validates the conceptual measurement model using different validation techniques such as Exploratory Factor Analysis (EFA), Confirmatory Factor Analysis (CFA) and the Structural Equation Modelling (SEM) in information security culture field.

Therefore, it appears from all above that there is a need for more investigation in the field to provide comprehensive frameworks and best practices of the establishment of information security culture in an organisation. In particular, a number of the studies that investigate the factors that shape or effect on the information security culture are limited. There are calls in

the literature to extend these areas of research. Moreover, it is clear that there is a gap in knowledge regarding how to develop a comprehensive model of constructs that most influence the effectiveness of information security culture in organisations.

This chapter also has investigated and discussed the main critical success factors that positively assist the cultivation of information security culture in an organisation. The literature review demonstrated the most important factors, which have a direct influence on individual behaviours in relation to the information security culture, where there is an agreement among the published studies. Therefore, the important factors that are necessary for information security culture existence are top management support, security policy, security education and training programs, security awareness, security ownership, security risk assessment and analysis, security compliance, ethical conduct, personality traits and job satisfaction. These factors should be considered in order to improve the security of information assets and measure the information security culture in organisations.

Since it is essential for the developed security culture framework to provide and clarify the interaction between identified factors or components, the number of studies that provide the empirical analysis with the relationships and the interactions between identified factors are limited. There is a need in the literature to extend these areas. There is a gap in knowledge regarding how to develop a model of factors that strongly influence the effectiveness of information security culture in organisations. Therefore, the current research proposes a comprehensive framework that integrates all important factors and presented later in Chapter 5 after specifies the research methodology in Chapter 4.

# Chapter Four :

# Research Methodology

## 4.1 Introduction

This chapter shows the research methodology that was applied in the current research. It also presents the data collection strategies and data analysis procedures of collected data that used in this research. The choice of a methodological approach and the subsequent methods for data collection is an important part for the research process. The chapter commences by providing a description of the research philosophy and general research approach that were have been selected for the current research. Following this, there is a description of the research strategy and design; mixed methods to combine both interviews and questionnaires, which are detailed in order to justify the research method selection.

In addition, the main used data collection strategies are documented, which included a literature review, interview and questionnaire. As a mixed method is used, both a qualitative and quantitative phase will be applied in the data collection strategies, together with an explanation and brief discussion of its development and how it is administrative. The chapter also provides relevant data analysis for the two methods, as well as the different statistical techniques used in the research. Finally, issues of reliability, validity and ethics are outlined. A conclusion presented at the end.

## 4.2 Methodology

The research methodology details the theoretical perspective that will be adhered to throughout the completion of the work, in order to answer the research objectives, which will help to determine the factors that influence appropriate methodology applications; and to detail the form of approach. The study follows specific methods and approaches based on the nature of this research. Figure 4.1 shows a generic research onion process which was developed by Saunders et al. (2003). This research followed this process in order to formulate an effective methodology.

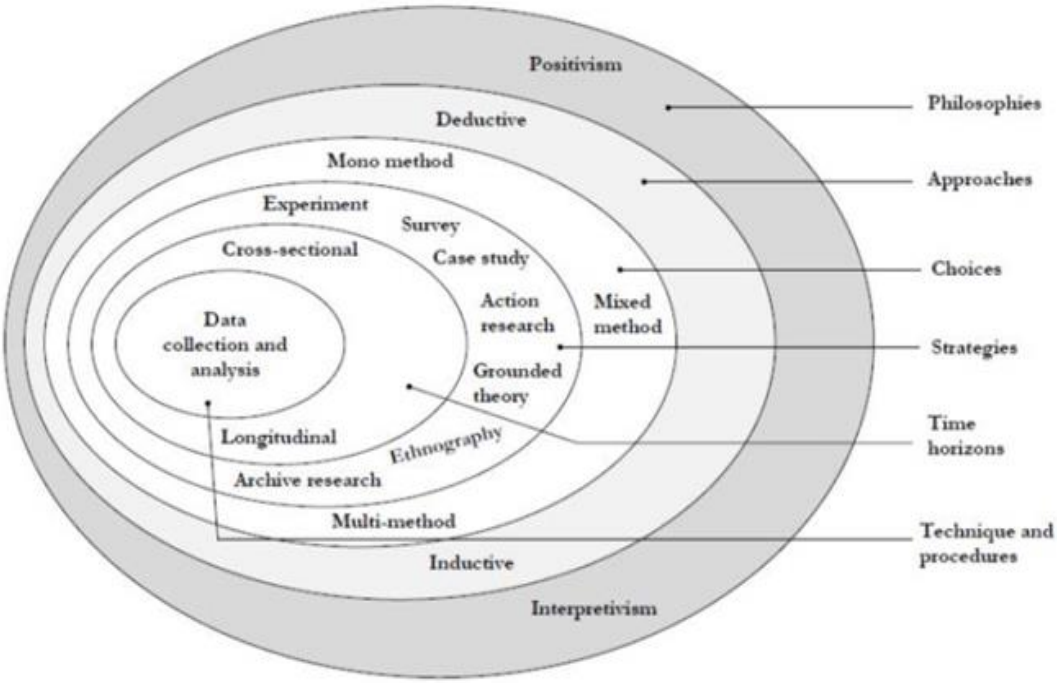



**Figure 4.1: Generic Research Onion Process (Saunders et al. 2003)**

A generic research onion process demonstrated what needs to be included in the development of a research strategy, as well as providing an effective progression for the design of a research methodology. The research onion's use is adaptable to different methodologies and contexts (Bryman 2012). This process includes various stages: initially, the research philosophies that require the definition that create the base to the second stage, research approach; thirdly, choices, where the strategy is adopted; fourthly, strategies; fifthly, time horizons; sixthly, where data collection methodology is shown. Overall, the research onion presents benefits that help to create different stages where varied data collection methods can be interpreted and comprehended while illustrating potential descriptions of a methodological study (Saunders et al. 2003).

### 4.2.1 Research Philosophy

The set of beliefs that concern the nature of the reality under investigation relates to the research philosophy (Bryman 2012). This is the central definition of knowledge and its nature, while the research philosophy and its assumptions stipulate the manner that the research will undertake (Flick 2011). Research philosophies often contrast between objectives and in relation to their form of applicability (Goddard & Melville 2004). Hence, the comprehension of utilised research philosophy creates the possibility to state the assumptions relating to the research

process, as well as how this relates to the methodology. Nevertheless, science philosophers have specifically analysed two fundamental issues, which are concerned with the nature of reality (ontology); and the construct of human knowledge (epistemology). The assumptions about knowledge and how a person develops it relates to epistemology, which shows how knowledge is possible and obtainable (Feast & Melles 2010). The research knowledge may be classified through three main epistemologies, which are: positivist, interpretive and critical (Oates 2005). Most research studies that have been conducted in natural science rely on these paradigms (Oates 2005). This form of classification method is commonly accepted in current information systems research, as the individual methods characterise a variety of forms that help to perceive social reality through a series of measurements, observations and understanding.

A greater level of comprehension into contextual phenomena is sought by the interpretive approach, which can potentially inform in relation to other contexts (Klein & Myers 1999). This approach demands that social scientists acquire data that helps to explain human behaviour in an objective manner, as well as the subjective meaning for individual people. Interpretive methods aim, through the study of information systems' research, to produce an understanding of different phenomena, as well as influential factors towards the context (Walsham 2002).

On the other hand, the positivist approach centres around epistemological perceptions that create different reality assumptions in an objective manner, which is capable of determining measurable elements that are not researcher dependent or reliant upon their selected application methods (Myers & Avison 2002). When formal propositions are present, quantifiable measures of variables are evident together with hypothesis testing, and inference regarding a particular sample phenomenon related to a stated population, then information systems research may be classified as positivist (Myers 1997). Moreover, subjectivism in critical research refers to the assumption that reality is based historically, and the comprehension of human behaviour is achievable by developing the understanding of different performers (Crotty 1998). Approaches to critique different processes are associated with participants, as well as active research that defines clear objectives in order to present critical approaches and potentially implement changes (Feast & Melles 2010).

In relation to information security research, the positivist and interpretive research paradigms have been defined (Dhillon & Backhouse 2001). Although during the 1990s, approximately

97% of security research was shown to stem from purely positivist epistemology (Dhillon & Backhouse 2001). Since the current research is concerned with the information security culture, it has been determined that the positivist paradigm is the best suited for this research as it is the most popular research philosophy in the information systems field. Although as a second approach the interpretive paradigm will be used in this research in order to obtain more in-depth information, together with enhanced the information security culture comprehension and understanding of influential processes.

### 4.2.2 Research Approach

There are two particular methodological approaches are present in the research: deductive and inductive. In order to analyse a theory and subsequently test an evaluated hypothesis from a designed research strategy, the deductive approach is used (Saunders et al. 2003). This is best applied to research project contexts in relation to examinations of observed phenomena and whether previous research expectations still correlate (Wiles et al. 2011). Additionally, this approach may be particularly relevant to the positivist approach, which helps to hypothesise levels of probability by testing statistical results (Snieder & Larner 2009). Nonetheless, the deductive approach can be used with qualitative techniques, although the expectations that are formed by previous research often contrast to the presently tested forms (Saunders et al. 2003).

On the other hand, when a researcher collects data and develops a theory following data analysis inductive research is used (Saunders et al. 2003). Generally, inductive research is used in qualitative research, while the absence of any theory to determine the process of research can potentially be of benefit by decreasing potential research bias in the stage of data collection (Bryman & Bell 2011). Indeed, this approach may also be used within positivist methodologies in an effective manner, where data is analysed initially to show patterns of significance, which helps to determine varied results.

In particular, one of the major differences between the two approaches deductive and inductive stems from previous theories and literature that help to guide present research, as the deductive approach can test theories, and thus accurately identify questions and/or interrelationships prior to the collection of data (Creswell 2002). Since the information security culture field still requires more theories for explaining and predicting real practices (Alantheer et al. 2012; Nasir et al. 2018), in this research it is vital to conduct an inductive approach in order to understand and interpret the research context.

### 4.2.3 Research Strategy and Design

The research strategy and design help the researcher to strategically create the process of undertaking research, which is vital as it develops the foundation for establishing the research objectives (Saunders et al. 2003). It formulates the possibility to answer the researcher's questions by providing logical data links (Cavana et al. 2001). The selection of research strategy needs to relate appropriately to the studied subject and be directed by the research aim and the nature of the topic. A choice of two common research strategies is prevalent within social research that helps to differentiate techniques of data collection and procedures of data analysis: qualitative and quantitative (Saunders et al. 2003). Within this process, various data collection methods are present, such as active research, case studies, experiments, interviews or surveys. The research strategies include a variety of forms to conduct social research, and thus, different research questions may require a specific distinct form of strategy (McDaniel 2004).

Quantitative research methods are shown to commonly gather and analyse data that may be based numerically or objectively, which use charts, graphs or tables to detail findings. Statistical methods may also be used in data analysis. The quantitative research is valuable in the process of providing behavioural quantification, together with qualitative analysis regarding opinions and beliefs from individuals that help to determine population perceptions regarding the different phenomenon. This is useful in hypothesis and theory testing procedures (Bryman 2015). Quantitative methods require large sample bases, as this ensures that populations can be more accurately generalised, in order to create comparisons and replication (Black 1999).

Comparatively, qualitative research helps to gather and analyse non-numerical data, which aims to strengthen subjective evaluation, in particular during the process of analysis (Lancaster 2007). This aims to create a greater level of comprehension and perceptions from both individuals and groups in regard to their experiences that can be effectual upon behaviours within certain contexts (Elsheikh 2012). Qualitative research is generally used to examine social phenomena and meaning, instead of attempting to understand correlations between established variables (Feilzer 2010).

In addition, using mixed methods of qualitative and quantitative that can be more valuable in measuring phenomena. Many studies support the use of a mixed method approach in analysing

information systems field (Alvesson & Berg 1992; Gable 1994). This generally includes a procedure of collection, analysis through the use of mixed methods within a single study in order to comprehend and determine a specific research problem (Creswell 2002). In the field of information security, it is imperative that a balance between rigour and relevance is achieved, which a mixed methods approach helps to develop. It has been also suggested that the mixed method creates a connection of support between the two approaches to benefit a single study (Lee 1989).

Due to the limitation of using a mixed method strategy in the information system literature as have concluded in several literature reviews that provided an overview of existing research focusing on the information security culture such as Alhogail and Mirza (2014), Hassan et al. (2015), Karlsson (2014) and Sas et al. (2020) studies. For instance, the study of Hassan et al. (2015) had found that majority of studies (50%) have performed quantitative methods and (5%) of these studies employed mixed methods. Van Nunen et al. (2018) and Sas et al. (2020) studies indicated the lack of using mixed methods in the information security culture field and the need to be used in order to get a detailed picture of the information security culture and to explore employee perceptions toward security issues.

As a result, this research uses more than one research strategies. This is appropriate to use in order to achieve the research aims and develop a reliable and valid information security culture framework. This research adopted mixed methods using semi-structured interviews in order to gather a detailed understanding of human behaviour and its effect, to identify the factors of interest that either constitute or influence the information security culture, and to identify which factors are viewed more important than others in the organisation. Also, this research used an exploratory survey in order to develop an initial understanding of the relationship between factors that influence the information security culture and factors that constitute the information security culture and to test the validity of the proposed framework.

## 4.3 Time Horizon: Cross-sectional

A cross-sectional (one-shot study) research was shown by Sekaran (2016) to be a form of research that requires the collection of data and can potentially last for the duration of weeks or months. Sekaran (2016) stated that longitudinal research is conducted at multiple moments, in order to determine the certain variable changes. In this research, a cross-sectional design has been selected, as it aims to explore the various factors that affect or comprise the information

security culture that uses multivariate analysis techniques. Similarly, Hair et al. (2006) suggested that a minimum sample of two hundred is always required if research requires the best results from multivariate studies that use techniques of structural equation modelling. Therefore, a cross-sectional study has been able to facilitate the application of a large sample within a minimal time period, which has meant that the researcher has not had to wait a substantial amount of time to examine the dependent variable changes (Bordens & Abbott 2007).

## 4.4 Data Collection Strategies

The process of data collection and analysis depends upon which methodological approach is used in the research (Bryman 2012). A multiple methodological approach can often be adopted in data collection, which involves both quantitative and qualitative data to help in supporting the outcomes. For instance, in the qualitative approach, there are interviews (semi-structured and unstructured); focus groups; direct observational methods; and document analysis that are used, whilst quantitative approaches may use structured interviews and survey.

Data could be collected by using secondary or primary sources. Both secondary and primary forms have been used extensively in research (both social and business). In the current research, the primary data adopted which has been recommended as the most beneficial strategy (Malhotra & Birks 2006). This collection of primary data can be achieved by implementing interviews and questionnaires (Saunders et al. 2003).

This research also used the mixed approach in order to identify and explore the present culture of information security in service and to determine the principal challenges in the promotion and enhancement of this culture. In particular, there were three phases of data collection in this study which are: a synthesized literature review and integrated mixed methods qualitative and quantitative approaches were used. The qualitative aspect was designed to develop the study framework. The quantitative approach was designed to test and validate the framework. The methods of data collections which that applied are presented in Figure 4.2 and Table 4.1.

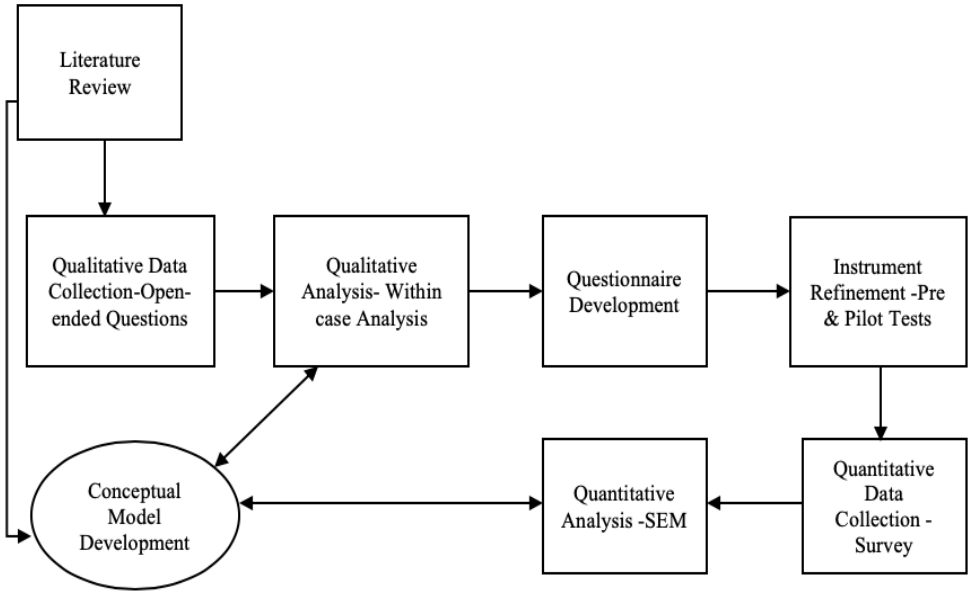



**Figure 4.2: Three Phases of Data Collection Process**

**Table 4.1: A Summary of Research Design and Process**

| Stage | Objectives | Data Collections method | Analysis method | Sample |
|---|---|---|---|---|
| Stage 1 | -Present a summary of current studies that examined various factors which could influence the information security culture.<br><br>-Identify the main factors that have a direct positive influence on the information security culture and factors that constitute the information security culture.<br><br>-Understand the relevance of these identified factors and their relationship with each other. | Literature review | - | - |
| Stage 2 | -Develop the framework that integrates all important human factors that should be considered when create or measuring the information security culture.<br><br>-Design the survey to gather quantitative data.<br><br>- Developed research hypotheses. | Semi-structured interview | A within case analysis | 13 IT and security experts' participants |

| | | | | |
|---|---|---|---|---|
| Stage 3 | - Provide a descriptive view of the practice, perceptions of organisation's members<br><br>- Validate the developed framework.<br><br>-Test the research hypotheses. | Survey | SEM | 266 participants |

### 4.4.1 Literature Review

A review of previous research, studies and documents was one of the principal tasks in the process of the current research. It provides a greater comprehension of the factors of information security cultural and its issues. This progressed to identify the stipulated knowledge gaps in the research and a conceptual framework to address certain deficiencies. Also, the information generated from the literature review was used to design the qualitative interview of this current research. This stage was presented in Chapter 3.

### 4.4.2 Interview Method

The interviewing is a means of data collection used in the process of qualitative research and help to explore individual perspectives, beliefs, motivational views and experiences. According to Mann (2011), the qualitative interview is a suitable data gathering technique to explore participant's experiences, beliefs or identities. This provides the researcher with a means to understand how respondents relate to different issues and actions they are involved with. Interviews provide the advantage of acquiring information that can develop conceptual understanding of various issues that had previously not been analysed or considered (Gay et al. 2009).

The interview provides a deeper understanding and detailed information when detailed insights are required from individual participants than what is available through other data collection methods such as survey (Seidman et al. 2012). The interviews provide a greater level of methodological control in relation to the forms of acquired data, in comparison to observations, as specifically designed questions are implemented. The interviews offer the researcher an opportunity to follow up ideas and clarify issues which might not be appropriately offered by survey. As stated by Creswell (2002), an interview creates the opportunity to gain more clarity through additional questions following unclear answers.

This research relied on prior literature to identify research gaps, develop the initial information security culture framework. It seeks to explore a more detailed view and understand of factors of interest with regard to human behaviour either constitute or influence the information security culture. The use of the interviews would allow for an in-depth understanding of factors affecting the information security. It would also reveal which factors viewed as more important in the organisation from the perspective of participants.

There are three forms of conducted interviews, which are structured, unstructured and semi-structured. A structured interview functions through a series of questions that are pre-designed and unaltered during the interview, where the answers are directed as definitive responses (Berg 2004). These are used when specific and exact information is required. An unstructured interview refrains from a restricted series of questions, as it progresses additional questions based on the participants' responses. This helps to further explore certain key areas of interest that arise. A semi-structured interview is a combination of the two forms, and frequently the most beneficial method, where the questions remain predetermined. Although the participant maintains more freedom in their answers, as well as allowing the interviewer the possibility to ask additional explorative questions.

Semi-structured interviews are a vital methodological tool in qualitative data collection. It is used in grounded theory and for ethnographies, as well as specifically in important case studies (Yin 2003). Additionally, semi-structured interviews, in regard to information systems, are commonly deemed to be appropriate when research is in its initial stages (Benbasat & Zmud 1999). Zakaria (2004) study suggested the use of semi-structured interviews in order to gather information regard employees' assumptions, real and implicit security behaviour in the information security culture research. Thus, the semi-structured interviews allow for research to be undertaken in a more beneficial way within the security culture of information, as they maximise interview flexibility whilst providing opportunities to guide and alter the interviews in a specific manner to each individual participant (Tashakkori & Teddlie 1998). Due to their benefits, semi-structured interviews are a form of appropriate research tool when undertaking information security culture research.

There are a variety of semi-structured interview forms: exploratory, explanatory, and descriptive (Yin 2003). In general, the exploratory form is normally utilised in relation to "What" style questions, where it is the aim to create a hypothesis and base for additional inquiry, and thus, helps to create research questions. Comparatively, an explanatory interviews

function around the questions of “How” and “Why”, where the aim is to determine whether causal correlations exist between different events and/or variables. Lastly, the descriptive interviews enable a researcher to acquire a greater level of descriptive data in regard to the topic. These are commonly used to provide answers to “How many” and “How much” from questions of “What” (Yin 2003).

In this research, the semi-structured interview was used in an exploratory manner in order to enhance theoretical propositions regarding the information security culture in organisations, to gain in-depth information from employees directly involved in the information security in organisations and to discover new issues that might affect the information security culture. The outcome of the semi-structured interview helps to develop the proposed framework and confirm the importance of identified factors in the framework.

Through the utilisation of interviews, it is possible to demonstrate candidate factors in the conceptual framework in relation to the model of information security culture. Subsequently, these findings are further tested through survey questionnaires. Accordingly, it is model testing that is specifically included in the development of the information security culture framework, while important new factors will also be included within the framework. The qualitative interview findings are combined with the literature review in order to develop a conceptual framework for the research. Hence, the main objectives of interviews are as follows:

1. To advance the framework for information security culture by determining whether all ten factors within the proposed framework are necessary for an organisation; and whether any new factors should be incorporated into the emergent framework.
2. To acquire sufficient information in relation to information security from participants directly involved with organisations.
3. To obtain input that can be used in the construction of the proposed framework and to gather evidence to justify the survey constructs and items.
4. To determine issues that the researcher has not previously considered which may potentially alter the information security culture.

#### *4.4.2.1 Interview Guide Development*

It is important to structure the interview to ensure that the sequence and consistency of questions constant for all participants (Yin 2003). The researcher has to construct questions in a manner to keep participants on focus with their responses to the questions (Creswell 2002).

The first step in conducting a successful interview is to prepare an interview guide (Gill et al. 2008). The interview guide is used as a general direction for interviewees in order to cover all topics and issues that needed to achieve the research objectives. The interview guide assists in maintaining the structure of the interview; the consistency of data; and reduces bias. The open-ended questions enable more in-depth responses from the participants, which improves the richness of the data. In this research, the interview guide was established to direct the interview process and maintain data consistency. The aim of the semi-structured interview in this research is to highlight the importance of all identified factors in the proposed framework that might support in the process of information security culture measurements. The questions of interview from each of these perspectives were designed in the interview guide. More detail about the interview guide design and process is provided in Chapter 6 (sections 6.3 and 6.4).

#### *4.4.2.2 Interview Guide Pilot Study*

A pilot study, or a 'pre-test', is an opportunity, before the execution of the research to measures the use of the research instrument, and to highlight potential challenges (Alreck & Settle 1995). A pilot study ensures that the interview guide is appropriate and also shows precisely what may be expected during the research method. This also determines the appropriate unit of analysis in the interview, which helps to improve the instrument of data collection instruments (Yin 2003). A pilot study enables the researcher to see whether the questions tap into the relevant phenomenon or topic, which relates to content validity. It also shows whether evidential phrase variations in the questions elicit similar responses, which ensures construct validity. Therefore, a pilot test for the interview guide has been conducted in order to check that there are no repeated questions, is free of unanticipated difficulties and that the participants could understand questions clearly without creating bias.

#### *4.4.2.3 Validity*

Validity in the research aims to ensure that measurement instruments function correctly in their process to include sufficient item representation in order to present the concept (content validity), differentiate sufficiently between items (criterion-related validity), and ensure that the measurements that are used fit the test's stated theories (Construct validity) (Sekaran 2003). It has been noted previously that validation is not vital in qualitative research, as different notions demonstrate the object of study (Mouton & Marais 1996).

However, Dikko (2016) stated that a pilot study of the research instruments is an important way to develop research validity. A pilot study was conducted to ensure the content validity of the interview in this research. It checked the interview relevance of the questions and considered evidential phrase variations in the questions elicit similar responses. The pilot supported this research in measuring the validity of questions in the interview guide.

#### *4.4.2.4 Reliability*

Reliability in research relates to whether the study could be replicated and repeated to produce the same set of data results. It must be consistent and enable any additional researcher to copy the set procedures and obtain the same results (Yin 2003). Therefore, the data collection procedure in this research for the interview process has been documented and the interview guide determined. A description of the selection criteria and analysis of data has also been documented. Hence, the current research could be shown to possess a high level of reliability.

#### *4.4.2.5 Interview Sampling and Methods of Sampling*

A research sample presents a section of a population that is selected in order to draw study conclusions (Bryman & Bell 2015; Sekaran 2003). A sample is a vital part of research, although often a challenging task. Cohen et al. (2013) stated that the research quality is commonly dependant on the suitability of the sampling strategy that was used in the study. There are two type of sampling strategy: probability sampling and non- probability sampling (Bryman & Bell 2015; Creswell 2002). In regard to the probability sample, the population's individuals receive an equal selection opportunity, while there is no selection predetermination in the non-probability sample (Bryman & Bell 2015).

The selection between the two forms of sampling is dependent on the design and method of the research. For instance, qualitative research normally incorporates non-probability sampling, due to the fact that it aims to develop a clearer specific understanding against more generalised data. Ritchie and Lewis (2005) added that non-probability sampling method is beneficial in qualitative research to select the research population. A researcher is able to choose different individuals from a non-probability sample based on their availability, convenience, and whether they fit with the stipulated characteristics (Cresswell 2008). Subsequently, the current research uses non-probability sampling, as the aim is to learn from different individuals who can provide clear information that connects with the particular area of research, instead of producing a representative sample with general findings.

Non-probability sampling has different techniques that can be applied, including: quota sampling, convince sampling, purposive sampling, and snowball sampling (Robson 2011). Purposive sampling and snowball sampling were used in the current research's data collection. Purposive sampling is a commonly used method in qualitative research (Cohen et al. 2013). Purposive sampling helps to access people with valuable and relevant information that have in-depth knowledge about a particular area or topic of study, as their professional roles, and experience prove important to a study's improvement (Cohen et al. 2013). In this research, the participants comprised of IT/ security specialists working in relevant organisations.

The snowball sampling is a technique that normally occurs after the study begins when the researcher requests the participants to recommend others to participate (Creswell 2008). The participants are able to provide key access to different relevant individuals, in order for the research sample to be created. Accordingly, snowball sampling was used in this research in order to gain access to relevant organisations, as this is not always easy in the United Kingdom, due to strict rules and regulations of security management, and other considerations.

The method of non-probability is not a representative form, as the findings are not necessarily able to be generalised. Nevertheless, the findings' generalisability was not the goal of this research, which was merely to acquire more information from individuals who are in positions to give it (Cohen et al. 2013). In general, there are no set regulations on how big a sample size should be, although certain factors are relevant that can restrict the size, which include time and the limitations of resources (Blaikie 2019), and the relevance to the study's aim (Cohen et al. 2013). In addition, Briggs (2012) noted that the selection of a small number of individuals to be included in intensive interviews can be beneficial. Consequently, this research used the two methods: purposive and snowball sampling, in order to interview ten to thirteen IT/ security specialists.

The main aim of the research is to create a conceptualisation of the cultural framework of information security, which will assist in the development of more effective information security in organisations from a variety of industries and sectors. This will enable greater levels of understanding of the culture of information security phenomenon, which will provide analysis from different backgrounds and produce new findings in order to progress the research. Therefore, it is important to select IT/ security specialist from organisations of a broad range of size, sectors and industries in this research. Organisations of size and complexity might require different levels of security and different awareness levels of the information

security culture. The selection of different type of organisations would help in the understanding of information security culture phenomenon from different perspectives and backgrounds in order to capture data from organisations with different levels of security. In addition, being able to differentiate between industry sectors and provide each industry specific information security culture benchmark would assist organisations to make individual decisions regarding their information security culture programs. This could be used to guide their investments in security awareness, security training sessions (Roer & Petric 2017). Detailed information about interview sampling provided later in Chapter 6 (section 6.5).

#### *4.4.2.6 Interview Process and Conducting*

Following the target population selection, the subsequent part of the interview was to conduct and detail the process with the participants. In this research, the interview process was based on Runeson and Höst (2009) stages that followed during the interviews, which included seven particular stages:

1. The interview starts with the researcher introducing himself and presenting the support letter.
2. The research objectives and the general purpose of a study are presented and explained with an interviewee.
3. A consent form is signed by both parties to show that the interviewee has understood the context of their participation. This includes the possibility to consider the information they provide and to ask questions when required. The interviewees should be aware that the participation is on a voluntary basis and that it is possible to withdraw at any moment, without reason. The Plymouth University Ethical Principles for Research Involving Human Participants will also be adhered to throughout the process. The information would also be anonymous in all reports, publications and presentations.
4. The potential interview duration is stated to the interviewee, as based on the pilot study's findings.
5. The interviewee is asked whether an interview recording is possible.
6. The interview starts with notes taken during the stage of the interviewee answering the questions.
7. Following the interview, the interviewee is thanked for their participation and information provided.

Furthermore, there are various forms of communication that can be used to conduct the interview such as face-to-face meetings or meetings online by using Voice over IP technologies. In this research, the interviews were carried out in the offices or meeting rooms of the interviewees or online video call using Skype, as this enabled all the interviewees to have equal participation and be able to discuss any details they required. Following the interview completion, the interviewees received the transcripts, as this allowed them to make any changes where relevant (Runeson & Höst 2009). Further details in relation to the overall process of the interviews are presented in Chapter 6 (see Section 6.6).

### 4.4.3 Survey Method

Survey is a research instrument that presents different questions that enable the acquisition of primary information from participants (Oates 2006). Consequently, the researcher acquires more knowledge of a particular topic of interest. The survey method is relevant to this research, as it is quick, inexpensive, and functions efficiently and accurately as a way to assess information in regard to a set target population (Zikmund 2003). A questionnaire helps to produce quantitative data that is subsequently analysed and to examine different variables of data. Zakaria (2004) recommended the use of the questionnaire in collecting information relate to employees' prior assumptions regarding security and their behaviour in information security culture research. Accordingly, a questionnaire style method was shown to be a reliable research method in this research. In total, four research design aspects have been stipulated for a survey method by Pinsonneault and Kraemer (1993), which all apply to this research. These include the questions of interest regarding the phenomena of what, how and why something is occurring. It is also the interest of the research to comprehend the factors that influence upon information security culture and which comprise information security culture as the necessary stages to develop the most efficient information security model.

In addition, the independent and dependent variables' control level is not a possibility and is not actually a desirable option. This research used the perceptions of the information security culture as the main observation unit. Moreover, the phenomena that are researched should be analysed in their natural environment. The information security culture of individual participants within their organisations' natural settings are used in this research. Also, a questionnaire can assist in the process of data collection from large representations of individuals in organisations.

The information security culture demonstrates a form of behaviour that is interesting and innovative in organisational development, as its creation may improve levels of effectiveness with regard to information security. The questionnaire helps to ascertain this information as there are numerous advantages to its implementation. Questionnaires are cheap to formulate and implement and have a standardised answer format that can make data compilation simple. Besides, the wording and structure of a questionnaire can prove to be very effectual upon on the overall data quality. Questionnaires have to be piloted first in order to ensure that respondents did not get frustration feelings. As questionnaires are often limited in options, and the respondents can sometimes read the questions and interpret them incorrectly.

Pinsonneault and Kraemer (1993) have stated that a survey research can be used for exploration, description, or explanation. The aim of the exploratory survey is to increase the level of familiarity with the particular researched phenomenon of interest, which focuses on taking the most important parts and determining the most beneficial way of measuring them (Recker 2008). This is used to develop different concepts, discover the likely response range in certain population dynamics, and to refine the concepts' measurement (Pinsonneault & Kraemer 1993). A descriptive survey is used in order to ascertain the situations, events, attitudes, and opinions that can be examined from a certain population (Pinsonneault & Kraemer 1993). The explanation survey tests the theory and causal connections between variables (Pinsonneault & Kraemer 1993). The main question in the explanatory study is whether the hypothesised causal connection exists, and whether it is there for the correct reasons.

In addition, Pinsonneault and Kraemer (1993) classified a survey research into cross-sectional surveys and longitudinal surveys. Cross-sectional surveys analyse the sample population through one particular moment in the collection of data. Longitudinal surveys help in the analysis of study variables over a period of time (Pinsonneault & Kraemer 1993). Due to the lack of reliability and validity in the information security culture measurements, as the literature shows, the exploratory survey has adopted in this research in order to validate the importance of each factor proposed in the framework, as the reliability of the framework is subsequently tested for practice. Also, the exploratory survey will enhance the testing of data validity and reliability (Alnatheer et al. 2012).

The explanatory survey is designed to test the causal connection between influential factors for security culture and ones that constitute the information culture of security. In this research,

cross-sectional surveys for data collection were used only once. Cross-sectional surveys are uncomplicated to design and simple to establish research validity levels. They also take less time than longitudinal surveys to implement and are known to be feasible and practical. The main objectives of the survey are as follows:

1. To test the validity and reliability of the study framework.
2. To validate the influential factors of the study framework.
3. To test the relationship between the factors influencing information security culture and factors constituting the information security culture.
4. To acquire sufficient information in relation to information security from participants who are directly involved with organisations.
5. To determine issues that the researcher has not previously considered, which may potentially alter the information security culture.

#### *4.4.3.1 Questionnaire Development*

The next stage is the establishment of the data collection instrument. It is considered to be an important, although complex process, to implement the survey research in order to achieve the set research objectives, and create the correct instrument that is relevant and accurate (Zikmund 2003). Specifically, the data collection tool has to be capable of answering the overall aims of study in relation to the particular measured phenomenon (construct validity) and its form of measurement (construct reliability) (Zikmund 2003; Sekaran 2016). The potential to assess organisational security culture levels is vital in exploring risk sources that assist in developing quality beneficial solutions (Okere et al. 2012). The level of assessment in the information security culture in any organisation is generally still questioned. It has been noted that a very few methods or utilised tools are present that define how to accurately assess its information security culture. However, very few accepted publications have been produced to prove this, which is why further research is required (Alhogail & Mirza 2015). To implement a questionnaire is one form of measuring the information security culture of an organisation (Martins & Eloff 2002; Schlienger & Teufel 2005). This will produce further comprehension of what influences the security behaviour of employees. Various advantages for the utilisation of a questionnaire have shown in the assessment of the information security culture (Da Veiga 2008; Martins & Eloff 2002), as shown below:

1. To identify potential concerns and improvement opportunities;

2. To help an organisation to define the present information security culture and the future aims, together with noting the necessary actions to accomplish a better security culture;

3. It can potentially increase awareness of information security culture while raising an organisation's commitment to make employees more connected to the process;

4. To monitor and evaluate how changes and performance improve; questionnaires may be used by management to analyse the improvements to an information security culture.

In this research, the questionnaire has the goal of evaluating the framework level and provide validity of the influential and reflecting factors that influence the proposed framework. Da Veiga et al. (2007) and Martins and Eloff (2002) studies stated that the questionnaire in the assessment of information security culture needs to adhere to the subsequent stages, which provide structure to the process and quality to the obtained data. These steps are present below. The details of the questionnaire design and distribution discussed later in Chapter 7 (sections 7.2 and 7.5).

1. To develop the questionnaire;

2. To administer the questionnaire, including distribution and response monitoring;

3. To analyse the data, in order to ascertain an indication of information security culture level;

4. To interpret and recommend the action plans in order to develop an information security culture quality.

#### *4.4.3.2 Validity and Reliability*

Validity and reliability concepts were considered as important in the survey development, to ensure the quality of the data collection tool. In relation to validity, this helps the questionnaire assessment of what it actually intends to assess (Martins & Eloff 2002). The information security culture is measured by connecting the correct aspects and framework components that function as the theoretical base to assess the information security culture within an organisation (Da Veiga 2008). It is also necessary for the presented questions to represent and cover the complete list of issues that the framework will measure. Reliability relates to the measurement

consistency levels when there is a replication of assessment process. Accordingly, the survey questions have been presented so that the respondents are able to interpret them in the same manner (Martins & Eloff 2002). Once these questions were prepared, a checklist was undertaken to show they had been designed correctly. The questionnaire checklist consisted of the following:

- Relevance of statements to the framework that focus purely on the information security culture composition within organisations.
- The statements do not include ambiguous technical terms, misunderstood abbreviations and terminology for specialists that cannot be interpreted by the participants.
- The framework's different elements need to be covered by a clear survey statement that ensures the validity of the results.
- The statements are clear and concise in order to be presented as understandable by the participants.
- The statements need to have only a single concept or issue, as this ensures that the correct and relevant data analysis.
- The selection options to questions must be clear and with clearly distinguishable alternatives.

#### *4.4.3.3 The Questionnaire Pre-test*

Prior to the official questionnaire being presented to the target population, a pre-test needs to be conducted on a smaller sample of employees. Following the design of the original survey tool for the research design, the subsequent step is to make the questions perfect and clear. This helps to produce a good level of understanding for a larger group, as well as to redevelop the questions when necessary (Berry & Houston 1993). The objective of the pre-test is to support the test of face validity for the questionnaire, which relates to the determination of whether the questionnaire assesses what it is supposed to (Berry & Houston 1993). It is normally necessary to make small adjustments to certain questionnaire statements in order to ensure that the employees can follow the same interpretation of the questions. In general, two common forms of pre-tests can be applied: panel judgments and pilot study. This research used both methods in the questionnaire testing process.

*4.4.3.3.1 Expert Review*

Expert reviews (panel judgements) have been used as methods for pre-testing surveys in order to identify problematic linguistic structures within different questions (Olson 2010). Expert reviews are commonly used as a method to evaluate questionnaires that can assess a survey content validity by requesting detailed responses that relate to clarity, relevance, and item quality. The main aim of an expert review is to show whether a survey instrument presents any issues, so they can be rectified before application in the final survey, or to place items into different groups which may potentially show errors of measurements (Olson 2010). Normally, in the process of questionnaire evaluation, an expert review is quick, inexpensive and simple to implement (Presser & Blair 1994). In general, the number of expert reviews in this method is minimal, with a range of two to three expert methodologists applied to twenty reviewers or more (Holbrook et al. 2007). The results are presented in Chapter 7 (section 7.3.1).

*4.4.3.3.2 Pilot Testing*

Pilot tests are invaluable in the process of questionnaire construction, as tests provide constructive feedback on the questions and structure, as well as removing ambiguity (Babbie 2012). A pilot test functions to check the feasibility of the questionnaire in relation to reliability and validity. This will improve the design of the instrument prior to the final data collection process (Zikmund 2003). It has also been noted by Ticehurst and Veal (2000) that a pilot test helps in the elimination of potential weaknesses in a survey's instrument, which analyses the wording, structure and layout, familiarity with participants, rate of responses, average completion time, and process of analysis. The optimum sample amount for a pilot test is normally ten to thirty individuals taken from the studied population demographic (Luck & Rubin 1987). The results of the pilot study conducted in this research are presented in Chapter 7 (section 7.3.2).

***4.4.3.4 Population and Survey Sampling***

The research sample population is a clear set group of people or objects that are observed and analysed for the purpose of research (Saunders et al. 2003). For certain studies, it is not feasible to undertake data collection in regard to an entire population demographic due to its size. Hence, the sample size is an alternative way functions in data collection to represent a study population (Saunders et al. 2003). It has been stated by Neuman (2006) that sampling helps to systematically select cases that will be included in a research study. Neuman (2006), added

that a researcher uses certain elements or samples that are easier to work with and are more cost effective in comparison to simply working with a full range of cases. The process of a sample population helps to reduce labour requirements and produces vital information more rapidly. A representative sample needs to be at the optimum size to enable quality and beneficial conclusions from the data, which would legitimately help to generalise the findings.

It is important to select the method of sampling before collecting the data. Sampling methods are divided into two categories: probability sampling and non-probability sampling (Creswell 2002). All different elements in the population within probability sampling have a non-zero probability of selection; while the sampling units' selection in non-probability sampling is based on the judgements of availability and potential convenience (Zikmund et al. 2010). The survey data is taken through the completion of a questionnaire only, although many potential participants view this as too time consuming and often refuse to participate. Within this form of research, it is difficult to accumulate a good number of responses, and employees to motivation to complete the questionnaire. Consequently, a non-probability sampling method was selected for the current research.

Within non-probability sampling method, snowball and convenience sampling techniques were used. A snowball sample technique is a type of non-probability sampling technique. The snowball sample is implemented following the commencement of the research, when the researcher requests participants to recommend different people to participate. This research used this technique as it helped to gain access to different participants, who subsequently completed the survey and were also able to invite other relevant people from their organisations to potentially participate in the survey as well. A convenience sample is a form of non-probability sampling method that stems from a researcher judgement and determining the optimum sampling size based on prior research and population limitations. The convenience sample allows the research to focus more on the analysis of the results. A convenience sample includes the selection of cases that are the simplest to ascertain, where the selection process continues until the desired size is obtained, although without a clear sample size requirement (Saunders et al. 2003). The size of the sample is based on a convenience sampling method in this research. The sample is comprised of individual employees who are willing to participate in the study, and the selection needs to be at least 10% of the stated population. Convenience sampling does include potential bias, which can be avoided through the distribution of the questionnaire to all stated employees in order to avoid the failure of certain parts. Additionally,

all the responses need to be kept and analysed, in order to ensure that all organisation members are represented, including different level of jobs.

This research aims to conceptualise the information security cultural framework in order to assist in developing better effective organisational information security for different industries. Subsequently, this will increase the level of comprehension of information security culture phenomenon, and simultaneously create an analysis from numerous backgrounds in order to present innovative findings that can progress the overall research. In order to choose the candidates for the study sample, it would be better to have organisations from a variety of industries to receive the questionnaire, as there might be different security levels required, and thus, contrasting different forms of information security culture. It would also be more productive to send the security culture questionnaire to the organisations' entire employees, as this would help to ensure data reliability. However, it could also be possible to send the questionnaire to set demographic groups of employees who share similar characteristics, which may include business units and their geographical locations (Brewerton & Millward 2002). This could develop the comprehension levels of information security culture phenomenon, as different perspectives and backgrounds would be presented, which would help to capture organisational data with a variety of security levels. This will also help to generalise the overall findings to many different industries. Detailed information about survey sampling provided later in Chapter 7 (section 7.4).

#### *4.4.3.5 Questionnaire's Administration and Process*

The administration of the questionnaire communicates the survey and its objectives to the employees, which will improve the response rate and quality (Dillon et al. 1993). There are numerous methods that can be used, which correspond with the input provided by the form of communication. For example, an organisation may circulate an e-mail for the survey launch in order to notify their employees of the questionnaire and to detail the objectives. Subsequently, weekly e-mails can be sent as reminders to complete the questionnaire prior to the stated due date. Other methods can be used, which include competitions to motivate participants, posters and additional incentives.

The questionnaire in this research was sent via e-mail with an invitation of participation to employees to complete online. It was distributed to and collected online from the survey population and accompanied by a covering letter. This letter ensured confidentiality and

anonymity. It gave a description of the questionnaire, and the allocated time to answer the questions. There are other forms of data collection, which could have been which include: paper surveys, e-mails, online surveys, and interviews (Da Viega 2010). Data collection through an online survey produces various benefits, as this helps with the automation of data entry, as well as its return. The current research used an online questionnaire because it was considered the most effective.

For the participants, the online format of the questionnaire protects their privacy and increase security levels, as well as providing a convenient time for them to complete the questionnaire at their discretion (Singleton et al. 2009). The researcher benefits from time saved in data-processing and eliminates interviewer bias (Selm & Jankowski 2006). The online survey software Qualtrics, was used to develop the online questionnaire, where the participants could answer the questions at their own convenience. The responses also need to be monitored in order to obtain statistically representative responses for different biographical areas, which include different job levels and departments. For these areas where the responses were deemed to be insufficient, different trends can be considered, as well as focus groups to better show the results. There is a more detailed about survey administration in Chapter 7 (section 7.5).

## 4.5 Data Analysis

Once the research design is established and the requirements for the collection of data, which includes both qualitative and quantitative data, the following stage is the data analysis and findings in order to provide results to support the research and to determine the main findings in regard to information security culture. Semi-structured interviews were used for qualitative data, which produced statistical analyses of the research issues. The questionnaire produced quantitative data that requires analysis of different statistical tests based on the questionnaire's main variables. These analyses are needed to achieve the overall research objectives, while the results from the data analysis are developed in the research discussions. The analysis process is presented briefly in this section. An additional detailed description is shown later in Chapter 6 (interview analysis) and Chapters 7,8 and 9 (questionnaire).

### 4.5.1 Interviews Data Analysis

Data analysis is a distinctly challenging aspect within qualitative studies, which is also one of the least developed and understood forms. Data analysis includes the necessity of examining, categorising, testing parts of evidence that will help in developing hypothesis (Yin 2003). The

process of qualitative data analyses involves stages of reduction/summarisation of the data, classifying and interpreting the findings. In this research, semi-structured interviews were transcribed in order to provide the necessary qualitative data. There are also different approaches that help in the analysis of qualitative data, which include grounded theory and content analysis. Specifically, grounded theory is acquired from presented data that obtained from social research (Glaser & Strauss 1967). The grounded theory involves developing a hypothesis from the data whilst conducting the research.

The content analysis is a form of methodology that uses different procedures to create valid opinions and inferences from a text. The inferences relate to who provides a message, the message itself and/or who receives the message, as well as how this process occurs and differs from the researcher's perception (Weber 1985). Content analysis has normally been used to analyse archival data, and not transcripts of interviews. Traditionally, the techniques have been quantitative with limitations placed by the text's characteristics. These quantified results can often include the word occurrence ratio and the number of words that relate to a specific theme, which are subsequently used for statistical analysis. This research used content analysis approaches to discover themes and patterns in elaborated responses.

Interviewee responses were scripted, as this would provide the possibility for content analysis and review. The obtained qualitative information was subsequently used and analysed in order to determine different opinions and to correlate into a proposed framework. The analysis of data used the within-case analysis strategy in this research. Th within-case analysis provides information within the context of reality, where the ascertained information would provide insight into the studied factors. Commonly, a within-case analysis includes detailed interviews and clear transcripts for each interview. The researcher is then able to gain a better understanding of the specific phenomenon by interpreting the qualitative interviews data that shows a variety of different comparative personal perspectives (Creswell 2002).

The current research adhered to set procedures of qualitative data analysis, as shown by Yin (2003). These included three different stages: selection of a general strategy in order to know what and why to analyse particular entities; to code the evidence; and to use an analytical technique for the development or testing of theories. A detailed description of these stages, together with an analysis process is detailed in Chapter 6 (section 6.7). The software program, Microsoft Excel, was used in the analysis of data, as this helped to show the event patterns that

related to comparative factors/constructs, which demonstrated forms of development and innovation within information security culture.

### 4.5.2 Survey Data Analysis Process

The survey data analysis was segmented into two stages: preliminary data analysis, which related to the preliminary data analysis that presents the descriptive statistics; and structural model evaluation, which provides the overall perception from the participant data and responses. The SPSS software version 25 was used to conduct the tasks from the pilot test, it has been referenced by many researchers as beneficial (e.g., Tabachnick and Fidell 2007). These tasks included: coding, editing, checking missing data, assumptions of normality, multicollinearity, outliers and factor analysis. There is a more detailed overview of the different tasks provided in Chapter 8 (section 8.2).

The following section of the analysis connects to the structural model's evaluation, which examines the correlations between both various independent and dependent variables that relate to information security culture. Additionally, demographic characteristics also affect the function of the analysis, and thus, the Structural Equation Modelling (SEM). Also known as path analysis with latent variables (Bagozzi & Yi 1988). It has been used in testing the theoretical model. Tabachnick and Fidell (2007) state that SEM functions as a group of statistical techniques which are able to establish and evaluate the correlations between multiple constructs simultaneously.

SEM's statistical techniques can be set into two broad groups: covariance-based modelling (e.g., LISREL, AMOS) and variance-based or component-based modelling (e.g., PLS) (Gefen et al. 2000). In this research, Partial Least Squares (PLS), a component-based SEM technique, has been used as the primary examination process for the structural model's paths. In particular, SmartPLS Version 3.3.2 has been used for the data analysis. PLS can be justified as valid to use in the current research, as it functions correctly with the process and has been popular in recent studies. For example, PLS has recently started to gain in interest, as it has a capacity to model latent variables for both sets of samples: non-normalised and small amounts. It is also beneficial in the examination of measurement paths and to detail structural paths' regression estimation (Henseler et al. 2009).

The structural model of this research has provided an evaluation in a two-stage process through a hierarchal basis (Henseler et al. 2009). Initially, an assessment of the measurement model

was conducted to examine psychometric reliability and validity tests. Additionally, multiple regression technique has been utilised in the structural paths' assessment (i.e., hypothetical relationships based on sign, magnitude and significance levels). The moderating impact of demographic information on the proposed relationships have been assessed by a Multiple Group Analysis (MGA) technique, that is similar to the hierarchical multiple regression process developed by Cohen and Cohen (1983) study. This research used the bootstrap method for a total of 500 cases with 2000 samples in order to obtain the t-value. This helps to determine the path relevance between different hypothetical relationships. Chapter 8 presents clear details of SEM's main concepts; the different analytical techniques that use SEM; practical considerations in the adoption of SEM; the measurement model' evaluation criteria; the structural model as taken from the two-stage process; and how MGA is used in the examination of a moderation effect.

## 4.6 Ethical Considerations

When research aims to analyse human behaviour, ethical considerations are important to the process, and need to be determined prior to commencement and adhered to throughout the entire research process (Zikmund et al. 2013). When ethical matters are not considered in the study, participants often fail to cooperate correctly, and thus, data collection issues arise. Ethical standards should always be adhered to, and consent needs to be obtained from the subjects in order to undertake the study. Sekaran (2016) states that a researcher must implement human rights within the research, as he/she needs to complete a sequence of ethical procedures. Initially, participants need to be assured that their data remains totally confidential at all times, as well as not having any of their information solicited to any third party. Additionally, the participants should be assured that none of the data taken from them is ever misrepresented, together with a clear representation of the research's aims shown. Participants' self-esteem and self-respect show never be violated during the study process, and consent should be obtained from each participant prior to participation, with a clear right to withdraw at any stage without the need to provide a reason.

Plymouth University Research Ethical Committee's guidelines have been adhered to, alongside the recommendations provided by Sekaran (2016), during the data collection process. As stated, it is always necessary to present a consent form that ensures that each participant understands the voluntary nature of their participation, and their free choice to withdraw at any

time without providing any reason. In addition, via the consent form, participants were informed that they were under no obligation to answer the questions, whilst being informed that all their information and specific answers would remain confidential through secured data that would not be shared with any third party. Following the requirements' completion and the development of the consent form, approval letters were obtained to collect data from both the interview and questionnaire (see Appendix B and Appendix C). During the process of data collection, the cover letter was attached with the different instruments, which included the research title and the ethical consideration requirements. The respondents were informed that that completing the interview or questionnaire and signed or returned it back to the researcher was assumed to be their consent of participation.

## 4.7 Conclusion

This chapter presented the empirical study's process with the goal to evaluate the validity and reliability of the proposed framework. It has also detailed the methodological approach used. This included the specific research paradigms and approach, as well as the research design's justification of use. Correspondingly, in relation to research into information systems, the positivist and interpretive perspective of information systems has been shown to be justified with an inductive approach. The research strategy used was through a mixed method process to data collection of qualitative (interviews) and quantitative (questionnaires) data. The qualitative data were incorporated with the literature analysis, as this helped to develop the framework for information security culture and assisted in the questionnaire design. In regard to the quantitative data, an analysis was used as a process for framework testing and validation. Following this, the subsequent three chapters detail the empirical study that shows the practical implementations of the interview process and questionnaire, as shown in this chapter. The empirical research findings from the qualitative interviews and findings from the quantitative questionnaire are documented in the following chapters, as well as the development of information security culture framework

# Chapter Five : A Framework for Information Security Culture

## 5.1 Introduction

The purpose of this chapter is to present the proposed research framework and its components by providing the theoretical base of the framework, and its basic development principles. The first section in this chapter justifies the need to develop a new framework. It explains the limitations of the current studies and models in covering the information security culture issues, which emerged from both of Chapters 2 and 3. This section provides a general overview of the limitations of the current studies that lead to identify the information security culture issues and factors that have not previously been considered in the existing studies; these are covered in the proposed framework. The second section defines a new comprehensive information security culture framework, which could be used to cultivate and assess the information security culture in an organisation in order to protect their information assets from internal threats. It presents and discusses the new proposed framework for the current research and its elements. Next, the interaction between components identified in the current research framework is explained and the practical use is exemplified, leading to resulting conclusions at the end.

## 5.2 Limitation of Current Studies Considering Information Security Culture Factors

In the information security culture domain, there are a considerable number of studies that have been published and contribute a good understanding of how to create and assess an acceptable level of information security culture, in order to ensure security and reduce breaches in organisations. Based on the literature review conducted for this research, most of the previous studies develop a comprehensive framework and demonstrates the importance of understanding various factors and issues that could possibly affect the information security culture.

However, there is still a need for more investigation in the field to provide a comprehensive framework for the establishment of the information security culture in the organisation. For instance, the comprehensive review revealed that there are limited of studies that developed a framework, which could be used for both creating and assessing the information security culture, in order to ensure the effectiveness of the approach and ensure content validity. There is no mutual agreement on the factors that have to be considered for establishing the information security culture. There is a lack of frameworks that guide and integrate all main

factors that should be considered to have an effective information security culture (Karlsson et al. 2015; Nasir et al. 2019; Sas et al. 2020). The numbers of the studies that identify factors that constitute or influence the information security culture are limited and still need more investigations (Alnatheer et al. 2012; Nasir et al. 2019; Walton 2015).

There is still limited coverage of other influencing factors. There are efficient factors that most widely investigated and examined in the literature on behaviour of employee in orgainsations that can motivate the employee behaviour toward the information security. These factors have not been deeply considered in previous studies in the information security culture field such as the individual difference variables and job satisfaction. In addition, McCormac et al. (2017) study indicated that the need for future research that examines the potential interplay between the information security culture and individual difference factors. As a consequence, this research will cover other factors that could possibly influence the information security culture in order to improve the security of information assets in organisations.

Additionally, very few studies have developed a theoretical framework, which substantially combines all important factors that positively influence the effectiveness of information security culture. Limited studies have provided empirical analysis that clarifies the relationship between the identified factors. Also, very few studies that provide a statistical analysis in their developed security culture assessment instrument. Neither where different validation techniques used such as, the Structural Equation Modelling (SEM), in order to validate their frameworks or measurement models in the information security culture domain. Most of the previous studies are based on qualitative technique without including empirical evidence or quantitative technique (Karlsson et al. 2015; Pevchikh 2015; Sas et al. 2020). This has to be considered a limitation.

## 5.3 The Information Security Culture and key Factors Framework (ISCFF)

The framework is defined as a basic layered conceptual structure, which demonstrates how its parts would be associated (TechTarget 2014). The framework is proposed to work as a support and a guidance for cultivating the information security culture; that structure could be expanded into a practical tool for organisations.

An early finding from the literature reviews indicated the lack of systemic treatment and measurement of information security culture. As a result, the main objective of the current

research is to present a comprehensive reliable and valid framework that incorporates aspects of human behaviour to address the insider threat. Also, to provide a guide for organisations and practitioners, in the cultivation and assessment of information security cultures. Therefore, this research proposes a comprehensive framework that combines key human factors to be considered in the development of measures to avoid insider threats to information security in organisations.

The proposed framework facilitates the understanding of information security culture and of elements that could reinforce the information security culture. The proposed framework could be used by researchers and organisations as a starting point to understand how to cultivate and measure the information security culture. The framework could help in the minimisation of risks posed by employee behaviour. The framework highlights factors that can have a substantial positive influence on the cultivation of information security culture. Raising awareness of what influences the information security culture can help employees to interact with information security requirements and assist in the protection of assets. The framework will also assist in the assessment of the relationship between factors that influence the information security culture, and factors that constitute the information security culture. The framework could be used as the basis for developing a measuring instrument for information security culture in an organisation.

### 5.3.1 The Development of the Proposed Framework

The development and construction of the proposed framework were based on the model from Alnatheer et al. (2012), and on a comprehensive review of academic and professional literature review on the information security cultural areas as presented at Chapter 3. Alnatheer et al. (2012) study was the only one that specified what factors constitute information security culture. The model was statistically tested for validity and reliability by using advanced techniques, such as a Structural Equation Modelling (SEM) approach to Confirmatory Factor Analysis. Other studies and models have been developed by using Alnatheer's model, such as Walton (2015). Chapter 3 discussed the most important factors that assist the cultivation of an information security culture in organisations. However, there was no clear demonstration of the integration between factors. The proposed framework highlights the integration between various factors associated with the information security culture. This framework can be used as a guide for managers and practitioners in the implementation process.

#### *5.3.1.1 The Framework Components*

In the proposed framework, information security culture comprises several factors (see Figure 5.1), that could motivate individuals toward compliant security behaviour in the workplace. There is strong agreement among the academic researchers on the key factors that have a positive impact on the information security culture. The main components of ISCFF are structured in three categories comprising of the top eight constructs/factors identified in Chapter 3, and which have a positive impact on an information security culture. There are other factors that contribute to a variety of workplace behaviours, such as personality traits and job satisfaction. These two factors have received little attention from scholars in the information security culture area. These factors have been added as candidate constructs to the proposed framework. It is important to note any potential interplay between these two factors and the information security culture. This research predicts that the personality traits and job satisfaction might positively influence the information security culture. These appear to be the most influential factors and are considered as part of the conceptualisation of information security culture. The rationale for grouping the components is based on the framework by Alnatheer et al. (2012) study and Greene and D'Arcy (2010) study. Figure 5.1 below provides the proposed Information Security Culture and key Factors Framework of this research. The total identified constructs/factors are described in the following sections.

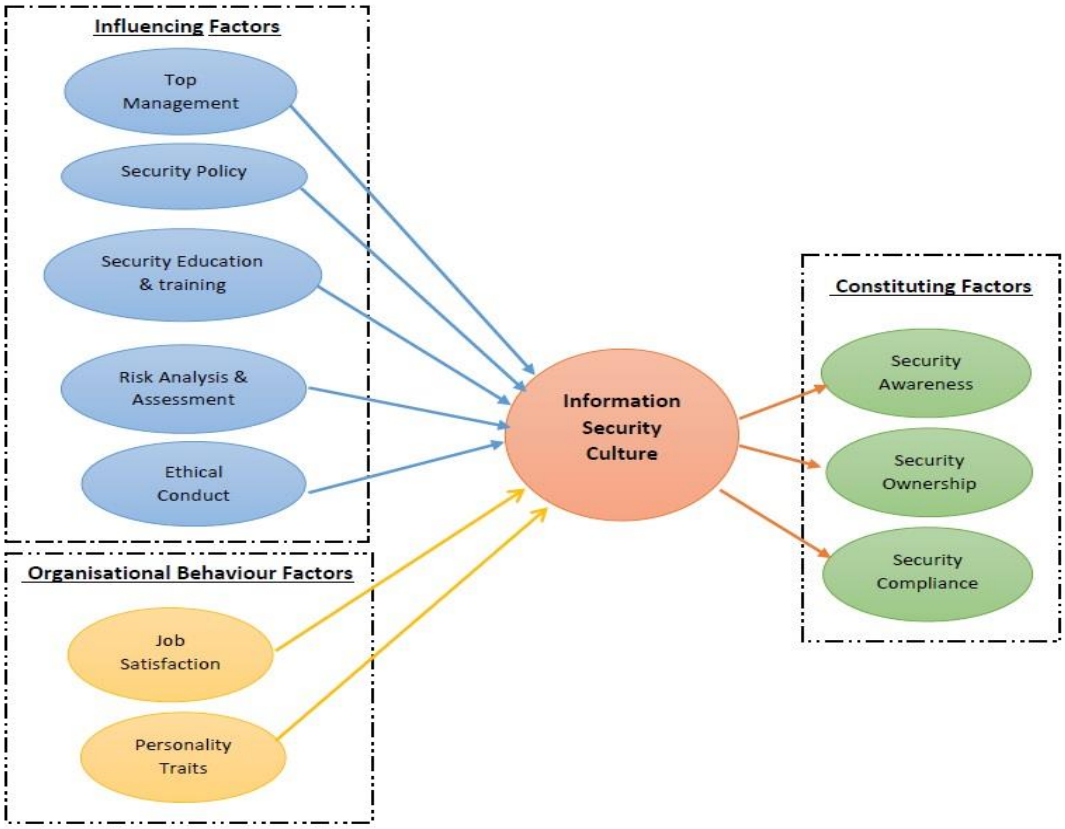



**Figure 5.1: The proposed Information Security Culture and key Factors Framework (ISCFF)**

*5.3.1.1.1 The Influencing Constructs/Factors*

The framework of this research has three categories, and this is the first category. Based on the literature review analysis, this category consists of five various constructs/factors, that positively influences the information security culture are the following:

- **Top Management**: Top management refers the senior leadership and how it understands the importance of the information security function. Also, if there is an understanding of how to involve information security activities for improving and establishing a strong information security culture (Knapp 2005; Martin & Da Veiga 2015; Sas et al. 2020). Top management is responsible for defining and communicating a security policy, user training, specification of employee responsibilities, promoting a security-aware culture (Fourie 2003). The involvement and support of top management leads to the success and effectiveness of information security in organisations. The support from top management helps to form the desired culture and predicts the quality of the information security culture (Dojkovski et al. 2007; Martin & Da Veiga 2015; Nasir et al. 2018).

- **Security Policy**: The security policy defined as a written document, which specifies the strategies and requirements of the information security approach and is connected to general policies that guide both management and employee's behaviour (Fulford & Doherty 2003). The security policy helps to create a consensus for the organisation's security. It combines with knowledge of how data and information is protected (Dhillon 2007). Having an effective security policy of positively affects the understanding of what is deemed responsible and acceptable behaviour to ensure a safe environment in the organisation (Da Veiga 2015; Knapp et al. 2006). When organisations build consistent security policy, the information security culture will be integrated into the daily work routines. This will develop awareness in employees of the need for a secure environment (Hovav & D'Arcy 2012; Da Veiga & Martins 2015).

- **Security Education and Training**: An organisation can develop a culture of information security through advanced security education and training (Da Veiga & Eloff 2010; Hassan & Ismail 2012). In order to reduce risks to information assets and to improve the awareness of employees, a security education and training is necessary. Employees need to develop security skills in order to perform required security procedures (D'Arcy & Greene 2009). The implementation of security education and training programs define achievable roles and responsibilities in the development of the information security culture (Nasir et al. 2018; Van Niekerk & Von Solms 2005).

- **Risk Analysis and Assessment**: The security risk analysis and assessment help organisations and its employees to raise awareness understand potential damage to security (Da Veiga & Eloff 2010). It is important to adopt 'countermeasures' that are adequate to decrease the probability of loss or the effect of loss to an acceptable level' (Caelli et al. 1989). Increased levels of security risk can lead to a reduction of risky behaviour by employees. Also, security risk assessment influences the overall understanding and potential acceptance of the need for security that subsequently influence the culture of information security (Alnatheer et al. 2012; Martins & Eloff 2002; Nasir et al. 2018).

- **Ethical Conduct**: The code of ethical conduct in an organisation is one of the foundations of information security culture. It refers to the values and rules that help to distinguish what is accepted a correct by the organisation (Hellriegal et al. 1998). An ethical code guides and supports employee behaviour and helps to ensure the security

of information. It outlines what is acceptable, by the organisation, as the right way of doing things (Flowerday & Von Solms 2006; Martins & Eloff 2002). The ethical codes can also 'facilitate responsible security awareness, as users are held personally responsible for ensuring sound security practices are implemented, reducing the security risks' (Mears & Von Solms, 2004 (p.5)). An ethical code encourages employees to integrate ethical behaviour that relates to the security of information into their daily working day (Alnatheer et al. 2012; Da Veiga & Martins 2015; OECD 2005). In short, the ethical code defines the actions that are deemed to be ethical and supports.

*5.3.1.1.2 The Organisational Behavioural Constructs/Factors*

The second category consists of two constructs/factors: personality traits and job satisfaction.

- **Personality Traits**: Personality traits describe and understand personality factors, and the potential effects (Mcbride et al. 2012). This helps the understanding of the variability between individuals and possible underlying psychological mechanisms, which might affect user behaviour (Stankovet al. 1995). The big Five Factor Model (FFM) of personality traits are used extensively in psychology to describe, understand and measure the human personality and predict various factors in diverse and complex environments (McCrae & John 1992; Shropshire et al. 2006). The model includes five factors: openness, agreeableness, extraversion, conscientiousness and neuroticism (John & Srivastava 1999). Personality tests are often used at recruitment level in many organisations. Personality test helps organisations on how to moderate the effectiveness of attitudes on use behaviour. The result from the personality test could provide a predictive value for security behaviour in organisations (Gabriel & Furnell 2011). Shropshire et al. (2006) and McCormac et al. (2017), indicated that the five personality traits have an impact on information policy and user compliance, which explained variance in individual security awareness. Furthermore, there is a strong correlation between the information security culture and security awareness. McCormac et al. (2017) considered the impact of personality on the security awareness and postulated a potential link between the personality traits and the information security culture.

- **Job Satisfaction**: Job satisfaction refers to the overall sentiment of 'well-being' in the workplace (Ang et al. 2003). Employees who report positive feelings are more likely to work well with the policies of their organisation, as their improved engagement

allows them to interact directly with their individual and collective responsibilities (Farokhi et al. 2016). Job satisfaction helps to determine how the employee could adapt to situational factors, such as remaining committed and not opting for easier options, which could prove detrimental to the organisation (Greene & D'Arcy 2010). Furthermore, there is a strong correlation between the information security culture, security compliance and the behavioural role of employees. Greene and D'Arcy (2010) indicated that the higher job satisfaction motivates employee to comply with security requirements. Therefore, this research postulates that there is a potential link between job satisfaction and the information security culture.

*5.3.1.1.3 The Constituting Constructs/Factors*

Based on the literature review analysis and Alnatheers' model of security culture, the third category of information security culture comprises of three reflective constructs/factors which are the following:

- **Security Awareness**: Security awareness refers to user awareness of potential information security-related issues and personal responsibilities with regard to security. Awareness often leads to the commitment to the ideal (Siponen 2000). Security awareness is a necessary part of information security protection. Awareness helps to embed compliance in line with the information security requirements of organisations (Dhillion 2007; Parsons et al. 2017). Security awareness must be a priority for an organisation in order to effectively manage and control information security and the culture of information security (Da Veiga 2015; Wiley et al. 2020).

- **Security Ownership**: Security ownership refers to how employees view their responsibilities, roles and willingness to enhance their own security performance, and to prevent and detect the security breaches (Alnatheer et al. 2012; Chia et al. 2002). When employees have a sense of ownership and responsibility for security practice, the employees will behave in a secure manner to protect the organisational information assets. This sense of ownership is vital in the cultivation of information security culture (Ruighaver et al. 2006; Sas et al. 2020; Walton 2015).

- **Security Compliance**: Security compliance refers to how employee behaviour complies with security policy, regulations and practice. Compliance is necessary to reduce security breaches caused by employee behaviour. It is a significant factor in the

information security culture of an organisation (Alnatheer 2014; Eloff & Eloff 2005; Schlienger & Teufel 2003). It is a vital factor as the information security culture influences employee behaviour in relation to official security policy compliance (Da Veiga & Eloff 2008; Masrek et al. 2017). Security compliance ensures that the organisation and its employees follow the international and national laws and regulations, related to the protection of information (Da Veiga & Eloff 2007).

### 5.3.2 The Interaction between Framework Components

The proposed ISCFF demonstrates the most critical success factors to be considered in order to improve the security of information assets and measure the information security culture in organisations. In the proposed framework, there is a clear distinction between factors constituting the information security culture (security awareness, security ownership and security compliance), factors influencing information security culture (top management, security policy, information security education and training, risk assessment and analysis, and ethical conduct) and new factors related to human behaviour (personality traits and job satisfaction). These factors influence the effectiveness of information security culture.

Each factor consists of a number of tasks/items that should be implemented in order to create or assess the information security culture in organisations. These tasks/items for each factor will have a direct impact on the emerging information security culture. At the same time, the information security culture will influence some components. These tasks/items will be identified based on controls suggested by various studies and the outcome from the qualitative phase of this research. More details about the relationship between these items and factors will be discussed later in Chapter 7, section (7.2.1).

There is strong evidence that the identified factors derived from the literature review analyses have a positive influence on the information security culture. For instance, several researchers have indicated the importance of top management commitment and involvement in the cultivation of information security culture (D'Arcy & Greene 2009; Knapp. et al. 2007; Martins & Da Veiga 2015; Nasir et al. 2019; Schlienger & Teufel 2003). Others revealed the strong influence of security policy on the creation of information security culture (Alnatheer et al. 2012; Da Veiga 2015; Knapp. et al. 2007; Masrek et al. 2017). Security education and training could also influence the cultivation of information security culture (Knapp. et al. 2007; Martin & Da Veiga 2015; Nasir et al. 2019; Schlienger & Teufel 2003). Finally, Alnatheer et al.

(2012), Martins and Eloff (2002) and Tarimo (2006) found that the ethical conduct policies are an important factor that influences information security culture. These factors have a positive influence on each other and in turn have a positive influence on the information security culture. At the same time, the information security culture will have an influence on some factors. The possible relationships between the factors will be tested statistically in order to determine whether the proposed information security culture framework is valid.

## 5.4 The Information Security Culture and key Factors Framework (ISCFF) Application Example

The main objective of this framework is to inculcate good information security assumptions, beliefs, knowledge and behaviour in employees to protect information assets. This may be achieved through implementing the main factors of framework in this research. This ISCFF could be used by security managers and practitioners to cultivate or measure the information security culture in organisations. It could also be used to monitor and create positive employee behaviour, thereby reducing threats that the employee might pose to information assets. The research framework will provide approaches for guidelines implementation of required information security culture factors. These guidelines will be targeted appropriate security practices of employee behaviour and inculcate an acceptable level of information security culture. This is achieved by providing a comprehensive view of important factors that have to consider and implement.

For example, if there is a start-up company ABC and they wish to create a strong information security culture from the outset. The ISCFF will provide guidelines and will assist the management in the development of important aspects of information security that will lead to the creation of information security culture. In order to cultivate an effective information security culture, a number of tasks/items under each factor will be considered and implemented. Management would consider these items under each factor beginning with top management support tasks.

- **Top Management:** It is imperative that senior management demonstrates clear commitment and support for a security culture through their words and actions. Top management is responsible for defining, implementing and revising security policies. Management should adhere to the security policies in order to send a strong message to the employees that there is full management support and commitment to security.

Sufficient time, money and other resources must be provided to ensure the protection of information assets. Management support will establish patterns behaviours that reflect accountability, professionalism and integrity in dealing with security issues. This may involve adjustments to the physical environment in order to cultivate a security conscious culture.

Furthermore, management should provide an efficient communications system in the organisation. Poor communications can lead to confusion and non-compliance of orgainstional policies. A top/down, bottom/up communication system would allow for interaction between all levels of staff. It would highlight issues that may arise due to mis-understanding or practical implementation difficulties. Such a communication system would allow employee to feedback ideas and involve them in the decision-making process. This will lead to have a sense of ownership among employees and encourage employees to behave in a supportive manner. An efficient communications system provides a variety of communication channels to prompt and assess levels of security awareness among employees, for example SMS notifications, emails, posters, brochures, newsletter, seminars and so forth.

- **Security Policy:** the company should have a written information security policies and guidelines, that should be clearly defined. This security policy should reflect the company objectives and be reviewed and updated periodically. The manager should make sure that all employees know the security policy of a company through a communication channel by doing, for example, an induction day and training program. This helps employees to know and understand the information security rules and policy. When security policy integrated into the daily work routines, it will positively affect the understanding of what is deemed responsible and acceptable behaviour. Hence, this will develop awareness and compliance in employees.

- **Security Education and Training:** Security training and education program is an essential tool in achieving an effective information security culture. The implementation of security education and training define achievable roles, responsibilities and develop security skills, which lead to improve the awareness and reduce risks to information assets. Employees should be educated and alerted about information security policy, controls, risks, dangers inherent in the environment around the information assets, and the information security requirements and benefits. They should be educated about their security related roles, their responsibilities and trained

of how to behave securely as well to explain what is expected from them. Employees should also be trained for the effective use of different information security-related application and procedures. Security education and training initiatives should be continuous and regular to respond to emerging threats. Also, a company should have a continuous, ongoing security awareness program. There are various methods of education and training that could be used, such as courses, presentations, newsletter and self-study in security applications.

- **Security Risk Analysis and Assessment:** The risk analysis and assessment help employees to be able to recognise and aware of the potential damages to security. The company should have ICT risk assessment team that perform a regular risk analysis and assessment to information security, in order to reduce the probability of loss or impact loss to the acceptable level. This helps to manage the security risks and implements the right countermeasure and controls to protect the information assets from any risks. This team should alert employees regularly about the risks and dangers inherited in the environment around the information assets. This would impact on understanding or acceptance of security beliefs of employees, which subsequently influence the effectiveness of information security culture.

- **Ethical Code:** Standards of ethical behaviour, which show clearly the values and principles of the company need to be developed, structured and translated into a corporate code of conduct. This code of conduct would establish ‘moral’ code of behaviour for all employees. It would outline ethical and non-ethical actions. It would reduce the possibility of the invasion of privacy risks and the potential to altered private data. Under the ethical policy, employees will, respect the privacy of company information, be held accountable in an appropriate manner for their actions, and behave ethically in their working day. It would facilitate ethical behavior and responsible security awareness, which will reduce security risks.

- **Job Satisfaction:** A company should have efforts to create a work environment where employees are satisfied and happy with their jobs. The Job satisfaction helps in determining how the employee could adapt to situational factors, such as remaining committed and not opting for easier options, which could prove detrimental to an organisation. A company also should enhance the company’s security posture by increasing security compliance among the company members and improve the overall

quality of life in the company. So, the company will have more satisfied employees and their willingness to fulfil job responsibilities, such as following corporate rules, policies and guidelines specified in their job descriptions. Thus, the employees will comply with company security policies and procedures.

- **Personality traits:** It will be essential for ABC company to understand the personality and characteristics of their employees and understand the underlying psychological mechanisms that might impact employee behaviour toward the information security. The company should use personality traits model, such as Five Factor Model (FFM), in order to understand and measure their employee's personality. Personality test will support the company to predict numerous factors that may affect the employee compliance with information security. Also, personality test will help a company in identifying areas where improvement might be required, and this could facilitate the development of security education and training programs. Security education and training programs could then be individualised and presented in a manner that matches the employee's personality profile and learning style, in an effort to maximise learning outcomes.

All the previous aspects shall help in establishing an adequate level of information security culture. At this stage, the employee must be aware of the importance of information security in a company. They should be aware of security policies, security requirements, their roles, and their responsibilities toward information security. Also, the level of their security knowledge, skills and performance will increase, which lead employees to have a sense of ownership and be responsible for security practice. The security compliance behaviour with the security policy of the company will increase. All these three factors will reflect a strong information security culture inside ABC company.

Another example would be for a company DEF, that wants to measure or assess their particular information security culture. This ISCFF would help the company to define the current level of information security culture and the future goals by identifying whether the information security culture is on an adequate level. ISCFF will help to diagnosis the security issues and prepare plans for improvements opportunities, in order to provide a protection of information assets. It will help the company to assess employees' perception of information security and identify aspects that require more attention. It will help to monitor and evaluate how changes and performance improve. It will also increase awareness of information security culture while

raising the company's commitment to make employees more connected to the process. This research will develop a questionnaire that provides a view of the company's performance in relation to its information security culture. The questionnaire contains statements that evaluate and assess factors against its tasks/items that will be presented in Chapter 7, section (7.2.1). These factors need to be considered and implemented for improving the level of information security culture in organisations.

For instance, the questionnaire results could help the management to determine whether its information security awareness programme had the desired or expected impact. When departmental security education and training sessions are conducted to explain security policy and requirements, management could easily detect that these have been effective when the questionnaire results of topics covered in the security education and training sessions improve significantly from one assessment session to the next. Furthermore, the questionnaire could help to determine specific areas of concern among a particular group of employees. For example, when mmanagement would like to determine whether IT employees find the information security policy easier to understand than do Human Resources employees, or whether the problem is that the security policy is not communicated productively to employees.

## 5.5 Conclusion

This chapter has presented a general overview of the limitations of existing studies that lead to identifying the information security culture factors, that have not previously been considered in the current studies. In general, it indicated that there is a lack of systemic treatment, understanding and measuring the information security culture. There is the need for developing a comprehensive reliable and valid framework that incorporates human behaviour in order to improve the protection of information assets and guide in creating and assessing information security culture. As a result, this research proposed a comprehensive framework that combine all important factors, which positively influence the effectiveness of information security culture. These factors should be considered to avoid insiders' threats to information security in the organisation. The Information Security Culture and key Factors framework (ISCFF) consists of three main categories comprising:

- Influential factors, which incorporates five sub-factors: top management support, security policy, security education and training, security risk analysis and assessment, ethical conduct.

- Organisational behaviour factors, that incorporates two sub-factors: personality traits and job satisfaction.

- Information security culture factors, which incorporates three sub-factors: security awareness, security ownership and security compliance.

These sub-factors appear to be considered as part of information security culture conceptualisation. By understanding the influential factors or reflection factors, it is possible to help in directing the interaction of humans with information security.

# Chapter Six :

# Formulation of the ISCFF: Qualitative Interviews

## 6.1 Introduction

The design, data collection, analysis and findings of the qualitative data for the current research are presented in this chapter. The initial section describes the overall goals from the qualitative interviews. The second section presents the development and guide design for the interviews. The third section presents the pilot study and analysis results, which was conducted in order to ensure better levels of reliability and validity. Next section describes the interview method sampling and population. Then, a section provides the interview process and administration in this research. The following section presents and details the data analysis and techniques that used in order to form a view of information security culture and important factors. The next section details the interview findings that provide specification of the factors that reflecting and influencing information security culture. There follows a discussion of ISCFF constructs, developments and hypothesis. Final section presents the chapter conclusion.

## 6.2 Overview

The conceptual ISCFF for information security culture was developed following a detailed review and analysis of the literature. One of this research objectives is to understand the relevance of identified factors and their relationship with each other. The use of the interviews would allow for an in-depth understanding of identified factors affecting the information security culture and reveal which factors viewed as more important in the organisation from the perspective of participants. Therefore, the main purpose of the qualitative exploratory study phase was to advance the ISCFF by determining whether all the ten identified factors in the current research framework are significant for an organisation; and whether any new factors should be incorporated into the current research framework. The exploratory qualitative interviews assisted the development of the potential framework for the information security culture. This included signifying the importance of different identified factors in this research that reflect the information security culture; and those that are influential for implementation of an information security culture. The identified factors in this research will be additionally tested in the subsequent phase of the survey questionnaires in order to validate it.

## 6.3 Development of the Interview Guide

In order to conduct a successful interview, it vital to design an interview guide (Gill et al. 2008). The interview guide is used as a general direction for interviewees to make sure covering all

topics and issues that needed in order to achieve the research goals. The interview guide supports in maintaining the interview structure; the data consistency; and reduces bias. The current research designed an interview guide in order to direct the interview process and to maintain the sequence of questions and a data consistency level during each interview.

One of the current research aims is to understand the relevance of identified factors and their relationship with each other that could potentially assist in the information security culture measurements and its development. Accordingly, the questions for the interview were developed in the interview guide from these different perspectives. The interview guide was divided into four parts. Part one relates to the demographics and a general overview of interviewees in respect of their represented organisations, which helps to determine how the participants work within information security measures. This included their levels of experience and what their main roles/ or services are in relation to it. The other three parts of the interview consist of a variety of questions that function with open-ended answers. The open-ended questions enable more in-depth responses from the participants, which improves the richness of data. Thus, the other three parts of interview would enable further exploration into the information security culture, how different organisations manage it and the behaviour of employees. The final part enabled interviewees with adequate time to construct individual interpretations about other issues that have not been discussed. From the base of relevant literature and research's framework, a specific series of questions guide the interviews (See Appendix E), while the questions are placed into the four individual parts as follows:

- **Part One** – Introductory questions that determine the interviewees' specific employment details.

- **Part Two** – Two questions that relate to the security practices of organisations, in order to present information regarding information security's measures and controls; how employees are educated and acquire the awareness of related security regulations through their organisation.

- **Part Three** – This part includes three questions. Two questions relating to employee security behaviour patterns in organisations and the most effective of security practices on employee behaviours. The third question relating to how an effective information security culture should operate in organisations and determines main factors that have a positive influence on information security culture.

- **Part Four** – Two broad questions relating to the improvements that may have a positive effect on the security culture in the organisation. This part provides interviewees with the opportunity to construct individual interpretations and consider new topics that have not been addressed. This helps to develop a more conclusive perception of an organisational security culture.

Specifically, designed questions help to reduce potential bias, and the interview guide, helps to maintain neutrality. Following the interviewee responses, appropriate supplementary or for clarification were used. Consequently, interviewees were able to discuss relevant themes with the interviewer, which assists in the acquisition of in-depth knowledge. Table 6.1 demonstrates the open-ended interview guide questions and their linkage to the research objectives.

**Table 6.1: The Interview Guide Questions and their Linkage to the Research Objectives**

| Research Objectives | Interview Guide Questions |
|---|---|
| 1- To explore and evaluate the conceptualisation of information security culture and the importance of implementation in an organisation. | 1- Do you have any information security education and training courses in your organisation? If yes, what are the different methods of security awareness and training sessions you get in your organisation?<br>2- Do you get regular information about risks and dangers inherent in your work?<br>3- In your opinion, what would an effective security culture look like in your organisation?<br>4- What changes or improvements would you think that might have the most positive impact upon the security culture in the organisation? |
| 1- To identify the critical success factors that have a direct influence or constitute information security culture components.<br>2- To identify any other security factors that could have a direct influence on the information security culture. | 6- What do you consider the main contributory factors in term of creating and implementing an effective security culture in your organisation?<br>7- What do you consider the main barriers or obstacles to achieving improved security compliance in the organisation? |

## 6.4 Pilot Study Interview Guide

In order to ensure that the interview guide was appropriate to this research and to make sure that it would not present any additional difficulties, the interview guide was initially tested through conducting a pilot study. The pilot study ensured that the interview guide was suitable and informs the research method. The pilot study was conducted with three professionals in information security, who works in a Saudi Arabia public education institution. Test interviews were conducted to ensure that the interview guide was appropriate, no questions were repeated,

and the participants could understand them clearly without creating bias. Also, the pilot study assisted in ensuring and measuring the content validity of the questions used and that information gathered would be relevant to the research objectives.

### 6.4.1 Analysis and Results of the Pilot Study

Respondents were able understand the context and the questions, because they worked with information security department in their organisations. A broad level of questioning was included that directed open responses in relation to the different framework components and perceptions into the information security and related topics. The interview protocol directed this process and resulted in-depth level of data collection. During the pilot study gaps became evident, between the initial questions and the data required. Consequently, the interview guide was changed. It was separated into four groups of questions in order to incorporate the information from respondents arising from the interviews. In this way a more coherent set of questions were developed that complemented each other and related directly to the research objectives.

Certain questions or wording needed to be changed for greater clarity. For example, within the third group of questions, a specific question (C-2) was changed to provide an evaluation of various dimensions within the research framework and rank their level of importance by choosing number one for an option of highest priority, two for the next priority and so on, as presented in Table 6.2. The final interviews included four general questions; three questions to evaluate and rank the relative importance of information security topics; and six open-ended questions. The pilot study produced an easily directed set of interviews that could be completed efficiently. The final interview guide of this research is presented in Appendix E.

**Table 6.2: Interview Question (C-2)**

| The Original Question | The Modified Question |
|---|---|
| (C-2): In your view, what are the effects of the following information security practices on the security-related behaviours of employees inside an organisation?<br><br>Top Management commitment (e.g., management gives a strong consistence to support to security program). | (C-2): What do you consider to be the most effective of the following security practices on the security-related behaviours of employees in an organisation? (Please rank it in order of effectiveness.) |

| The Original Question | The Modified Question |
|---|---|
| IT department initiatives in your organisation (e.g. policies, procedures, guidelines, risk analysis, education and training program).<br><br>Information security technical countermeasure (e.g. Anti-viruses software, firewall and intrusion detection).<br>Personal values and beliefs (culture) about information security. | Top Management commitment (e.g. management gives a strong guidance to support to security program).<br><br>IT department initiatives in your organisation (e.g. have clear policies, procedures, guidelines, risk analysis, education and training program).<br>Information security technical countermeasure (e.g. Anti-viruses software, firewall and intrusion detection).<br><br>Personal values and beliefs (culture) about the information security. |

## 6.5 Interview Sampling

The aim of the sampling is to produce reasonably accurate findings without the need for collecting data from every member of a research population. The selection of the sample should be done by a probability or non-probability method when selecting the sample. The non-probability sampling means that the researcher selects informants knowingly for a different reason because of sufficient experience or knowledge of the subject might not occur in the general population. This method allows to select individuals and sites that are available, convenient, and represent some characteristics the researcher wants to study (Ary et al. 2002; Cresswell 2008). Most qualitative studies select non-probability sampling method when the research does not intend to generalise the findings, but rather to gain an in-depth understanding of the main phenomenon (Creswell 2008). As the point of the interviews in this research was, to gather insight and information related to the main identified factors affecting the information security culture, non-probability sampling was used.

Techniques used for this research were, purposive sampling and snowball sampling. Purposive sampling method allows to be hand-picked basis on their relevance and knowledge. So, they might provide valuable data related to the subjects of the research (Cohen et al. 2013). In this research, IT/ security specialist working the area of information security were selected in order to explore and discuss the opinions and perceptions of key security practices and information security culture in their organisations.

Collecting and access to the specific people is not easy and requires inner relationship inside the organisation especially with this form of research. The topic of information security is considered sensitive as it is linked to rules and regulations of security management, it is difficult to accumulate a good number of responses. There were certain access difficulties to appropriate people in this research. Due to the sensitives of the current topic and the researcher had no experience in working in the cyber security field, there were no initial acquaintances within those IT/ Security specialists.

The snowball sampling technique is useful when it is difficult to identify appropriate participants (Bryman 2015). This difficulty was also applied to the current research. The snowball sampling includes selecting those cases that are easiest to reach where the selection process is continued until the defined sample size has been reached, however there are no clear requirements for the sample size (Saunders et al. 2011). This technique is based on the researcher makes initial contact with a small group of people who are relevant to the research topic and then uses these to establish contacts with others. Therefore, a snowballing technique was used to recruit the participants for this research.

The selection of a target population for the research is a main part of any research success (Baker 1994). In this research, the selection of people from organisations for the interview sample had to be from numerous sectors and industries, in order to develop better comprehension of information security culture and to confirm the importance of the identified factors, relevant to the proposed framework. As this would help to provide analysis from different backgrounds and produce new findings in order to progress the research. Each industry could require different levels of information security culture. Therefore, organisations from industries such as education, law, insurance and mining were interviewed. The interviewed organisations were from a range of sectors and environments including public, private and semi-public companies. The current research varied the size of each organisation using the criteria of the United States International Trade Commission. For example, small and medium organisations (SME) have fewer than 500 employees, while large organisations have greater numbers than 500 and more (Okun et al. 2010). However, access issues in this research did not allow it to reach a quantity balance between small and medium organisations and large organisations. This research had organisations ranged in size from small to large. Five organisations were large, and two organisations were small and medium enterprise (SME). The representative sample of organisations was finally achieved.

The initial choice of location was in the United Kingdom, due to the research's location. Eight hundred organisations from a range of sectors were invited to participate through an invitation letter (See Appendix E). Access to appropriate organisations was difficult for this research. Some organisations refused to participate because of the restricted rules and regulations of discussing their security management to a third party, or to work commitments. Only one organisation – a law firm- agreed to take part in this study. The researcher then approached delegates to the ninth Secure South West (SSW9) conference hosted by Plymouth University. Delegates were given a one-page invitation flyer that explained the purpose of the study (See Appendix D). However, only one further respondent from an education institute had interest in participating in this study.

The low level of response resulted in an invitation e-mail sent to international organisations in Saudi Arabia and the United State of America. These organisations had cooperated in academic research in the past. Ultimately, seven organisations: two in the United Kingdom, one in the United State of America, and four in Saudi Arabia participated in this research. The respondents were from the private, public and semi-public sectors, and included various industries - four in education, one in insurance, one in law, and one in mining. These organisations have the security infrastructure in place; have technology adoption and used information security management practices. In addition, the diversity of geographical locations was considered a positive as it would assist in advancing the understanding of the information security culture phenomenon from different contexts and environments.

However, selecting and specifying the exact number of a sample size could be a complex task. The sample size depended on saturation being reached when no new knowledge is collected (Guest et al. 2006). Saturation is usually achieved around twelve interviews (Guest et al. 2006). The aim of this research was to acquire an in-depth information from those who are work in IT or security department in organisations in order to confirm the identified factors of more critical importance within organisations in this research. Thus, there was no restriction in sample size and how large the size of the sample should be.

There are methods that could be used to decide the right sample size for the research. The methods for calculating the sample size are divided into statistical, pragmatic, and cumulative (Denscombe 2014). The cumulative sizing is usually connected with qualitative studies of a smaller scale. The sample in this method is increased until the researcher feels that sufficient information has been gathered and the increase in the sample size would not provide more

relevant information (Denscombe 2014). Therefore, this research applied cumulative sizing for the interviews as the sample size is relatively small. This research aims to interview ten to thirteen people in order to answer the achieve research objectives.

A semi-structured interview was used in an exploratory manner. This exploration could provide indications of the validity of factors intended in the ISCFF. Access to people with relevant knowledge and experience of organisations' security was difficult, nevertheless, thirteen IT/Security specialist from seven different organisations located in three different countries agreed to patriciate in the interview. Their experience and knowledge yield rich data. Table 6.3 below lists the demographic features, for participant organisations in this stage of the research. Each organisation was abbreviated by a specific symbol. For example, the first organisation was denoted as organisation A and the second organisation as organisation B, etc.

**Table 6.3: Demographic Profile of Organisation**

| Org | Type | Size | Location | Sector | No. of | Interviewees Position |
|---|---|---|---|---|---|---|
| A | Public | 4000 | SA | Education | 3 | IT assistance director and IT Specialists |
| B | Public | 5000 | SA | Education | 2 | IT Specialists |
| C | Private | 6000 | USA | Education | 2 | IT Specialists |
| D | Public | 5000 | UK | Education | 1 | Enterprise security architect |
| E | Private | 400 | SA | Insurance | 3 | IT supervisor and IT specialists |
| F | Semi-Public | 4000 | SA | Mining | 1 | Security manger |
| G | Private | 1500 | UK | Law | 1 | Security manger |
| **Total** | | | | | 13 | |

Note: Org: Organisation, SA: Saudi Arabia, UK: United Kingdom, USA: United State of America, IT: Information Technology

## 6.6 Interview Process

The ethical issues were considered as part of the research methodology. Prior to interview, respondents were advised of reasons for the research and its potential risks and benefits. Then, the constant form and interview questions sheets were provided to the interviewees. Interviewees were informed of their rights to the transcripts and results. Confidentiality and anonymity were assured by not using their name or company name. Once interviewees were comfortable and willing to continue, they should sign the constant form and return it back to

the researcher. In addition, the interviews should not continue if new insights, perceptions or ideas fail to be found, or if the interviews merely start to repeat prior analysed conclusions. Hence, when an interview fails to provide innovative data, a certain level of saturation can be determined to have been reached. The interview process adhered Plymouth University Ethical Principles for Research Involving Human Participants.

The process that follows in this research to conduct the interview are the following: a researcher first established a key contact person in each chosen organisation. A contact list was established between the researcher and the key contact person in each chosen organisation. Interviewees were selected on the basis of the role they played within the organisation in terms of information security management. Second, respondents were nominated by the key contact person in their organisation and they were contacted by the researcher. Next, a researcher emailed them and introduced the purpose of the interview. Then, the researcher set the interview dates and times in advance, as guided by the availability of the interviewees, who generally worked as security managers or as IT/security experts within their respective organisations. Table **6.4** illustrates a summary of the interview process in this research.

**Table 6.4: A Summary of the Interview Process**

| # | Steps |
|---|---|
| 1 | Establish an initial contact with the interviewee. |
| 2 | Email the interviewee to schedule the interview. |
| 3 | Establish date and time based on interviewee availability. |
| 4 | Conduct the interview (on-site or Skype) based on the interviewee preference. |
| 5 | Transcribe the interview. |
| 6 | Allow access to the interview transcripts and study's findings for participants. |

Thirteen semi-structured interviews were conducted with IT/ security specialists from seven individual organisations (one education institute and one law company in the United Kingdom, one education institute in the United State of America, two educations institutes, one insurance company and one mining company in Saudi Arabia). Individual face-to-face and online interviews were conducted (between October 2017 and January 2018) in order establish trust and to collect thorough, meaningful information from participants.

Due to the geographical distribution of the sample and the physical distance between the researcher and participant organisations, it would not be time-efficient or economical to conduct face-to-face interviews for some participants. These interviews were conducted by visiting the site or by meetings online using Voice over IP technologies such as Skype. Using Skype for interviewing participants was convenient in this research. In fact, the Skype interview was just as good as the data gathered using face to face interaction. Moreover, some participants who interviewed over Skype tended to talk for longer and were less worried about time because they felt at home in a comfortable environment. For instance, one of the interviews went on for thirty-five minutes, which produced some very useful information. Both tools provided the same sufficient quality of data.

The interviews were either in English or Arabic depending on the preference of each interviewee. The transcripts were transcribed in English. Twenty to thirty-five minutes was requested from the interviewees to complete each interview at their own convenience. The average time of interviews was twenty-five minutes. Some interviews took longer depending on how the interview was progressing and the interviewee personality. A voice recording machine was used if the participants agreed beforehand, or only hand-written notes were taken if the participants preferred. Certain interviewees refused to have their interviews recorded due to the perceived sensitive nature of the information required, even though the identity of the interviewees and the data were kept confidential. All information that might identify the participants or their organisations is anonymised. Thus, this research does not contain specific information about the organisation and participants. Instead, each participant's response was assigned a sequential number, for example, [A2] (where A2 means participant 2 from organisation A). The interview details are summarised in Table 6.5.

**Table 6.5: Interviews Details**

| Participant | Date | Time | Duration | Location | Type | Language | Participant Position | Recorded |
|---|---|---|---|---|---|---|---|---|
| A1 | 14/12/2017 | 11 a.m. | 20 min | Online | Skype | English | IT assistance director | No |
| A2 | 14/12/2017 | 3 p.m. | 22 min | Online | Skype | Arabic | IT specialist | No |
| A3 | 15/12/2017 | 1 p.m. | 23 min | Online | Skype | Arabic | IT specialist | No |

| Participant | Date | Time | Duration | Location | Type | Language | Participant Position | Recorded |
|---|---|---|---|---|---|---|---|---|
| B1 | 16/12/2017 | 11 a.m. | 26 min | Online | Skype | English | IT specialist | No |
| B2 | 18/12/2017 | 4:00p.m. | 27 min | Online | Skype | English | IT specialist | Yes |
| C1 | 20/01/2018 | 5 p.m. | 23 min | Online | Skype | English | IT specialist | No |
| C2 | 22/01/2018 | 4 p.m. | 35 min | Online | Skype | English | IT specialist | No |
| D1 | 16/10/2017 | 3 p.m. | 28 min | Organisation | F2F | English | Enterprise security architect | Yes |
| E1 | 08/12/2017 | 1 p.m. | 20 min | Online | Skype | English | IT supervisor | No |
| E2 | 08/12/2017 | 10 a.m. | 25 min | Online | Skype | English | IT specialist | No |
| E3 | 10/12/2017 | 4 p.m. | 27 min | Online | Skype | English | IT specialist | No |
| F1 | 13/12/2017 | 2 p.m. | 20 min | Online | Skype | English | Security manger | No |
| G1 | 18/01/2018 | 1 p.m. | 30 min | Online | Skype | English | Security manger | No |

Note: IT: Information Technology

## 6.7 Qualitative Data Analysis - Interviews

This section presents the data analysis process and techniques used in the research. Within the process of conducting qualitative studies, data analysis is one of the most challenging concepts and also one of the least developed processes. Yin (2003) states that data analysis includes the necessity to examine, categorise, test and/or correlate evidence in order to progress a hypothesis. In this research, a content analysis approach was used in order discover themes and patterns in elaborated responses. The collected qualitative data was used and analysed in order to determine different perspectives and to correlate into a research framework.

Also, a within-case analysis strategy was used for data analysis. A within-case analysis commonly involves detailed interviews and transcripts for each interview (Yin 2003). Each

interview helps to provide further insight into framework factors and how different constructs are perceived within contexts in real life situations. These interviews in the current research provided data regarding information security culture in the form of a narrative discussion, instead of an analysed interpretation. When conducting qualitative research, an interpretative approach refers to the researcher's personal views that influence the knowledge base to gain a broader understanding, which is drawn from prior studies and results (Creswell 2008). The broad understanding in the current research was obtained by reviewing the significant findings and comparing personal views with the literature.

However, Yin (2003) states that the procedures of qualitative data analysis include three steps:

1. To select a general strategy that helps to choose which parts to analyse and why specifically;

2. To code the presented evidence;

3. To use an analytical technique, in order to develop or test theories.

These steps are discussed in the sub-sections that follow.

### 6.7.1 General Analytic Strategy

Two analytical strategies are prevalent in qualitative research: firstly, theoretical propositions that help to organise qualitative data; secondly, a strategy to create a descriptive framework that organises the data (Yin 2003). It was important to identify, code, and categorise the data patterns present (Patton 1990). It was decided the second strategy, which categorised and identified different themes that were shown from the data in the transcripts, would be the most suitable. The data analysis process is illustrated in Figure 6.1.

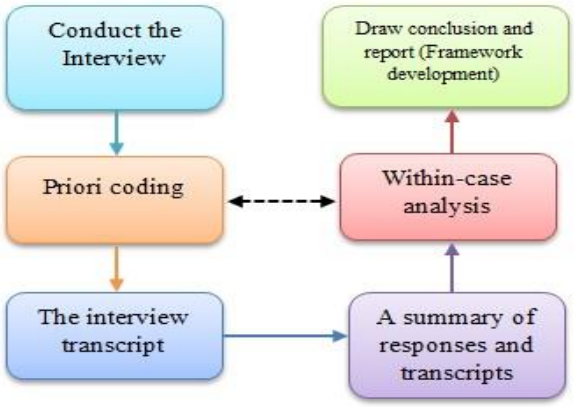



**Figure 6.1: Interview Data Analysis Process**

The interview data analysis process involved four stages:

1. Stage one started with coding theme, with the identification and categorisation of patterns for interview transcript analysis.

2. Stage two aimed to create a clear picture of the responses from the interviewees. This was concerned with the organisation and providing a summary of the transcripts, which included the analytical technique of 'reduction' (Miles & Huberman 1994). All responses questions were combined into a single document.

3. Stage three included the analysis of 'within-cases', summaries of the transcripts and responses summaries.

4. Stage four gave a report of the interviews and arrived at conclusions.

### 6.7.2 Analytic and Coding Techniques

The pattern coding assists in reducing extensive data into more manageable units of analysis. Pattern coding allows for the grouping of summaries into a smaller number of overarching themes or constructs (Miles & Huberman 1994). It represents sets of the emergent codes developed during the data analysis process (Miles & Huberman 1994). Pattern matching is also used to prove the correlation between different concepts, as shown in the conceptual framework (Yin 2003). The pattern matching is important in the process of linking data to propositions and the concepts that have been identified through the conceptual framework. Hence, pattern matching was used in the analysis. Data pieces were taken from the analysis and compared

with all other forms of data to see which parts were similar or different, and thus, data correlations were established (Thorne 2000). The initial stage of the coding process was to identify the key data themes (Oates 2005). In order to summarise the analysed data, three themes were identified.

1. Data irrelevant to the research aims was ignored;
2. The provision of general descriptive information that was required in a case study description.
3. The identification of data that corresponded to the research objectives.

Therefore, this research was directed through the third theme. Units of data, words, phrases or paragraphs were analysed in relation to the research aims. During the analysis, both explicit and implicit results were derived from the data. By coding the data, the qualitative interviews were sufficiently analysed. This was a repetitive process that involved determined consistency and the provision of data links to the constructs of the research model. The data from this repetitive process were subsequently correlated and coded into constructs during the analysis stage. This resulted in counts and data points for further analysis.

Data categories were identified and organised into the main categories corresponding to components of the research's conceptual framework. The main categories that have identified during data analysis are top management, policy, education and training, ethical conduct, risk assessment and analysis, awareness, compliance, ownership and job satisfaction. Interviewee comments were coded under these categories. Comments were analysed at various levels, such as the structure of comments made, the overall content of what was said and the vocabulary that was used. Table 6.6 shows an example of data categorising and Appendix G and Appendix H show a full list of the data categories. Furthermore, the data were analysed by using Microsoft Excel, which helped to demonstrate patterns related to constructs.

**Table 6.6: Example of Data Categorisation**

| Example Excerpt from Interview | Category |
|---|---|
| C-3 (a) In your opinion, what would an effective security culture look like in your organisation? | Policy |

| Example Excerpt from Interview | Category |
|---|---|
| "In order to have an effective security culture, it is absolutely vital for the company to have very clear [policies and procedures] that are clearly described, and everyone must follow "[C6]. | |
| C-3 (b) What do you consider the main contributory factors in term of creating and implementing an effective security culture in your organisation?<br><br>"Excellent [top management] participations and involvement are the most important factors for creating an effective information security culture" [A3]. | Top Management |

## 6.8 Interview Findings

Using the semi-structured interview in an exploratory manner, the participants responded to the four individual parts of questions concerning their organisation's actual practices. The aim was to determine whether or not the ten identified factors within the study's framework are important for organisations. Therefore, the findings of the interviews have been illustrated the relevant signify factors and correlation in regard to the information security culture. There were four general questions; three questions to evaluate the relative importance of information security topics and rank them; and six open-ended questions. The attitude and perception of employees towards the information security culture have been discovered. Data analysis helped to understand the importance of identified factors that relate to the information security culture.

A summary of the findings for each part of the semi-interview questions, which are the employment details, information security culture practices, the employee security behaviour patterns and the perceptions for improving the information security culture are presented in sub-sections that follow. Quotations are used to support and highlight explanation of the findings. Each quotation starts with this symbol " " followed by a specific symbol that denoted for a name of the organisation and the participant number, e.g. " " [A1].

### 6.8.1 Employment Details

This part is an introductory question regarding the number of working years in their current position in order to get the employment details about respondents.

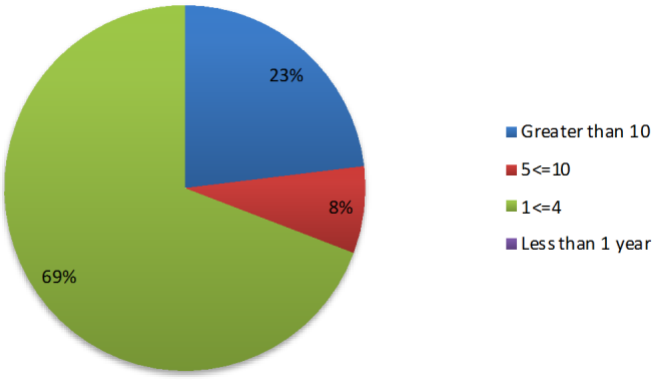



**Figure 6.2: Years of Work Experience for Participants**

Nine of interviewees have work experience between one to four years of experience with their current position and company, as shown in Figure 6.2. Respondents have quite a good degree of understanding of their organisation and provided information in relation to views of information security, its best practices. Also, their responses are credible.

### 6.8.2 Information Security Culture Practices

This section attempts to uncover information regarding security rules, measures and practices; how employees are educated and acquire the awareness of related security regulations and risks inside their organisation.

#### *6.8.2.1 The Main Information Security Practices and Rules Used in the Employee Organisations*

Interviewees provided a range of main security practices and measures that generally used in their organisations.

**Table 6.7: The Main Information Security Practices and Rules Used in Participating Organisations**

| The Main Information Security Practices/Rules in Organisations |
|---|
| Have a well-configured firewall and internet gateway by blocking some websites to prevent any users within the organisation accessing untrusted websites. |

| The Main Information Security Practices/Rules in Organisations |
|---|
| Have a secure configuration for all hardware and software, such as remove any unused software and services or keep it up to date. |
| Install anti-virus or anti-malware products and keep it up to date. |
| Maintain regularly software and computer equipment to keep it running smoothly and fix any security issues. |
| Access control to the organisation system. Each user has own username and passwords and should change the password regularly. |
| Aware the members of organisations about security policies and security problems. |
| Train the members of organisations about security issues. |

The findings indicated that all seven participating organisations use general information security practices and rules such as security policies, security training, physical and technical measures. These aimed to ensure the confidentiality, integrity and availability of organisational systems and services, as summarised in Table 6.7.

#### *6.8.2.2 Security Education and Training Courses in the Organisation*

Of thirteen interviewees, six respondents from organisations in Saudi Arabia and two respondents in the United States of America reported an absence of security education and training programs. Five respondents reported security training courses in their organisations which are two organisations in the United Kingdom and one in Saudi Arabia. The findings are that three of the participating organisations in the United Kingdom and Saudi Arabia such as A, D, G adopt the education and training programs related to information security. A, D and G organisations all had a specific budget for security education and training programs. Each organisation informed their members about information security matters through the induction training. The respondent G1 stated that:

> *"The training session I received was when I first started my work in the company. It covers different security related topics such as security policies, client security, access security and privacy in the organisation"*

#### *6.8.2.3 Methods of Security Awareness and Training Sessions*

Participating organisations use various channels to distribute information on security awareness to employees, such as e-mails, seminar and training courses, text message, posters or via the organisation website. The findings revealed that all seven organisations adopted information security awareness activities. Those activities are accomplished by the IT departments cooperation with the human resource departments.

The comparative analysis suggested some differences in the data sets in this study. In particular, the adopting methods of information security awareness and training differ from one organisation to another. For example, organisation A usually uses e-mails, text message and training sessions to raise aware of any security issues. In organisations B and C, e-mail and posters were the main information security awareness activities used. In organisation D, the main information security awareness methods were email, training courses and displaying security information on the organisation website.

> "*We usually rely on emails system or display the security issues on the information security section on our website to pass on the security awareness. Sometimes, the company go through additional training workshops where new security policies are discussed as are any data breaches that may have happened and challenges that come up in surrounding environment*" [D1].

Organisations E and F used e-mail notification. Organisation G used e-mail, text message, training courses, and display information security on an organisation website.

#### *6.8.2.4 Regular Alerts about Any Risks and Dangers in the Organisation*

The findings showed that five of the participating organisations usually alerted their employees and provided some information about the security risks and any threats inherent in an organisation. Three interviewees from organisation B and G reported that employees are not alert about the security risks or breaches that happen inside their organisations. Ten interviewees from organisations A, C, D, E, F reported that all the members of the organisation

are alerted about any security risks and dangers inherited in the work environment around the information assets.

#### *6.8.2.5 Information Security Level in the Organisation*

Interviewees rated the level of information security in their current organisations in general.

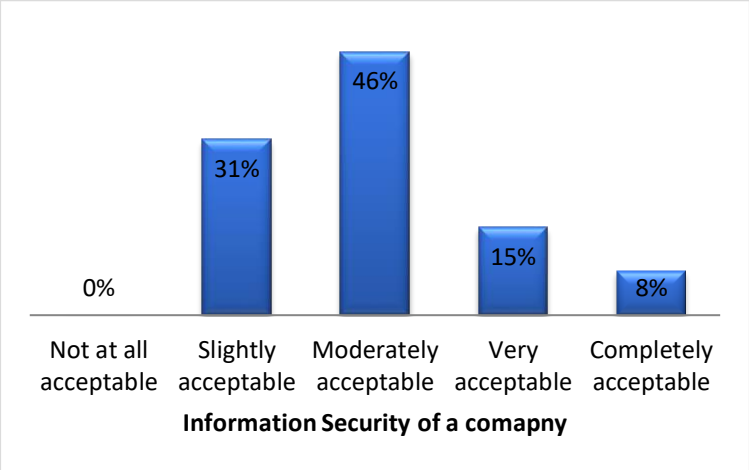



**Figure 6.3: Information Security Level in Organisations**

The data revealed that the overall level of the information security in four participating organisations is a moderately acceptable (see Figure 6.3). Six respondents stated that their organisations have a moderately acceptable level of information security. Four respondents thought that their organisations have a slightly acceptable level of information security. Two respondents claimed that they have a very acceptable level of information security at their organisations. One respondent stated that the level of information security is completely acceptable in his organisation.

### 6.8.3 Employee Security Behaviour Patterns

This section attempts to uncover information regarding the employee's security culture behaviour, knowledge and practices of employees in organisations.

#### *6.8.3.1 Employee General Security Behaviours*

In order to obtain a broad picture of the employees' security behaviour, respondents were asked to rate employee security behaviour with regards to how it reflected what they had told about security responsibilities.

**Figure 6.4: Employee's General Security Behaviour**

Eight respondents stated that the level of employee's security behaviour in their organisations is OK. Whereas four respondents collectively thought that the employee's security behaviour in their organisations is poor or very poor. Only one respondent claimed that the security behaviour of employees in his organisation is good as shown in Figure 6.4.

### *6.8.3.2 The Most Effective Security Practices on Employee Security Behaviour*

Interviewees were asked to rank the levels of effectiveness security practices in their organisations. These security practices include: top management commitment, IT department initiatives, information security technical countermeasure and personal values and beliefs about information security.

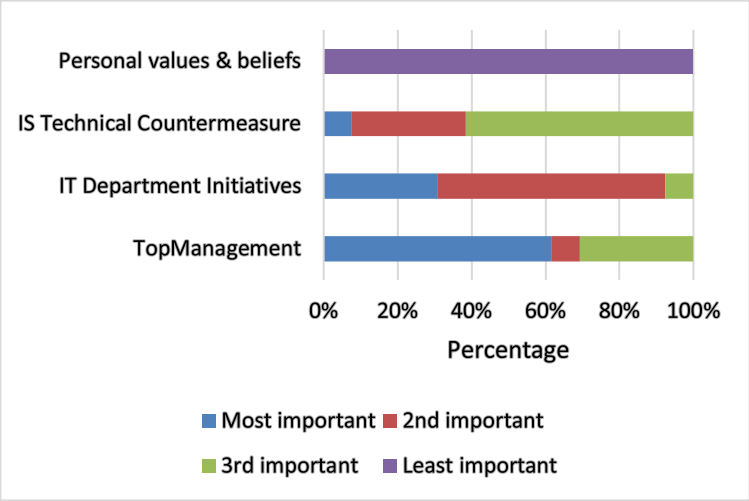



**Figure 6.5: The Most Effective Information Security Practices on Employee Security Behaviour**

Eight respondents rated top management involvement as a first priority. Four respondents rated the IT department initiatives as a second priority. Third priority for the information security technical countermeasure, and last priority for the personal values and beliefs as demonstrated in Figure 6.5.

#### *6.8.3.3 Perceptions of an Effective Information Security Culture*

The participants reported their perceptions of how an effective security culture should operate in organisations.

**Table 6.8: The Participants' Perceptions of Having an Effective Security culture**

| **Perceptions of an Effective Information Security Culture** |
|---|
| Establish training workshops for employees. |
| Develop clear policies and procedures that are clearly described. |
| Increase the awareness and make some creativity into the awareness efforts. |
| Instil a concept that a security belongs to everyone responsibilities in order to enhance the sense of ownership. |
| Active and continuous engagement of security by all levels of leadership and management. |

They made a range of discursive statements that aimed to form an efficient information security culture in the organisation. Responses were grouped under common threads and are summarised in Table 6.8. All thirteen interviewees reported, that establishing and conducting an information security training program for all employees, would be an effective basis for an adequate level of information security culture in their organisation. Nine interviewees affirmed this statement:

> "*Educating employees about the information security to increase their knowledge and make the right decision to have an adequate level of security culture in the organisation. This approach, where you educate the employee, is seen as more conducive to me*" [B1].

The comparative analysis showed differences in the data sets collected in the United Kingdom, the United State of America and Saudi Arabia. Organisations in the United State of America and Saudi Arabia indicated that developing security policies and support from all levels of leadership were the essential elements that could support the development of an effective information security culture. For example, the respondent [F1] asserted about the role played by the security policies in the organisational security culture effectiveness:

> "*Managing the information security according to the security policies and standards will give a base for the organisation to build an effective security culture*".

Respondent [C7] highlighted the top management commitment towards developing a positive information security culture in an organisation:

> "*To create or expect some sort of an efficient security culture, there should be an active, continuous engagement and endorsement of information security by all levels of leadership and managers in a company*".

Respondents in in the United Kingdom and Saudi Arabia stated that developing and increasing security awareness would be a necessary part of security protection that supports in establishing an adequate level of information security culture. Finally, four respondents in Saudi Arabia suggested that enhancing the sense of security ownership in employees would play a vital role in the promotion of an acceptable level of information security culture.

#### *6.8.3.4 The Main Contributory Factors for Establishing an Information Security Culture*

Respondents reported on contributory factors that might have impacts an effective security culture in organisations.

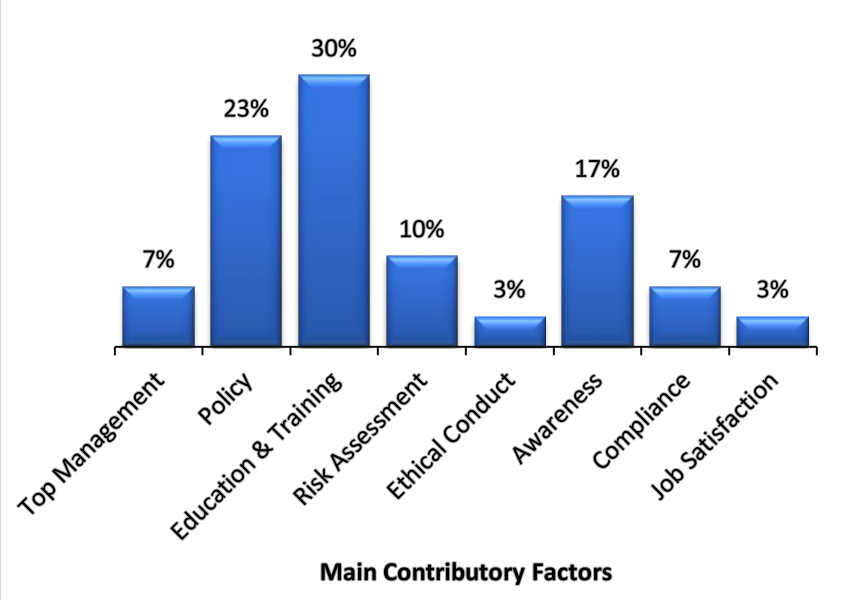



**Figure 6.6: The Main Contributory Factors for Establishing an Effective Security Culture**

Respondents offered factors that they felt should be implemented in the organisation (see Figure 6.6). Nine respondents revealed that developing security education and training sessions for all the member of the company are considered one of the highest contributory factors for establishing the information security culture.

> *"The security training program is one of a success factors for educating members of our company to adopt security and influence the employee behaviour which will lead to establish a security culture in my organisation"* [A2].

Seven respondents from organisations C, E, F and G indicated that developing clear security policies and rules as a second top contributing factor for having an effective information security culture in an organisation. They affirmed the effectiveness impact of a security policy in the information security culture.

> "*Implementing the security policies and guidelines in a company will be efficient because it helps employees to clarify and get a detailed understanding about the company security requirements, and the way to comply with the information security rules*" [E3].

Five respondents from organisations A, C and G mentioned that increasing security awareness among employees is the third factor that supports the information security culture in

organisations. Three respondents from organisations A and E signified that periodical risk analysis and assessment is another important factor to consider in order to improve the information security culture. Two respondents from organisation A and E suggested that information security culture could be effective if there is a support from the top management and leadership at all levels together employee compliance with security policy and procedures of the organisation. One respondent from organisation B stated that understanding ethical obligations of the organisation is an essential to improve the information security culture. Employee job satisfaction was also vital in improving security culture.

There was some agreement among the respondents' perceptions of organisations in the United Kingdom, the United State of America and Saudi Arabia. All thirteen respondents considered that the information security policy and the security awareness are two of the main contributory factors in cultivating the information security culture in organisations. All respondents demonstrated the importance of the security awareness and its impacts on the organisation as the respondent [C6] illustrated that:

> "*It is impossible to achieve our security objectives without employees help. For example, a company should not expect that the employees know everything about the security issues. The company should try to clarify things and aware them about company's policies and employee responsibilities towards the security. This will help a company a lot and their employees in applying the security policy"*

However, the comparative analysis illustrated some differences in the data sets, including data collected in the United Kingdom, the United State of America and Saudi Arabia. For instance, there was some commonality among the respondents' perceptions in the United State of America and Saudi Arabia. Four respondents from organisations A and C in the United State of America and Saudi Arabia signified that the top management support is an effective factor for creating the information security culture in the organisation.

> "*Excellent top management participation and involvement is very important for the security success and improve a security culture in a company*" [A3].

Also, respondents from these two countries, organisations C and E believed that employees' security compliance is one of the contributory factors for developing the information security

culture. They suggested that improving security compliance will change the organisational security culture.

> "*The security culture can be established effectively if all members of the company comply with security policy and regulations*" [E3].

Five respondents from organisations A, B and E in Saudi Arabia considered additional factors such as security risk analysis, ethical conduct and job satisfaction that would contribute to the organisational security culture. One respondent pointed out the importance of implementing risk analysis and assessment in an organisation.

> "*Understanding the risk involved with information security and more importantly conducting periodical risk assessment is vital factors for establishing a security culture environment"* [A3].

Another respondent affirmed the effectiveness of the ethical conduct policies for the advancement of organisational security culture.

> "*Understanding the ethical codes and obligations is an essential key to improve a security culture*" [B4].

One respondent suggested that the job satisfaction could motivate employee's behaviour to comply with organisations' security requirements, which in turn prompt an acceptable level of information security culture in the organisation.

> "*One of the issues that should be considered in the company is the employee's satisfaction with his/her job. When the employee has a positive feeling about his job, he will be more likely to comply with company security policies"* [E10].

#### *6.8.3.5 The Main Barriers or Obstacles to Achieving Improved Security Compliance*

All respondents listed the main barriers that should be considered to increase the security compliance in organisations as illustrated in Figure 6.7.

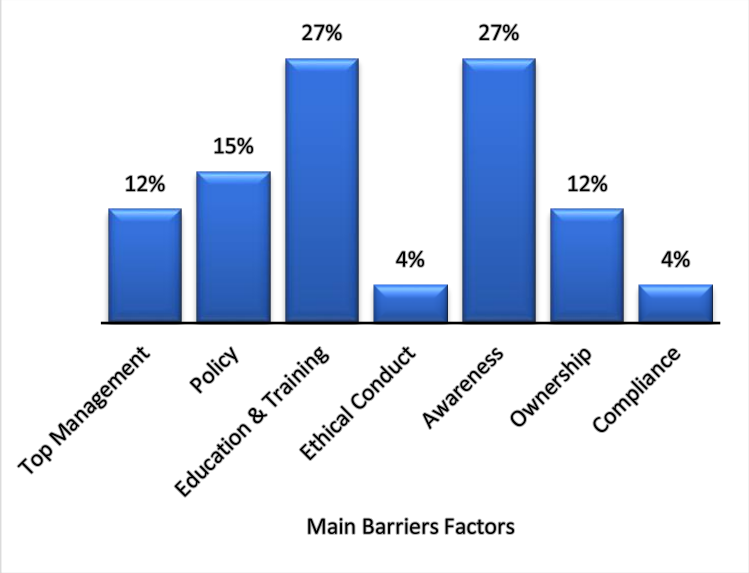



**Figure 6.7: The Main Obstacles to Achieving Improved Security Compliance**

Nine respondents from organisations A, B, E and G that the lack of awareness among employees and the lack of training and education programs as the first obstacle. The lack of clear direction in security policies and roles in the organisation was a second barrier. A lack of leadership support and lack of the ownership were the third obstacle. Two respondents from organisations B and C considered that a misunderstanding the ethical obligations of the company was implicated in certain behaviours of employees. They also felt that there should be consequences for employees who fail to comply with security procedures. Both of these factors needed attention if the security culture of information was to be improved.

The comparative analysis demonstrated some differences in the data sets in the United Kingdom, the United State of America and Saudi Arabia. There was some agreement among eight respondents' perceptions of organisations B, D, G, E and F in the United Kingdom and Saudi Arabia. These respondents considered the lack of education and training programs as a major factor in achieving improved security compliance. They considered that security education and training sessions tend to achieve security compliance together with security policy and regulations. One respondent suggested that the lack of security education and training programs led to non-compliant security behaviour due to the lack of knowledge of employees.

> "*We have simple security policies but most of employees in a company lack relevant training and hardly follow any security policies. Therefore, the training program plays a vital role in educating all employees in the company*

> *to comply with the security procedures and guidelines. As a result, we could have an effective security cultural environment*" [F1].

Respondents from these two countries, organisations B and D also concluded that the lack of security awareness-raising efforts and inappropriate values and knowledge could be linked to the organisation's weak security culture.

> *"In my company, the lack of the security culture was because most of the members lack the relevant security awareness and hardly follow or comply with the security regulation and rules*" [B2].

Respondents from these two countries, originations F and G also signified that the lack of security ownership as one of the major obstacles that could affect the security compliance of an organisation. It was suggested that each member of an organisation must view security as an essential aspect when interacting with information assets by understanding their security.

> "*Our employees do not understand their responsibilities and roles. So, it is very hard to get them to feel the ownership of protecting information security. Therefore, it is very important for the company to instil a concept that shows the security belongs to everyone responsibilities"* [F1].

The comparative analysis found that four respondents from organisations C and E in the United State of America and Saudi Arabia considered the absence of clear security policies or the lack of clarity about the enforcement of regulations were a significant factor in non-compliance with information security.

> "*If there are no clear policies and procedures related to the information security issues in a company, this leads to security incidents or mistakes caused by self-judgment* "[E1].

Respondents from organisations in the United State of America and Saudi Arabia also believed that the top management's support is very vital key to enforce the employees' compliance with security strategies and policies in the organisation. Three respondents from the United State of America and Saudi Arabia revealed that some of the organisations' top management lack the appropriate commitment to promoting the security policy.

> "*In my company, I have not seen or observed any serious commitment or motivation from the top management to enforce or commit to enhancing the information security in the company. So, the lack of leadership support and activism at all levels and consistent support in the organisation would result in a badly constructed security culture*" [C2].

One respondent from organisation F in Saudi Arabia considered ethical conduct as an obstacle that would have an impact on the organisation's security compliance. One respondent from the United States of America considered that the lack of security compliance was a factor that was a barrier to the information security culture.

### 6.8.4 Perceptions for Improving the Information Security Culture

Respondents were given the opportunity to construct individual interpretations and consider new issues that had not been addressed. Some changes or improvements that might have a positive effect on the information security culture were suggested.

**Table 6.9: Respondents Recommendation for Improving the Information Security Culture**

| Perceptions Improving the Information Security Culture |
|---|
| Conduct training and education sessions for employees. |
| Increase the awareness of employees. |
| Develop policies and rules that are clearly described. |
| Active and continuous support to security by management and leadership. |
| Strength the sense of ownership in employees. |
| Establish a code of ethics to know the accepted ethical behaviours. |
| Conduct a risk assessment regularly. |
| Outlining the consequences on staff not complying with a security. |

| Perceptions Improving the Information Security Culture |
| --- |
| Motivate employees that do the right thing for security to enhance their job satisfaction. |

Respondents had different recommendations and they made a range of discursive statements that aimed to improve the information security culture in the organisation. Their responses were grouped together under common threads and summarised in Table 6.9. There was some agreement among respondents' perceptions of organisations in the United Kingdom, the United State of America and Saudi Arabia. Four respondents agreed that the involvement and support of top management and leadership in enhancing the information security in organisations would prompt an adequate level of information security culture. However, the comparative analysis illustrated some differences in the data sets, including data collected in the United Kingdom, the United State of America and Saudi Arabia. For example, there was some commonality among the respondents' perceptions in the United Kingdom and Saudi Arabia. Eight participants from these two countries considered that implementing and increasing security awareness as an effective factor for developing a sufficient security culture in organisations.

Comparative analysis demonstrated that nine respondents from organisations in the United State of America and Saudi Arabia signified that conducting security education and training sessions, and developing clear security policies are the most positive factors. These two factors would help in improving the information security culture in organisations. Four respondents in Saudi Arabia suggested additional factors, such as enhancing the sense of security ownership in employees, developing ethical conduct, conducting a periodical security risk analysis, and enhancing the employee job satisfaction that would contribute to the improvement of a security culture in an organisation.

One respondent in the United States of America suggested the importance of security compliance. The respondent suggested to outlining the consequences on employee's non-compliance would help in improving the information security culture. Three respondents from the United Kingdom and Saudi Arabia said that there was the need for a tool or a model that could be used as guidance in the implementation of security culture factors. This tool or model should target appropriate tiers of employee behaviour and inculcate acceptable levels of security culture.

## 6.9 Interview Discussion

The qualitative interviews aimed to provide further knowledge and information for the conceptual framework. This would help to develop the model to be subsequently tested in the survey questionnaire stage. As detailed in Chapter 3, information security culture is limited in its ability to provide unambiguous concepts regarding security culture factors. Information collected from the interviews helped to support identified factors found in the literature review. The interviews attempted to identify potential gaps that exist between what is implemented and what the employees are aware of.

The qualitative phase provides rich data from thirteen experienced and knowledgeable respondents in seven organisations in the United Kingdom, the United State of America, and Saudi Arabia. The interviews confirmed existing factors in ISCFF, and these factors continue to be significant. These factors have an effect on the employee behaviour in relation to the information security culture. From the interview's findings, it can be noticed that the level of the information security culture is highly linked to a number of factors appear to be interrelated. These factors should be considered in order to improve the security of information assets and the information security culture in organisations. Indeed, through the interviews and its analysis, the information security culture was shown to reflect the security awareness, security ownership and security compliance in relation to security within organisations. Moreover, the security education and training impact on the effectiveness of the information security culture was found to be one of the most influential factors, as well as related security policy, top management's involvement within information security, risk analysis and assessment, ethical conduct and job satisfaction.

However, the interview revealed an apparent gap in the efficiency of providing education and training programs and security policies. Respondents stated the requirement for periodic security training sessions. Information security is mentioned once on induction day when the employee starts working for an organisation. As a consequence, the security awareness of employee is still low.

> "*Education and training are not memorised for long; once the new employee finishes the first week of training, information security is forgotten*" [A1].

There was also concern regarding the limitations of a training and education programs to key managers and IT members.

> *"The staffs, supervisors, all of the members of the company have to be trained about information security. For example, most of the time, the CEO's secretary has the CEO's passwords and has a weak password on her computer. Any adversary can get easily on her computer and get all the information that related to the CEO such as getting the entire mailing list, customer list and all the contact information. This happens due to the limitation of training was reflected in the low of security culture among people at the lower level in the company*" [A3].

Respondents concluded that there is a need for a structured security education and training program aimed at all the member of the organisation.

> "*In my company, we have done quite well in training the members at the managers' level; but I think we need to do more training program for the members at the users' level*" [A2].

Respondents indicated that they were unclear how policies were implemented and updated. There was concern about the lack of clarity of organisational policies. Security policies have to be clear and updated regularly, because information security is constantly evolving in response to changing threats. Consequently, the security controls and procedures have to change accordingly. Monitoring and regular updating is important.

> "*The threats are always changing, the environment is always changing, and information security is always changing. So, it is important for a company to have policies that are clearly described; improve the security policies by reviewing it continuously and maintain it up to date*" [A2].

Respondents also stated that the security policy is an important security measure. But it might be insufficient if the members of the organisation are not well-informed or aware of existing security policies and are familiar with its content. Consequently, it is reasonable to assume that there will be a lack of awareness about policies that might lead to noncompliant behaviour.

> *"We have a security policy written in documents. But no one knows what is in the documents, no one ever reads it and some of the employees are not aware of the existing rules. So, the written security policy does not have the desired influence on the employee security behaviour"* [C1].

These issues taken into consideration when constructing the survey questionnaire.

A comparative analysis highlighted some differences in the data sets collected in the United Kingdom, the United State of America and Saudi Arabia. In particular, there are similarities and differences among the respondents' perceptions regarding the main factors for cultivating an effective security culture. There were similarities regarding the important factors in establishing organisational security culture. Based on the findings, it appears that security education and training programs, security awareness and security policy are the most significant factors that contribute direct impact toward the information security culture.

Security education and training are considered the most important factors that influence information security culture's effectiveness. It was shown through the interviews that it is vital to communicate policies to all staff members. This affects how they conduct themselves in the creation of information security culture in the organisation. These details support the previous studies from the literature review, which show that an information security culture is unattainable without the sufficient level of security education and training for all employees in organisations (Hassan & Ismail 2012; Tarimo 2006). It is essential to implement and conduct periodic security training sessions in organisations to develop a security culture and to improve employee's awareness, which tends to encourage security compliant behaviour (Da Veiga & Eloff 2010). Additionally, it was indicated that in three participating organisations the security lessons had been learned following specific incidents (Da Veiga 2015). Security education and training improve the creation of information security culture, as it improves employees conduct and increases their levels of security awareness. As a consequence, security education and training are imperative in order to establish the information security culture (Da Veiga 2015; Von Solms & Von Solms 2004).

The interviews indicated the importance of security awareness in promoting the information security culture. Both security education programs and security policy encourage compliant behaviour by increasing employees' security awareness. The findings show that some organisations viewed security awareness as important in establishing a common understanding

of information security culture. It helps structure how employees think about information security. It provides the common language and base of useful knowledge when discussing various security-related topics.

> *"It is important to create a mindset within employees; you have to develop active awareness programs, and that will give the employee a high level of awareness*" [G1].

Three respondents stressed that sometimes the security awareness might be inadequate if members are not aware of possible consequences of security breaches and cannot see the value of their security role in the organisation's holistic security work.

> "*Most of the time, the poor security practices due to the lack of security awareness that lead to the lack of security culture in the company"* [E1].

Demonstrating a high level of security awareness would lead to security-cautious behaviour. This tends to encourage security compliance, while also improving the information security culture (Da Veiga 2015). Security awareness is known to improve the conduct of employees, as it influences their contribution to the stated organisation and improves the progress of information security culture.

The findings also demonstrate that a clear and sufficient security policy could promote security-cautious behaviour through security awareness and establish an acceptable level of security culture. It was suggested that the security awareness needs a foundation of security policies in order to succeed in the organisation.

> "*When employees are aware of the security policy of their company, they are less likely to engage in security threats or misuse*" [B2].

These interviews also showed that to audit security practices and procedures may enforce the policy that helps to develop the creation of organisational security culture. Security policy is enforced by reporting and taking action against those individuals who fail to adhere to the security policy. Four respondents stated that security policy is an important measure. Although it might be insufficient if members are not well-informed. It is not easy to accomplish this level of the policy enforcement, as it requires effort, strong commitment, and top management support (Von Solms & Von Solms 2004). Having an effective policy of security helps to affect

the understanding of what is deemed responsible and acceptable behaviour that ensures a safe environment in the organisation (Da Veiga 2015; Knapp et al. 2005).

The interviews revealed other factors that should be considered in establishing organisational security culture such as top management support and security ownership. Respondents from the United Kingdom, the United State of America and Saudi Arabia agreed that gaining top management commitment and support is significant in increasing organisational security effectiveness. The findings indicated the importance of management commitment and support should be from all managers at all level in the organisation.

> "*The level of top management support in our organisation is good but we need more support and commitment from other managers at all level to enforce our related policies and procedures"* [A3].

Support from top management assists the awareness of security issues. It can provide in-depth training, and enforcement and maintain employees' affiliation to the security policy (Knapp et al. 2005). Indeed, the support and commitment from top management helps to form organisational security and predict information security culture quality (Martins & Da Veiga 2015). This also involves the allocation of resources, budgets and the correct level of training. There were concerns regarding the failure of top management in enhancing the information security culture through the development of appropriate structures, education and training.

> "*Employees in the company understand the importance of security; although we do not yet have a robust security policy because of that the top management is still in the process of establishing the company security activities and structures*" [E2].

Respondents from the United Kingdom and Saudi Arabia discussed how the security ownership could play a critical role in establishing an environment that promotes the cultivation of the information security culture in the organisation. They revealed that when employees understand security responsibilities and personal ownership, they comprehend security risks and behave more securely. The responsibility and ownership by employees are required in order to protect information security (Alnatheer et al. 2012; Alhogail & Mirza 2014; Chia et al. 2002). This tends to increase security awareness and security policy compliance; thus, better information security culture (Maynard & Ruighaver 2002; Van Niekerk 2010).

> "*We do not expect to establish a security culture if our employees do not understand the importance of protecting information and it is their responsibility"* [B1].

Respondents from Saudi Arabia and the United State of America suggested three factors; security risk analysis; ethical conduct; and security compliance. The qualitative findings highlighted the importance and benefits of developing the risk analysis of information security in order to reduce the probability of loss and implement the right controls to protect the information assets from any risks in organisations. The findings demonstrated that the security risk analysis tends to assist the organisation and employees to become capable of understanding the potential damage to security. The increased security knowledge reduction of misbehaviour helps to create security awareness and improve information security practices and establish the information security culture (Alnatheer et al. 2012; Ramachandran et al. 2008).

The interview also found that ethical conduct is a vital factor that influences information security culture. It supports employees to integrate ethical behaviour, ensuring the security of information and what is accepted by the organisation (Flowerday & Von Solms 2006; Martins & Eloff 2002; OECD 2005).

> *"Understanding the ethical codes and obligations is an essential key to improving a security culture"* [B1].

The literature review has demonstrated that security compliance is necessary to the management and control of information security, and specifically to the security culture cultivation (Alnatheer et al. 2012; Da Veiga & Eloff 2008; Schlienger & Teufel 2003). The qualitative findings illustrated the importance of improving security compliance in information security culture creation to increase an organisation's security and ensure that employee behaviour complies with the security policy.

> "*Employees are often unaware of the consequences of security breaches caused by their actions; the company should have a method that ensures employees' behaviour continues to be monitored to the compliance program's effectiveness"* [C1].

Based on the interviews analysis, security compliance appeared to improve the entire security level, which is significant as the information security culture influences employee behaviour in relation to security policy compliance in organisations.

Another vital factor suggested by one respondent from Saudi Arabia was employee job satisfaction. It tends to promote security-cautious behaviour, which develops the information security culture (Farokhi et al. 2016; Greene & D'Arcy 2010). The respondent argued that the organisation should have efforts to create a work environment where employees are satisfied with their jobs. This will enhance the organisation's security posture by increasing security compliance among all staff population and improve the overall quality of life within the organisation. Hence, this leads to an organisation with satisfied employees with the right attitudes, a willingness to fulfil job responsibilities, with a proper commitment to information security culture in the organisation. Interview analysis supports other studies and highlights the significance of factors that have an impact upon employees' security behaviour. These factors are important to be considered as part of information security culture conceptualisation. They have a positive influence on each other, and thus, have a positive influence on the information security culture. The possible relationships between factors will be tested statistically and presented in Chapter 8 to determine whether the ISCFF is valid.

Personality traits have received little attention from researchers, despite indications that personality traits directly affect individual behaviour (McCormac et al. 2017). The interview findings demonstrated how personal values and practices are important in the process of the information security culture. However, this factor has received a weak degree in the qualitative phase. No respondents had mentioned during the interview. This is important for future research and will be an essential factor in the construction of the survey items. The interview findings provide some insights, although these are not generalisable, as additional investigations are required. Therefore, this study was expanded to develop a statistical framework that would identify the correlations between factors. Knowledge management would be integrated to develop a framework that would help organisations to create the culture efficiently and predict how the information security culture could be improved. Consequently, a quantitative survey was conducted (see Chapter 7 and Chapter 8).

## 6.10 Hypothesis Development

The conceptual ISCFF had been developed based on conclusive analysis of literature relating to the information security culture. This research identified several important factors related to the information security culture. This framework includes being able to identify factors that constitute the information security culture, and factors that could prove influential in the adoption of the information security culture. Each of the identified factors in ISCFF might contribute positively or negatively to the level of the information security culture in organisations. The exploratory interviews conducted to explore whether all identified factors in ISCFF are necessary. The qualitative findings confirmed the identified factors of ISCFF except personality traits. However, information gained from the interviews provided further framework factors, and how constructs are viewed in relation to reality settings. The identified factors in ISCFF had signified its importance and have an effect on the employee behaviour in relation to the information security culture. In addition, these identified factors in ISCFF would improve the security of information assets and information security culture in organisations.

It is evident from the literature and the interviews carried out in this research that an information security culture is linked to a number of inter-related factors. There is strong evidence derived from the qualitative interviews and the literature review analyses that the identified factors in ISCFF should make the security culture more effective. Security education and training impact on the effectiveness of information security culture and was found to be one of the most influential factors, as well as security policy, top management involvement, risk analysis and assessment, ethical conduct and employees job satisfaction. This research developed and formulated seven hypothesises with respect to the discussed theoretical background and research objectives. The developed hypothesises (H1 to H7a-e) explain the relationship between constructs based on the qualitative interview findings incorporated with the literature review analysis to be tested through the survey phase.

The support from top management and commitment has been shown to be one of the important factors that leads to the information security success in organisations (D'Arcy & Greene 2009; Dojkovski et al. 2007; Martins & Da Veiga 2015). The involvement by the top management in an organisation relates to whether senior management figures exercise dedication to information security. The qualitative findings supported this concept in the development of information security in different companies. Top management figures are able to ensure that

staff members remain accountable for each action and decision in relation to security. Consequently, the top management influences the creation and maintenance of information security culture. This would not be developed without implementing consistently positive encouragement and involvement from these figures (Masrek et al. 2017; Martins & Da Viega 2015). Therefore, it hypothesises the following:

***Hypothesis (H1): Top management support has a positive influence on the effectiveness of the security culture.***

Security policy was considered one of the important factors in the cultivation of the information security culture. The findings showed that a clear and effective security policy has a tendency to promote security-cautious behaviour in organisations. Combining the findings from the literature reviews and interview data, it has been suggested that a security policy must be enforced and be a top priority in organisations. It will encourage security compliance, through security awareness and establish an acceptable level of information security culture (Alnatheer et al. 2012; Alhogail 2016; Da Veiga 2015). As a result, it is hypothesised:

***Hypothesis (H2): Security policy has a positive influence on the effectiveness of the security culture.***

Security education and training is the most important factor that influences the effectiveness of information security culture in organisations. It was shown through interviews that it is important to communicate the policies to staff members. This affects how they conduct themselves in the creation of information security culture in the organisation. This qualitative finding supports the previous arguments from the literature review, which show that an information security culture is unattainable without the sufficient level of security education and training for all employees in the organisation (Da Veiga & Eloff 2010; Hassan & Ismail 2012). It is important to implement and conduct periodic security education and training sessions in order to develop a culture of information security. This helps to reduce risks to information assets and to improve the awareness of employees which, in turn, has a tendency to encourage security compliant behaviour (Da Veiga & Eloff 2010; Tarimo 2006).

***Hypothesis (H3): Security education and training has a positive influence on the effectiveness of the security culture.***

The importance of implementing security risk assessment and analysis has been shown in the literature review and qualitative. Security risk analysis and assessment help the organisation and its employees to capable of understand potential damage to security. It helps to increase awareness and knowledge, which improves the level of information security culture (Alnatheer et al. 2012; Martins & Eloff 2002; Nasir et al. 2018).

***Hypothesis (H4): Security risk analysis and assessment has a positive influence on the effectiveness of the security culture.***

The findings also suggested that ethical conduct is another vital factor that influences the cultivation of information security culture. Ethical conduct is important in the creation of information security culture. It serves as a guideline that simplifies, clarifies and defines actions deemed to be ethical. Ethical conduct enables employees to understand their own responsibilities. As the employee adhere to the policies it reduces potential security behaviour risks (Alnatheer et al. 2012; Martins & Eloff 2002; OECD 2005). Some organisations in various industries have failed in their practice of ethical conduct (Alnatheer et al. 2012), and thus, negatively influences the cultivation of information security culture. Ethical conduct policies strongly affect the information security culture in organisations. When failed to be applied, the security nature in the organisation decreases. Thus, this needs to be developed in order to have an effective information security culture.

***Hypothesis (H5): Ethical conduct has a positive influence on the effectiveness of the security culture.***

It is evident from the literature review and the interviews that another important factor in security compliance is job satisfaction. The job satisfaction plays an important role in employees' behaviour and attitudes towards the information security in organisations (Farokhi et al. 2016; Greene & D'Arcy 2010). Job satisfaction helps to determine how employees may adapt to situational factors, such as remaining committed and not opting for easier options, which could prove detrimental to the organisation (Greene & D'Arcy 2010).

In the interviews, employees who reported positive feelings and job satisfaction were more likely to comply with the organisation's security requirements. Their improved engagement allowed them to interact with their individual and collective responsibilities, as well as to improve the overall quality of life in the organisation. As a consequence, the organisation will have more satisfied employees with the right attitudes and willingness to fulfil job

responsibilities and commit to the information security culture. The review of the literature supported this concept and indicated that higher job satisfaction motivates employees to comply with security policies and regulations in the organisation.

***Hypothesis (H6): Job satisfaction has a positive influence on the effectiveness of security culture.***

These factors appear to play a significant role in affecting and directing the interaction of humans with information security. They are important to be considered as part of information security culture conceptualisation in order to improve the security of information assets. However, there is another factor that contributes to various workplace behaviours, that is personality traits. This factor has failed to receive sufficient attention and analysis in regard to information security culture area. This factor was also not well noted during the interviews. McCormac et al. (2017) suggested the need for future research to examine personality traits and their impact on information security culture. Indeed, studies that examined the relationship between personality traits and information security culture are rare. This research examined whether personality traits contribute positively or negatively to the level of information security culture in organisations.

Individual differences play a ubiquitous role in information security. Researchers such as Gabriel and Furnell (2011) and McCormac et al. (2017) incorporated relevant cognitive and personality-related variables into numerous outcome models for information security success. Employee behaviour are commonly emphasised by studies focusing on human factors within information security (Bulgurcu et al. 2010). The research studies, such as Shropshire et al. (2006) and Mcbride et al. (2012) have provided assessments of relevant topics through the presentation of strategies of prevention for end-user contexts in relation to employees' contributions regarding individual mistakes or failings, in order to increase the level of information security. The literature review and its subsequent findings demonstrated that individual personality traits affect security behaviour. The personality traits potentially assist in improving individuals' awareness of security and information asset security within organisations (McCormac et al. 2017). Studies have analysed the personality test factor (Gabriel & Furnell 2011; McCormac et al. 2017). Specifically, Gabriel and Furnell (2011) analysed the correlation between personality characteristics and quality security behaviours. They presented a summary of the personality test results that could potentially function to predict security behaviour within organisations. McCormac et al. (2017) analysed the

correlations between personality traits and levels of security awareness in different individuals. Their study resulted in the conclusion of considering individual contrasts (i.e. personalities) in regard to their security awareness. The findings functioned to help organisations to determine which areas need to be improved or to implement relevant training courses.

An individual personality is formed from a consistent pattern of how he/she responds to the environment, and how they react to different events. The most commonly used taxonomy in research into peoples' personalities is the Five-Factor Model (FFM) (Barrick et al. 2001). This FFM model is one of the most frequently utilised multidimensional forms of measurement into people's personalities. This has become widely accepted in this form of research, as it has good validity, which was shown by various empirical studies (McCrae & John 1992). A main advantage of the FFM stems from its generalisability, which is essential to its systematic and comprehensive approach to personality (Goldberg 1993). These factors are not supposed to show any specific theoretical viewpoint. They instead should form an overall taxonomy of the terminology that enables people to be able to describe themselves and others alike (John & Srivastava 1999). This form of generalisability allows FFM to be used across various disciplines, including ones that could be similar to security in information technology.

The FFM also helps to determine behavioural patterns that are relevant to the factors that are well known when compared to the large number of particular factors (Cellar et al. 2001). The FFM is used to better comprehend individual human personalities and to predict various factors in contrasting environments (Shropshire et al. 2006). The aim of the model is to divide human personality into five factors that enable the theoretical conceptualisation of personalities: extroversion, agreeableness, openness, neuroticism, and conscientiousness (Costa & McCrae 1992; John & Srivastava 1999). Table 6.10 provided a description for five factors.

**Table 6.10: Five-Factors Traits as Described by John and Srivastava (1999)**

| Factor Name | Factor Description |
|---|---|
| Extroversion | Extroverts are more out-going and friendly, and thus, interact more with others, as they are more sociable, active, assertive, and have positive emotions; contrastingly, introverts are more reserved individuals. |

| Factor Name | Factor Description |
|---|---|
| Agreeableness | Individuals who are agreeable function with cooperation, are eager to assist others and exercise reciprocity; contrastingly, an egocentric and competitive nature is shown by those who have scores low of agreeableness. |
| Openness | Openness is the willingness to attempt new experiences, with individuals who present high scores tending to use more imagination and have increased intellectual curiosity. These individuals are also commonly open to innovative and potentially unconventional concepts and beliefs. |
| Neuroticism | This presents a tendency for an individual to have negative feelings, which include: anger, disgust, fear, guilt and/or sadness. When one has a high neuroticism score, this demonstrates that an individual is prone to irrational thoughts, and is less likely to be able to control certain impulses and be able to cope with stressful situations. |
| Conscientiousness | Those who are conscientious demonstrate high levels of self-control with good organisation skills. These people are commonly purposeful and strong-minded, as well as being dependable for others and hardworking. A high level of conscientiousness, nonetheless, can potentially manifest in over-work and in a compulsive nature in regard to cleanliness. |

Previous meta-analytic evidence has shown certain FFM traits to have more relevance in providing explanations of behavioural factors (Barrick et al. 2001). For instance, people who present with high extraversion scores connect with better training proficiency (Barrick et al. 2001). While agreeableness is beneficial in completing tasks, which require a high level of interpersonal interaction (Mount et al. 1998). Both of these particular traits relate to social interaction factors in humans. Hence, the levels of extraversion and agreeableness are able to be determined by information security dimensions that include interpersonal interactions. Comparatively, an individual's openness is seen to be vital in research which focuses less on interpersonal interactions (Mount et al. 1998). Evidence shows that those who present reduced levels of emotional stability are often more averse to risk-taking (Lauriola & Levin 2001), and not as focused on goals (Judge & Ilies 2002). Consequently, these normally indicate individuals' attitudes toward long-term and economic perceptions. Meanwhile, when a person is conscientious, he/she exercises dutifulness and a focus on achieving something, which is fundamental to intrinsic motivation with a high job performance level (Barrick et al. 2001; Devaraj et al. 2008). Due to these facets, it is more probable that conscientiousness has more relevance to research studies that aim to investigate various performance factors.

In addition, McCormac et al. (2017) analysed the correlation between specific differences, including through personality tests and security awareness levels. It was subsequently determined that the levels of individuals' conscientiousness, agreeableness and emotional stability noticeably presented contrasts between people's security awareness. Their study suggests the requirement for additional research in order to analyse individual differences, as well as how they impact on the information security culture. Various studies such Alnatheer et al. (2012) and Martins and Da Viega (2015) have concluded that a strong relationship is evident between the information security culture and security awareness. Whilst McCormac et al. (2017) study analysed how an individual's personality impacts upon security awareness levels. Therefore, from these findings it can be deduced that particular personality traits are hypothesised to relate to certain information security components. Specific hypothesised correlations are relevant when they are appropriate to the study and supported by theoretical and empirical research findings. In regard to the objectives, this research has focused purely on the five global dimensions of FFM, and not on the particular facets. Thus, the current research used these insights in order to investigate the relationship between personality traits and the information security culture. It is hypothesised the following:

***Hypothesis (H7): Personality traits has a positive influence on the security culture.***

Results from Barrick et al. (2001) study indicate that agreeableness is a positive factor in relation to work. It involves notable interpersonal interaction, particularly in regard to job tasks through helping others and cooperation. People who have a personality trait of agreeableness are commonly courteous, trustworthy, cooperative, compliant, and are often tolerant and forgiving (Barrick et al. 2001). When a person exercises agreeableness, they normally maintain more harmonious relationships and have the ability to work better in a team (Mount et al. 1998; Neuman & Kickul 1998). This functions with being able to adapt and to be innovative (LePine & Van Dyne 2001). An individual's agreeableness has been deemed to have a vital and positive connection with increased levels of organisational safety. Whilst accidents were not as likely for those with stronger levels of interpersonal orientation (Cellar et al. 2001).

Another study of Shropshire et al. (2015) analysed people's self-reported intentions and personality in order to create a web-based security software programme, which had the potential to utilise security software in relation to higher agreeableness levels. Separately, Pattinson et al. (2015) study provided an evaluation of non-malicious computer-based behaviour, as well as analysing different relevant factors: people's ages, connection with

computers, and education levels. It was determined that when an employee presents naivety in relation to accidents that they are not at such a high risk when they are more agreeable. Those with high agreeableness scores normally become more concerned with security issues, as they commonly think about others' opinions of them (Korzaan & Boswell 2008; Shropshire et al. 2015).

Agreeableness, as shown by Pierce and Hansen (2008), positively affects perceived team effectiveness. The correlation between agreeableness and information security has been analysed to stem from an employee's attitude towards information security when this involves cooperation and collaboration with others. Individuals who have high agreeableness scores are more likely to have greater empathy towards end-users and/or team members, which makes them more helpful with security problems (Ashenden 2008). Similarly, agreeableness was shown to have greater effects on policy in regard to user compliance (Shropshire et al. 2006). Mcbride et al. (2012) study presented empirical evidence that showed theoretical model validity that attempted to assess personality factors and their potential factors and effects. The results showed that security policy compliance was more likely in individuals with higher agreeableness scores. It can be deduced that agreeable employees are influential upon positive information security cultures.

***Hypothesis (H7a): Agreeableness has a positive influence on the effectiveness of the security culture.***

Conscientiousness is one of the most relevant personality traits to information security behaviour (Hu et al. 2012; Shropshire et al. 2006). Conscientiousness is a trait associated with planning and persistent behaviour. When people are conscientious, they are hard-working, as normally focus on achievement are motivated, dependable, responsible and ambitious (Barrick et al. 2001). Various studies such as Arthur and Graziano (1996) and Cellar et al. (2001) have highlighted a notable inverse correlation between levels of conscientiousness and involvement in accidents in organisations. People are not as likely to be involved in accidents when they score high in delaying gratification, thinking prior to acting, adhering to rules and regulation, as well as being able to plan and organise tasks (Arthur & Graziano 1996).

Previous studies have also presented positive relationships between conscientiousness and employee job performance levels (Barrick et al. 2001). There is a strong impact of conscientiousness upon mindfulness in IT innovations (Goswami et al. 2009). Bansal (2011)

showed how conscientiousness positively correlates with security concerns. While Shropshire et al. (2006) noted that it has the highest impact upon information policy with user compliance. Compliance with security policy was more likely with conscientious individuals (Mcbride et al. 2012). Similarly, McCormac et al. (2017) determined that conscientious individuals are significantly more security aware. The higher levels of conscientiousness commonly resulting in more care as organisational security requirements are considered more, with a focus on improving information security and the overall information security culture (Li et al. 2006). Therefore, conscientiousness in an individual positively influence the information security culture.

***Hypothesis (H7b): Conscientious has a positive influence on the effectiveness of the security culture.***

Costa and McCrae (1992) stated that openness is fundamental to a person's personality. Openness enables the ability to explore various forms of information that attracts different situations. Employees who are open to experience, are generally inventive, creative, open-minded, more intellectual and imaginative (Barrick et al. 2001). For example, openness to experiences presents opportunities to recognise the capacity to acquire deep information, analysis and the ability to examine disconfirming data (Shane et al. 2010). Additionally, openness results in a wider scope of thought and awareness (Junglas et al. 2008); as well as better deep-minded thinking (Costa & McCrae 1992). McBride et al. (2012), developed comprehension levels for personality traits which comprise behavioural patterns and impact upon employees' intentions to adhere to the security policies. Their study results showed that security policy compliance is more likely with employees who are more open. Employees who present higher levels of openness to new experiences are normally better at problem solving. They have better critical thinking skills, that increase security awareness and security compliance. Hence, it is hypothesised that openness influences the information security culture in a positive manner.

***Hypothesis (H7c): Openness has a positive influence on the effectiveness of the security culture.***

An extraverted personality has been shown to result in improved task performance through interpersonal interactions (Mount et al. 1998; Mount et al. 2005). Extraverts normally aim to establish a favourable social status and then maintain it (Devaraj et al. 2008). When an

individual is extroverted, they generally exhibit positive emotionality, ambition, energy and dominance in various situations and settings. For instance, in training settings, it has been revealed that that extraverts are more likely to demonstrate an active nature and become involved in opportunities that provide and obtain information from particular settings (Costa & McCrae 1992). Bansal (2011) analysed the relation of FFM, focusing on website security and privacy and showed that extraversion has a positive effect on security concerns. Hence, it may be surmised that extroverted employees have better positive attitudes toward information security. The extroverted employees exercise a proactive external nature with internal information procurement in relation to security breaches, possible risks, and legislation and communication through. This helps to increase their awareness and performance levels (Whitten 2008). Employee who are highly extraverted are more likely to have a positive attitude towards the information security culture.

***Hypothesis (H7d): Extraversion has a positive influence on the effectiveness of the security culture.***

Emotional stability (the counterpart of neuroticism) has been shown as a valid predictor that improved job performance (Barrick et al. 2001). Emotional stability is the opposite of neuroticism. The individual becomes less anxious, pessimistic, hostile, and less personal insecurity. In contrast to individuals who are emotionally stable, those with a neuroticism personality are normally more averse to risk-taking (Lauriola & Levin 2001). Neurotic individuals demonstrate levels of worry, sadness, low-confidence, depression, anger, and feelings of insecurity (Barrick et al. 2001). Frequently, these individuals fail to perform well with tasks and struggle to deal with changes or new challenges (Barrick et al. 2001). The study by Mcbride et al. (2012) increased the understanding of individual personality traits that comprise behavioural patterns. The individual personality traits are impactful on employees' intentions that adhere to security policies, with neuroticism often leading to security policy violations. McCormac et al. (2017) study analysed the correlations between certain personality differences through personality tests and security awareness measurements. It was consequently determined that emotional stability is noticeably effectual upon employees' security awareness. Therefore, this research hypothesised the following:

***Hypothesis (H7e): Neuroticism has a negative influence on the effectiveness of the security culture.***

Table 6.11 summarises the main hypothesis to be tested through the subsequent survey phase. Three hypotheses (H1, H2, H3) have been proven to have a positive impact on the information security culture in previous studies, such as Martin and Da Veiga (2015), Knapp et al. (2007) and Nasir et al. (2019).

**Table 6.11: Research Hypothesis to be Testing in a Subsequent Survey Phase**

| **Research Hypothesis** | |
|---|---|
| **H1** | Top management support has a positive influence on the effectiveness of the security culture. |
| **H2** | Security policy has a positive influence on the effectiveness of the security culture. |
| **H3** | Security education and training has a positive influence on the effectiveness of the security culture. |
| **H4** | Security risk analysis and assessment has a positive influence on the effectiveness of the security culture. |
| **H5** | Ethical conduct has a positive influence on the effectiveness of the security culture. |
| **H6** | Job satisfaction has a positive influence on the effectiveness of the security culture. |
| **H7a** | Agreeableness has a positive influence on the effectiveness of the security culture. |
| **H7b** | Conscientious has a positive influence on the effectiveness of the security culture. |
| **H7c** | Openness has a positive influence on the effectiveness of the security culture. |
| **H7d** | Extraversion has a positive influence on the effectiveness of the security culture. |
| **H7e** | Neuroticism has a negative influence on the effectiveness of the security culture. |

However, Alnatheer et al. (2012) noted that it necessary to distinguish between factors that constitute the information security culture and those that affect the information security culture. As this will help organisations to direct human interaction with the development of information security, and thus, advance the protection of information assets. However, there remain only limited studies that have identified factors which constitute the information security culture

(Walton 2015). Alnatheer et al. (2012) is the only study that states factors that form the information security culture. Although it was unable to validate certain identified factors, including security compliance. Due to the evident gaps in the literatures about what constitutes an information security culture in regard to necessary identification factors that help to create the information security culture, this research has determined that the information security culture is connected to security awareness, security ownership and security compliance.

The qualitative interviews provided confirmation of factors that reflect the information security culture. It was shown to be constituted of security awareness, security ownership and security compliance. The findings from the interview presented that the perceptions by IT/ security experts in relation to the security awareness are imperative elements in the development of information security culture. The security awareness is a requirement in the cultivation of information security culture environments. It is documented as a serious issue when the security awareness is not considered (Magklaras & Furnell 2005; Parsons et al. 2017).

The security awareness is an imperative factor of information security culture. It is unfeasible to create this without the security awareness. When there is a distinct lack of knowledge and awareness by employees, the information security becomes threatened (Thomson & Von Solms 1998). Awareness by employees is one of the main challenges the organisations face in achieving an adequate level of security (Siponen 2000). Both security education programs and the security policy have tendency to encourage compliant behaviour by increasing security awareness of employees. For example, when employees are aware of security policies, compliance with the security policy is achieved; hence, there is a development in information security culture (Schlienger & Teufel 2003). As a result, security awareness is commonly the main factor that results in greater levels of compliance and advance information security culture implementation (Alnatheer et al. 2012; Da Veiga 2015; Wiley et al. 2020).

The findings have shown that security ownership is vital in the information security culture cultivation. Employees need to comprehend precisely what their own roles and responsibilities are in their organisation. This improves security performance, and thus the information security culture of the organisation. When the responsibilities are understood, as well as the necessity of protecting information security, employees are able to understand the security risks that could be a result of their own actions. Consequently, this increases the security awareness, and increases the security policy compliance and thus lead to the establishment of information security culture (Van Niekerk 2010; Tarimo 2006). When an employee is responsible and has

a sense of ownership, employee behaviour changes in relation to organisational asset protection, and results in improved the information security culture creation (Ruighaver et al. 2007; Walton 2015).

The qualitative results illustrated the importance to improve the security compliance in organisations towards the creation of organisational security culture and improving the entire security level. This is vital as the information security culture influences employee behaviour in relation to official security compliance. The literature review demonstrated that the security compliance is necessary to the management and control of information security, and specifically to the information security culture creation (Da Veiga & Eloff 2010; Masrek et al. 2017; Schlienger & Teufel 2003). Eloff and Eloff (2005) noted that the security compliance improves an organisational security culture, as an organisation is capable of decreasing the number of security breaches that are a direct result of employees' conduct. Poor levels of conduct by employees have the potential to influence the practice of information security, and potentially result in damages and/or losses to the assets of an organisation (Von Solms & Von Solms 2004). Additionally, the findings in this study have shown that security compliance is a cultural factor which undoubtedly improves the information security culture establishment.

Based on the findings of interviews and literature, strong correlations exist between the information security culture and its reflection factors (Alnatheer et al. 2012). These three factors connect with the development of information security culture. These factors will be used as the reflection for the information security culture. Indeed, the research determined that the information security culture is perceived as a second-order factor, which involve security awareness, security ownership and security compliance, as these three have a high correlation with each other. The second-order models are normally applicable to research studies, where measurement instruments provide an assessment of various connected components, which are all measured by numerous items. The second-order model shows the hypothesis which evidently distinct, although related components are able to be accounted for through base higher order constructs. Therefore, second-order construct the security culture is measured through the utilisation of the lower-order factor indicators, as aforementioned above.

## 6.11 Conclusion

This research aimed to further comprehend various factors that positively assist with organisational information security culture from the employee perspective. Existing literature

identifies factors that should be considered in order to create an environment that promotes better information security culture. An exploratory interview presented important factors that potentially affect organisational security culture. It also identified existing gaps in levels of awareness. The analysis of qualitative data design has been detailed and evaluated and included data sampling and analysis. Information acquired helped to determine how organisations focus and maintain the information security. Respondents comprised thirteen experienced and knowledgeable security specialists from seven organisations located in the United State of America, the United Kingdom and Saudi Arabia. These interviews were analysed to highlight the significant factors in the information security culture stemming from respondents' experiences. The findings from the interviews contribute to the existing knowledge by providing factors that are significant in affecting human behaviour and which are vital in information security culture.

The information gained from interviews provided further knowledge of how different factors were viewed regarding reality settings. The interview data concludes that continuously subjecting employees to targeted education and training programs and on-going security awareness development improves the information security culture. The findings also revealed a gap in the implementation of organisational policies, and ineffective security education and training programs that lead to a lack of security awareness and security compliance. The result of the findings cannot be generalised but can be viewed to be indicative. The analysis of pervious research studies and qualitative findings has helped to develop hypotheses that are associated with the current research framework elements and constructs.

# Chapter Seven :

# Empirical Study Methodology- Survey Design and Development

## 7.1 Introduction

The survey design and development are detailed in this chapter based on the process presented in Chapter 4, section (4.4.3). The first section presents the questionnaire design and content development. The Second section presents the questionnaire pre-test results including the expert panel feedback and findings from the pilot study in order to determine the survey instrument's reliability and validity. Next section describes the survey method sampling and population. After that, a section provides the questionnaires administration and process in the current research. The final section presents the chapter conclusion.

## 7.2 Survey Design

The survey design is considered to a vital process in the research. It helps to achieve the research goals, as well as implementing the selection of the most relevant and accurate tool (Zikmund 2003). Specifically, this research tool needs to be able to answer the research question(s) in regard to the measurement (construct validity), together with the way that the measurement was undertaken (construct reliability) (Sekaran & Bougie 2016). The main aim of the survey in this research is to provide validity of the framework's influential and refection factors. It is necessary to test the correlations between factors that are influential in information security culture and those factors that reflect a culture of information security. This survey/questionnaire contains relevant questions that show particular variables from the model, with an analysis of the findings in order to present conclusions for a subset of the total population or a particular section of a population.

The questionnaire contains pre-formulated questions that helped to obtain relevant information for the research focus. Respondents recorded answers by adhering to the set protocols (Sekaran & Bougie 2016). These protocols are imperative to the provision of accurate and reliable data (Alnatheer et al. 2012). The questionnaire also needed to be effective in the identification of factors that relate to the information security culture, whilst measuring values, beliefs and the security behaviour of organisational members. The template questionnaire was designed based on the specific framework components that identified and issues that related to information security culture. Published information security culture assessment instruments, such as Da Veiga (2018) and Alhogail and Mirza (2015) survey assessment tools helped in the design process.

Researchers have stated that previously validated survey instruments should be used where possible in order to facilitate the confirmation of reliability and validity, instead of developing new ones for specific research (Bélanger & Crossler 2011). In this research, previously validated questionnaire items were revised and used together with five items that been created for this research. This ensured that the measures would be sufficient, representative, and suitable for use, and improve content validity levels. Different researches Alhogail and Mirza (2015), Alnatheer et al. (2012), Da Veiga (2018) and Knapp et al. (2007), were incorporated in order to develop the survey instruments that related to the information security culture.

The assessment of information security culture, by Da Veiga and Eloff (2010), and Alhogail and Mirza (2015), was used to initiate the questionnaire design. These studies used similar approaches in the implementation of surveys that helped in the development of certain statements for this research framework. The overall design of the questionnaire stemmed from these models, especially in relation to the answers' scale and general structure. The questionnaire also included measurements of personality traits with (FFM) items, taken from Goldberg (1993) and Shropshire et al. (2006). Furthermore, six different experts provided their advice on whether the questionnaire measured constructs adequately. Their feedback resulted in necessary amendments to the wording and structure of the questionnaire. The research questionnaire was developed based on the component of the ISCFF, and information from the interviews and expert reviews.

### 7.2.1 The Questionnaire's Content Development and Operational Items

The content for the questionnaire stems from the research objectives, which aim to validate factors that relate to organisational security culture, as well as to provide measurements of employees' values, beliefs and security behaviour. The questionnaire included items that covered the investigated subject and demographic details that enable analysis of either personal or organisational aspects. The questionnaire began with an introduction and clear guidance. The consent form provided details of the research and defined "information security culture". The researcher's contact information was also provided, as this enabled participants to present any potential concerns where relevant.

In addition, Plymouth University's code of ethics has been adhered to throughout this process, which is why a consent question was included to confirm the participants were all above 18 years of age. They were also asked to confirm that they all understood the full research

conditions and how their participation in the study functioned. In the final section of the questionnaire, a comment box enabled the participants to provide feedback, as well as to construct individual interpretations in regard to other issues that were not part of the questionnaire (see Appendix J for the full survey). There were four sections: Demographics; knowledge; practices and behaviours; personality traits.

***Demographic Information***

The questionnaire gained demographic data on the type and size of the organisation, the organisation industry, gender, age, country, employees' qualification levels in the field of IT, experience levels, hierarchal job level, and whether they had received an induction and whether the induction include information security measures. Demographic data is important as it helps to determine that the respondents represent the overall target population. No personal details are required, and thus, the individuals' information remains anonymous and all personal data is confidential. A multiple-choice scale was selected in order to make the responses clear and simple. This section helped to show how jobs functioned within information security measurements and to compare respondents.

***I. The Knowledge Sections***

This section attempted to measure the employee levels of data security knowledge and their levels of security awareness in organisations. This aimed to help to determine the potential strengths or development areas. It was achieved through the implementation of particular questions in relation to the awareness programme and issues regarding the form of information management required. This section included nineteen questions that focused on the research framework's scope, with the majority taken from a variety of different studies such as Alhogail and Mirza (2015), Da Veiga (2018), Da Veiga and Eloff (2010), Knapp et al. (2006), and Martins and Eloff (2002). There were only three questions that were developed specifically for the current research (Questions 9, 17, 18), as they were shown suitably connected to the qualitative findings. Four interviewees remarked upon the benefits of comprehending the risks involved in information security culture and a periodical security risk analysis and assessment for a better information security culture. Question 9 checked whether the employee knew and was aware about the organisation consistently assess and generates a report for the security risk analysis or not (see Table 7.1).

Table 7.1 presents the full source breakdown for each question, with the first column outlining the knowledge statements, and the second stating the used source as a form of input and guidance for statement design. The questions' scale was "Yes/No" or "do not know" as the options. In addition, one of the experts for Question 17 stated that an addition of another question would be useful in order to ask respondents whether security training sessions occur within their organisations together with a series of options, as individuals may differ in their definition of a training session (i.e., a casual conversation against a web-based training session). Separately, Question 18 introduced Question 19, which showed that it is necessary to initially demonstrate whether respondents normally like to receive security awareness in their organisations.

**Table 7.1: Knowledge Questions**

| # | Statement | Source |
|---|---|---|
| **1** | The organisation has formal documents for information security policies. | (Da Veiga & Eloff 2010) |
| **2** | I have read the information security policy sections that are applicable to my job. | (Da Veiga 2018) |
| **3** | Are there disciplinary consequences if employees do not comply with the information security policies in the organisation? | (Alhogail & Mirza 2015) |
| **4** | The organisation consistently reviews and updates the information security policies on a periodic basis. | (Knapp et al. 2006) |
| **5** | I am informed regularly about information security requirements and updates. | (Da Veiga & Eloff 2010) |
| **6** | Are your security responsibilities and roles clear? | (Alhogail & Mirza 2015) |
| **7** | Does the organisation have a person/team that is responsible for assessing the risk of information assets? | (Martins & Eloff 2002) |
| **8** | I am regularly informed and updated information about risks associated with security breaches such as scam email attachments, unknown senders, etc. | (Alhogail & Mirza 2015) |
| **9** | Does the organisation consistently assess and generates a report for the information security risk analysis on a periodic basis? | Developed for this research |

| # | Statement | Source |
|---|---|---|
| **10** | To whom you should report information security incidents? (Please select all that apply).<br><br>☐Help desk ☐Human resources ☐IT department<br><br>☐My immediate manager ☐ Group information security officer<br><br>☐ I do not know ☐ The whistle-blowing process should be used | (Da Veiga 2018) |
| **11** | The organisation has an ethical code of conduct. | (Alhogail & Mirza 2015) |
| **12** | Does the organisation have an ethics committee/advisory that is responsible for the code of conducts? | (Martins & Eloff 2002) |
| **13** | Is the organisation's code of conducts clear and easy to understand? | (Alhogail & Mirza 2015) |
| **14** | I am informed about information relevant legislation and regulations, such as of intellectual property and copyright laws. | |
| **15** | Is there a procedure to ensure the safety of data at the end of each working day? For example, not leaving confidential documents on the desk when you leave the working area. | |
| **16** | Do you as an employee know where to find/access the following:<br><br>a) The organisational information security policies.<br>b) The organisation's ethical code of conduct.<br>c) The security-related training programs.<br>d) The update information/materials regarding the organisation's security. | |
| **17** | Have you attended any security training in the organisation such as Induction training or Web based training?<br><br>☐Induction training ☐ Hands-on training sessions ☐Web based training ☐All the above | Developed for this research |
| **18** | I would like to receive information security awareness. | |

| # | Statement | Source |
|---|---|---|
| **19** | How do you prefer to receive information about security awareness? (Please select All that apply).<br><br>□ Induction training □ e-mail □ Posters □ Video's<br>□ SMS messages □ Hands-on training sessions<br><br>□ Web based training □ Discussion group<br>□Business unite presentations □Articles in new frontiers | (Da Veiga & Eloff 2010) |

### *III. Information Security Culture Practices and Behaviours*

This section provides an assessment of the organisational security culture, as documented by the employee perceptions based on the components of the ISCFF. Nonetheless, operationalising the framework constructs aims to measure the main concepts, particularly those involving the comprehension of employees' feelings and attitudes in this respect (Sekaran & Bougie 2016). Even though overview framework construct definitions were detailed previously, they are ultimately not sufficiently specific and do not provide sufficient measures to document the full meaning of different constructs. This process started by determining the constructs dimensions, and subsequently moving them into clear measurable elements that are able to shape construct measurement indices (Sekaran & Bougie 2016). Consequently, the elements that stem from this particular process were chosen as measurement variables and used in the development of the constructs' multivariate measurements. The number of items in the process of construct measurement needs to sufficiently sample the studied phenomenon. When a questionnaire has an excess of items, this can potentially create response bias from participants, while the validity of context and construct validity are threatened when there are not enough (Sedera et al. 2003).

A comprehensive literature review and qualitative findings were combined, together with expert reviews in order to determine the specific constructs and their related survey items that influence and constitute the information security culture. The questionnaire dimensions were identified to measure the ten different constructs: top management; security policy; security education and training; security risk analysis and assessment; ethical conduct; job satisfaction; personality traits; security awareness; security ownership; and security compliance. The components of the framework were also divided into various measured representative tasks

and statements. Subsequently, statements were placed together in certain clusters that represented the dimensions' different elements and their connections (Da Veiga et al. 2008).

The majority of statements were taken from different studies and validated based on the scope of this research framework. Most of statements were adapted from questionnaires from these studies (Alantheer et al. 2012; Alhogail and Mirza 2015; Da Veiga 2018; Da Veiga and Eloff 2010; Knapp et al. 2006; Spector 1997). From these adapted scales, it was possible to increase the framework's level of reliability and validity. Hence, it is beneficial to use the constructs' measurement scales, which enable content validity (Nunnally & Bernstein 1994). Consequently, numerous scales were adapted from previously validated instruments; while other statements were taken from the interview responses and the feedback from the experts, which helped to address various issues from the framework.

The questionnaire statements were chosen to best implement representation of the different factors for the framework's dimensions. For instance, a security policy is shown in the statement: "The contents of the information security policy prescribed by the organisation are easy to understand". Meanwhile, the statement: "I feel satisfied with the kind of work I do in this job" represents job satisfaction. This section includes thirty-four particular statements with both open and closed answers that can provide an assessment of employee perceptions in regard to the research framework's components. These thirty-four statements included a brief description, together with option ratings based on a five-point Likert scale (1 = strongly agree to 5 = strongly disagree). The research also presents a full description of the constructs with the number of measuring items, scale, and their adoption source as presented in Table 7.2. The first column shows the statements on the information security culture that are placed together in dimensions that stem from the research framework's components; the second presents the utilised theoretical references and the guidance on statement development; and the third demonstrates an inclusion tick on whether the statements stem from the input obtained following the interview results.

**Table 7.2: Information Security Culture Questionnaire Operationalisation Statements**

| **Construct** | **Survey Items** | **References** |
|---|---|---|
| **Top Management** | TM1: Top management perceives information security as an important organisational priority. | (Knapp et al. 2006) |

| | | |
|---|---|---|
| | TM2: In my organisation, all levels of leadership are always involved in key information security activities. | (Alnatheer 2012) |
| | TM3: Top managers give strong and consistent support to the security program. | (Knapp et al. 2006) |
| | TM4: Top managers provide the required resources for training and learning to enable me to comply with information security requirements. | (Alhogail 2016) |
| | TM5: The involvement and support from top management has a significant role in establishing the security culture. | |
| **Security Policy** | SP1: The information security policy clearly states what is expected of me with regard to the safeguarding of information. | (DaVeiga & Eloff 2010) |
| | SP2: The contents of the information security policy prescribed by my organisation are easy to understand. | (DaVeiga 2018) |
| | SP3: The information security policy is applicable to the information I use in my daily tasks. | |
| | SP4: The written information security policy is important to create effective security culture. | Qualitative Data and expert's feedback. |
| **Security Education and Training** | SET1: The security-related training program explains what is expected of me, as well as the related information security requirements, policies and how to behave securely from the start of employment. | (Alhogail 2016) |
| | SET2: I received adequate information security training appropriate for my daily job duties. | (Knapp et al. 2006) |
| | SET3: I believe that it is necessary to have security refresher training on security policies or any updates in my organisation. | |
| | SET4: The appropriate information security education and training contribute to creating effective security culture. | (Alhogail 2016) |

| | | |
|---|---|---|
| **Risk Analysis and Assessment** | RA1: I believe the risk assessment processes of the organisation are adequate to identify risks that negatively impact on information security. | (DaVeiga & Eloff 2010) |
| | RA2: It is important to understand the security threats, vulnerabilities, and be alerted of any risks inherent to information assets in my workplace. | |
| | RA3: The security risk analysis and assessment are important in creating an effective security culture. | Qualitative Data and expert's feedback. |
| **Ethical Conduct** | EC1: It is important to have a clear ethical code of conduct and direction in protecting sensitive and confidential information by applying related regulations. | (Alhogail 2016) |
| | EC2: It is important to take care when talking about work or confidential information in public places. | (DaVeiga & Eloff 2010) |
| | EC3: The security-related ethical code of conduct is important for creating an effective security culture. | Qualitative Data and expert's feedback. |
| **Job Satisfaction** | JS1: I feel satisfied with the kind of work I do in this job. | (Spector 1997) |
| | JS2: I feel I am being paid a fair amount of money for the work I do. | |
| | JS3: I am satisfied with chances for promotion and rewards. | |
| | JS4: I am satisfied with the benefits I receive. | |
| | JS5: I feel satisfied with the organisation's level of supervision. | |
| | JS6: I like my co-workers. | |
| **Security Awareness** | SA1: I am aware of the information security policies and security aspects relating to my job for example, password policy. | (Alhogail 2016) |
| | SA2: I am aware of ongoing initiatives about security awareness. | |

| | | |
|---|---|---|
| | SA3: It is important to raise awareness about information security with employees. | |
| **Security Ownership** | SO1: Protecting information security is the responsibility of every employee in the organisation. | |
| | SO2: It is important that individuals are involved in the development of security policies in the organisation. | Qualitative Data and expert's feedback. |
| | SO3: It is important to have a sense of ownership regarding the organisational security practices to enhance the security culture of the organisation. | Qualitative Data and expert's feedback. |
| **Security Compliance** | SC1: It is important to follow the information security policies and practices such as not sharing passwords to enhance the security culture in the organisation. | (Alhogail 2016) |
| | SC2: The organisation enforces adherence to the information security policy. | (DaVeiga & Eloff 2010) |
| | SC3: I believe that the attention should be drawn on incidents of not adhering to the information security policies and requirements. | |

A total of five items are used to measure top management involvement in information security, which were taken and reviewed from Alnatheer et al. (2012); Alhogail and Mirza (2015); and Knapp et al. (2006). From Knapp et al. (2006) study, two items were used including the consideration of top management, about information security as an important organisational priority; and the continual support of information security programmes. The second item adopted from Alnatheer et al. (2012), includes the involvement of all leaderships in information security activities. Other two item from Alhogail and Mirza (2015) study. These items include providing the necessary resources to train employees in order to comply with required security measures, and employees' viewpoints and perceptions in relation to top management involvement and support as imperative to developing the information security culture.

Four different items are used to measure security policy. Three of items taken from Da Veiga (2018) and Da Veiga and Eloff (2010). These items include defining security policy clearly; whether the policy contents are easy to comprehend; and whether security policy is applicable to the daily tasks of the employees. A single item was developed for this research in order to

show the relevance of a written security policy that would create an effective and beneficial information security culture. This item was included in conjunction with the qualitative findings as interview respondents reported positive impacts of a written security policy. The findings also indicate that clear and sufficient security policies can increase relevant security-cautious behaviour through the enhancement of security awareness.

Four items used with regard to security education, two were adapted from the study by Alhogail and Mirza (2015). These two items included the security training programme content that details the related requirements; and the best ways to behave securely with the relevance of security education and training in advancing information security culture. Knapp et al. (2006) was used for two specific items, which included receiving sufficient security training and the value of security refresher training upon policy or organisational developments. Separately, three items were used in the measurement of security risk analysis and assessment. Two items adapted from Da Veiga and Eloff (2010), included the risk assessment processes as adequate in identifying the risks that negatively impact upon information security; the importance of understanding security threats, and to be alerted to any risks inherent to information assets in organisations. The third item stemmed from the findings of the qualitative interviews. As respondents demonstrated the benefits of risk comprehension that is involved in information security, which improved awareness and information security protocol, in order to have a better establish information security culture. This third item includes the importance of security risk analysis and assessment in creating an effective security culture.

Three items were used to measure ethical conduct. First, an item from Alhogail and Mirza (2015) study was included, which showed the importance to have a clear ethical code of conduct and direction in protecting confidential information. The second was adapted from Da Veiga and Eloff (2010), which included the relevance of exercising care when talking about work or confidential information in public spaces. Third, one item was implemented specifically for this research, which arose from the qualitative interviews. The respondents stipulated that ethical conduct policies are important in the development of organisational information security culture. These policies, support employees in the process of integrating ethical behaviour; secures information/data; and determines what an organisation accepts. This particular item focuses on the importance of an ethical code of conduct in developing an effective information security. Six items were used for the measurement of job satisfaction measurement, with the items used from Spector (1997). All six items focused on the following

points: employee satisfaction in relation to tasks; salary; potential for promotion and rewards; received benefits; the supervision level; and co-workers.

In this research, the measurement of information security culture was taken as a second-order construct. It included three sub-constructs as a first-order construct: security awareness, security ownership and security compliance. Three items were used to measure security awareness, which were all adopted from Alhogail and Mirza (2015) and Da Veiga and Eloff (2010) studies. The first item adapted from Da Veiga and Eloff (2010), which included how aware and familiar an employee was with their organisational security policy. The second came from Alhogail and Mirza (2015), which included the awareness of continual initiatives regarding security awareness. The third came from Alhogail and Mirza (2015), which included the relevance of increasing employees' security awareness.

Three items are used in the measurement of security ownership. The first item taken from Alhogail and Mirza (2015) focuses on the relevance of information security protection as part of the employee jobs. The other two items were developed for this research, due to a lack of validated tools from the reviewed literature that would work with the qualitative findings. The two items measured security ownership are: firstly, the importance of allowing individuals to become involved in their organisation security policy development; and secondly, the relevance of implementing a feeling of ownership that would improve the level of information security culture. These particular items were implemented following the findings from the interviews. Four of the respondents noted that improving employee security ownership would help in the promotion of acceptable information security culture levels. In regard to security compliance measurements, three items were adapted from Alhogail and Mirza (2015) and Da Veiga and Eloff (2010) studies. The first item was adopted from Alhogail and Mirza (2015), included the importance to adhere to an organisation security policy and practices. While two items were taken from Da Veiga and Eloff (2010). These two items are: first item, organisations enforced adherence to security policies; and second item, employee perceptions in relation to the attention that should be drawn on incidents of not adhering to the security policies and requirements.

### *IV. All About You*

This fourth section relates to Five Factor Model significant personality traits dimensions (FFM). It aims to present a better understanding of human personality traits and to identify

organisational predictive values for security behaviour. This section contains a total of forty-four items that cover these major five dimensions: agreeableness, conscientiousness, extraversion, neuroticism, openness (see Appendix J). All these dimensions were adapted from Goldberg (1993) and Shropshire et al. (2006) studies. This section was completed through a five-point Likert scale (1=strongly agree to 5=strongly disagree). (See Figure 7.1).

**Figure 7.1: Example of Statements Related to the Major Five Dimensions in the Questionnaire**

### 7.2.2 Measurement Scale

The measurement scale helped to ascertain data in regard to the measured variables (Martins & Eloff 2002). The selection of the measurement scale is taken after determining the focus of measurement, and the data or information that the measurement scale aims to obtain (Martins & Eloff 2002). Two groups of measurement scales were defined by Sekaran and Bougie (2016): ratings and rankings. Sekaran and Bougie (2016) also stated an additional ten methods of scale, with items chosen for a variety of constructs based on the five-point Likert (1932) scale. The Likert scale measured levels of agreement/disagreement in statements made by respondents, by showing perceptions and beliefs that would help to measure perception on factors that (a) influence information security culture and (b) those that reflect information security culture.

This scale has been used in many research studies relevant to this research such as Alhogail and Mirza (2015), Alnatheer et al. (2012), Da Veiga (2018), Knapp et al. (2006) and Martins and Eloff (2002). The Likert scale enables measurements and compares answers with different respondents in order to produce an aggregate score from a combination of the answers (Martins & Eloff 2002). The Likert scale varied from a 2-point Likert scale (Binary choice) of Agree and Disagree answers to a 7-points Likert scale, that depending on the question and potential

answers to avoid bias. For instance, binary choice questions are used in the process of obtaining particular data, which was implemented into the questionnaire with a “yes” or “no” answer.

The five-point Likert scale were used in this research. The five-point Likert scale helped in the measurement of the constructs’ operationally defined element from the proposed framework, and to determine the employee viewpoints of different factors that influence on information security culture (for more details see the survey in Appendix J). The concept categories were placed as: strongly agree = 1, agree = 2, neither agree/disagree = 3, disagree = 4 and strongly disagree = 5. The used scale example is represented in Figure 7.2. It is evident that these figures do not represent the true distance between perceptions but are sufficient to produce relevant results (McClendon 1994).

**Figure 7.2: Measurement Scale Example**

A separate scale was used for the knowledge section was (Yes/No or do not know). This scale measured information security knowledge levels and employee awareness. Figure 7.3 presents an example of this section.

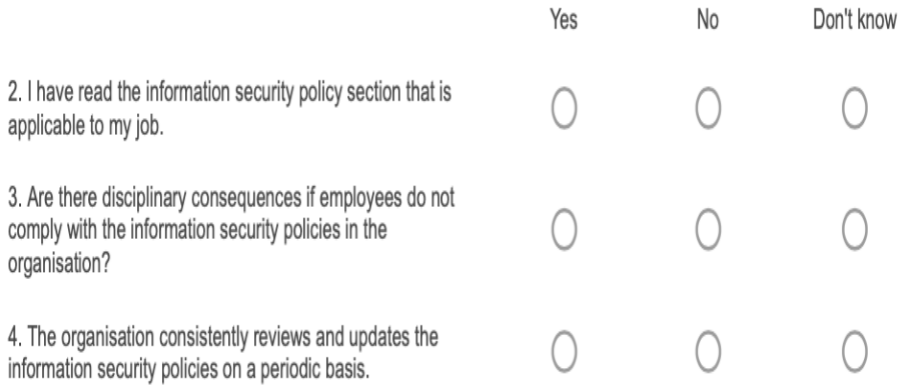



**Figure 7.3: Measurement Scale (Yes/No) Example**

The multiple choice/multi response scale (see Figure 7.4), was used for certain questions in the knowledge section, which contained a few potential selection options.

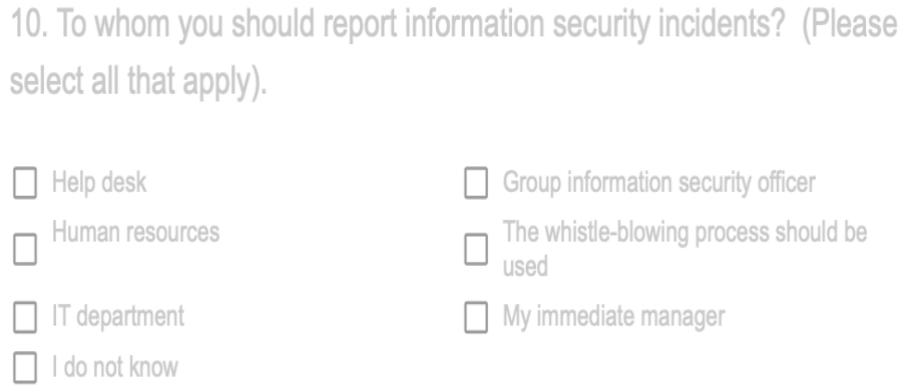



**Figure 7.4: Measurement Scale (Multiple choice) Example**

## 7.3 Questionnaire Pre-test

The questionnaire was pre-tested to ensure that questions would be understood correctly, as well as to identify possible problems with the wording (Sekaran & Bougie 2016). This would enable the researcher to predict and comprehend the reactions from the large group, as well as to redevelop the questions if required (Da Veiga 2008). Two distinct methods were used. A panel judgment helped to ensure validity of content; and secondly a pilot study identified potential ambiguous points, together with allowing the researcher to check whether the data functioned as anticipated (Sekaran & Bougie 2016).

### 7.3.1 Expert Review

The panel judgment incorporated expert reviews. The pre-test questionnaire was sent to experts to judge whether the items measured the presented theoretical construct. The expert review provided an assessment of the survey content validity. Reponses were requested on clarity, relevance, and the quality of items, as well as the relevance of the data collection tool.

The panel consisted of six renowned professional experts in the field of information security culture implementation and training. They were from education and consultant organisations working in information security culture practices. There were five academics with over fifteen years' experience in information security. One development director had over ten years of experience in information security culture and values. These individuals were contacted through sending an e-mail.

The experts were provided with a letter that detailed the research intent, and a guideline that includes the original copy of the questionnaire. The respondents were asked to complete the questionnaire and critique the parts that they believed can be improved from the initial design, as stated by Lewis et al. (2005), such as: content, format, potential misunderstandings, terminology, and ease to completion. They were also asked to provide feedback on the overall survey design and on various issues. These included: firstly, the clarity of instructions, questions, and measurements; secondly, how the measurement indicators were relevant to the structure of the information security culture; and thirdly, how the items affected each variable and provided additional comments for the items and measures in general.

The review experts gave insight into how to measure the information security culture. The review experts agreed that the designed questionnaire was functional and beneficial. However, certain changes were made to the survey following the review in order to increase readability. Various items were also changed, and items included following certain critique. Additionally, six items were rewritten, as this improved their meaning and comprehension, while four were shortened instead of changing the overall content. These modifications were applied to three sections in a survey. In the demographic section, three experts suggested additional options to the two questions: determining the organisational type by including a fourth option in the "other" form of organisation; and including "security staff" in the job level option.

Two experts suggested that a question should be included that would identify the industry or sector of respondent organisations. These two experts added that the survey results need to

present differences between industries, which could be stated through a specific "Organisation industry" question. A finance organisation could possibly produce different results from education, healthcare or retail. One expert suggested a question that would improve the level of clarity (see Question11), which included possible examples (see Table 7.3).

**Table 7.3: Survey-Demographic Section (Question 11)**

| The original question | The modified question |
|---|---|
| Did the induction include security awareness? | Did the induction include security information awareness about using and protection of data and organisation's information? |

Two of the experts stipulated that participants commonly answer statements that begin with "I know how" with "yes", as a low level of knowledge is often something that most people do not want to declare. It is better that statements are able to be made more indirect, as this will enable respondents to answer honestly in their answers; for instance, Statement number 3 was rephrased as shown in Table 7.4.

**Table 7.4: Survey-Knowledge Section (Statement 3)**

| The original question | The modified question |
|---|---|
| I know the problems associated with not complying with the information security policies in my organisation. | Are there disciplinary consequences if employees do not comply with the information security policies in the organisation? |

One expert stated that certain questions would require further clarity. The expert noted that some statements would need to be explained to the respondents. For instance, statement (17) inquired whether a respondent possessed security awareness and whether their organisations provided training sessions. The expert added that certain respondents sometimes regard information coffee sessions as a form of training, whilst other respondents received web-based training. The question should be converted to one that provided specific options, in order to avoid ambiguity (see Table 7.5).

**Table 7.5: Survey-Knowledge Section (Statement 17)**

| The original question | The modified question |
|---|---|
| Is there any security awareness/training available in the organisation? | Have you attended any security training in the organisation such as Induction training or Web based training? (**Please select all that apply :**) 1- Induction training. 2- Hands-on training sessions. 3- Web based training. 4- All the above. |

In the third part of information security culture practice and behaviour, three experts suggested adding item scales with a minimum of three to four statements for each dimension. This was particularly relevant in the current research, as it intends to complete factor and item analyses. Subsequently, each construct would have more than three items for each dimension. For instance, there were only two items for measurement in the security compliance construct, and thus, one item was added: "I believe that the attention should be drawn on incidents of not adhering to the information security policies and requirements". The experts said that certain statements were unclear, and would require re-wording, while the language would need to correspond with the terminology of the specific organisation. For instance, in the scale of security education and training, there was a statement that required re-wording, as it could be a yes/no answer and failed to determine respondent perception as shown in Table 7.6.

**Table 7.6: Survey-Information Security Culture Practice and Behaviour Section (Statement 3.3)**

| The original question | The modified question |
|---|---|
| There is security refresher training on security policies or any updates in my organisation. | I believe that it is necessary to have security refresher training on security policies or any updates in the organisation. |

The draft questionnaire was reviewed and adapted following comments from the experts. Various items were re-worded; another item was added prior to the questionnaire distribution.

### 7.3.2 Pilot Study

Following the review of the questionnaire, a pilot study was conducted with an educational institute in the United Kingdom. The pilot study aimed to test the questionnaire. This included:

question wording, sequence, format and structure, familiarity, response rates, general completion time, and analysis (Ticehurst & Veal 2000). The pilot study also aimed to review the questionnaire's face validity, and to ensure that the questionnaire can provide a measurement of information security culture. The content validity and reliability levels were evaluated in order to determine whether instructions and questions were understandable, as well as the scale of questions (Sekaran & Bougie 2016).

'Face validity' criterion (question wording, sequence and format) was tested prior to the survey distribution, as certain survey was sent via email to the faculty members who worked in the public organisation in November 2018. Data collection occurred during the pilot study for an original period of three weeks. Initially, only eleven employees from two different departments, and from different professional levels, participated in the pilot survey. One respondent was from a department of managers and supervisor, while ten of the respondents were operational staff members. All the respondents had worked in for their respective organisations for a period of four to ten years. The pilot showed that respondents would take, on average, approximately fifteen to twenty minutes to complete the survey.

The pilot study was used to measure the questionnaire in order to highlight parts that require change, ensure validity, and cover the main objectives of the research. The questionnaire was adapted before the final study. Respondents of pilot study in this research would not be invited for the final study, as it could negatively influence the reliability of the final results (Haralambos & Holborn 2000).

#### *7.3.2.1 Pilot Study Analysis and Results*

The questionnaire was tested on the eleven respondents stated previously. A reliable SPSS version 24 was used to analyse the survey results, which helped to determine how the questionnaire assessed what it was supposed to. The analysis results were promising and generally suitable for a pilot study, even though the pilot did produce a sample size that was less than ideal for the study (Kline 2005). The small sample size limited the amount of statistical analysis that can be performed on the data of this pilot study, although the data from the pilot study data were informative in two ways. Histograms and statistics on skewness and kurtosis were analysed to show whether the distribution of responses for the items/variables were bell-shaped.

The results of normal distribution tests determined that the skewness and kurtosis absolute values from the different variables had a range from (-1.112 to 0.949) and (-0.594 to 1.905), respectively; these fall within recommendation of value between (-2.00 to +2.00) (Hair et al. 2006). Second, through the use of the Cronbach's alpha test, the survey was assessed for its level of reliability, as this instrument produces measurements that are error-free and helps to determine the attitude items that measure the construct; thus, producing consistent results. The general reliability levels of the instrument within the pilot were $\alpha$=0.705 (70%), which falls within the recommendation threshold 0.7 for the study (Nunnally & Bernstein 1994). Also, a good level of internal consistency for the instrument that measured participants' attitudes was indicated from the individual construct reliability range between (0.520 to 0.876) as displayed in Table 7.7. Additionally, the items that failed to exhibit reasonable response variability levels were revised or removed.

**Table 7.7: The Shape of Data Distribution Based on Skewness and Kurtosis Values and Reliability**

| Construct | N | No of Statement | Cronbach's alpha α value | Skewness | | Kurtosis | |
|---|---|---|---|---|---|---|---|
| | | | | Statistic | Std. Error | Statistic | Std. Error |
| Top Management | 11 | 5 | 0.818 | 0.949 | 0.661 | 1.562 | 1.279 |
| Security policy | 11 | 4 | 0.791 | 0.437 | 0.661 | 0.745 | 1.279 |
| Security education & training | 11 | 4 | 0.871 | -0.864 | 0.661 | 1.033 | 1.279 |
| Risk analysis & assessment | 11 | 3 | 0.520 | 0.448 | 0.661 | -0.594 | 1.279 |
| Ethical conduct | 11 | 3 | 0.730 | 0.561 | 0.661 | 0.790 | 1.279 |
| Job satisfaction | 11 | 6 | 0.876 | 0.490 | 0.661 | 0.196 | 1.279 |
| Security awareness | 11 | 3 | 0.533 | 0.180 | 0.661 | 0.891 | 1.279 |
| Security ownership | 11 | 3 | 0.874 | -1.112 | 0.661 | 1.905 | 1.279 |
| Security compliance | 11 | 3 | 0.754 | -0.696 | 0.661 | 1.640 | 1.279 |
| Extraversion | 11 | 8 | 0.760 | -0.210 | 0.661 | 0.040 | 1.279 |
| Agreeableness | 11 | 9 | 0.820 | 0.640 | 0.661 | 0.911 | 1.279 |
| Conscientiousness | 11 | 9 | 0.654 | 0.708 | 0.661 | 0.720 | 1.279 |
| Neuroticism | 11 | 8 | 0.730 | -0.212 | 0.661 | -1.060 | 1.279 |
| Openness | 11 | 10 | 0.815 | 0.234 | 0.661 | 0.033 | 1.279 |

Notes: N: number of Responses, No of Statement: Number of Statement, Std. Error: Standard Error

The pilot test produced findings that were able to be used to improve the survey. Through the pilot study, minor amendments could be made to certain questionnaire statements in order to make sure that the respondents would understand the questions and maintain face validity accuracy. Certain statements that were unclear were reviewed and the comments from the participants in regard to the wording and structure were used to improve the survey. Some modifications were also conducted for the improved final questionnaire, including fixing grammatical errors. Similarly, certain statements or their particular wording required alterations following the pilot study, as this helped to improve the level of clarity. For instance, Question 14 from the knowledge section had its wording changed as demonstrated in Table 7.8.

**Table 7.8: Survey-Knowledge Section (Question 14)**

| The original question | The modified question |
|---|---|
| I am informed about information relevant legislation and regulations, such as of intellectual property and copyright laws. | I am informed by my organisation about information relevant legislation and regulations, such as of intellectual property and copyright laws. |

The final survey to be used included four individual sections. The first section was for demographics, which segmented the data and provided potential comparisons between respondents. The knowledge section was the second section, which determined and evaluated the security knowledge level of respondents, as well as their levels of awareness that would help to create an assessment of organisational security culture. The third section was the practice section for the information security culture, which helped to assess respondents' perspectives in relation to the factors from the framework, and to identify possible strengths or weaknesses in certain areas. The final section of the four was the personality test (all about you), which obtained a broad picture in regard to the respondent personalities.

In general, the pilot study showed that the respondents understood what was expected of them when completing the survey. The pilot was important to the overall study, as it enabled a clear format of questions that could be completed in a short period. The questions were easy to comprehend with a 5-point Likert scale suitably used, as shown in the literature review. The final survey was also revised, which provided approval of the new instrument to measure the specific phenomenon (see Appendix J).

## 7.4 Population and Survey Sampling

The process of sampling is vital to the overall research, as it helps to provide reasonably accurate findings. However, the selection of a representative sample is often challenging, as this is commonly dependent on the method of sample strategy that the researcher uses (i.e., probability or non-probability). With probability sampling is how the individuals from the target population have an equal opportunity to be included in the sample. Non-probability involves selection individuals through a non-systematic approach that does not guarantee full equality in opportunities for all those in the target population to be a part of the final sample. This method is commonly used when the implemented sampling frame remains unknown, which can include who or how many individuals, or in relation to limited time and costs matters

(Robson 2011). This research was limited in relation to both time and cost. Thus, the non-probability method was deemed to be the most beneficial to be used.

Access to the target population is often difficult. The collection of a high number of responses is easier if the researcher has inner relationships in an organisation. Therefore, convenience sampling and snowball sampling was used in this research. A convenience sampling technique was used in this research. The overall sample was developed by the number of participants willing to participate in the research. This technique helped to select cases that were easy to reach, and the set sample size was accessed through a continual process of selection. Also, a snowball sample method was used as part of the sample, which implemented after the study started. The researcher asked the respondents who completed the survey and were also able to invite or provide key access to other relevant individuals from their organisations, in order to participate in the survey of this research. This technique helped this research to gain easy access to different participants.

The selection of a target population helped to set the research's generalisability boundaries, which can often restrict the hypotheses that are produced from the conceptual framework (Baker 1994). In general, the selection of appropriate population assists in determining the most beneficial way of examining the proposed theories and hypotheses to draw the best findings and conclusion. The target population selected for this research were individual employees who work in any type of organisation. The target population included a representative sample of American, British and Saudi societies because this research interviewed thirteen employees from the United Kingdom, United State of America, and Saudi Arabia in the first phase of qualitative data collection.

It is always beneficial to send a questionnaire to different organisations from a wide range of sectors and industries, as this could present different security levels. The ability to compare between industry/sectors helps to demonstrate particular information security culture traits for each one, which can potentially result in different levels of investment in security awareness and relevant security training programmes (Roer & Pertic 2017).

Invitation emails, that contained a link of the online questionnaire, were sent to 600 organisations from a range of industries, that included education, health, and finance. Seven organisations had been part of the qualitative interview phase. The overall candidate sample was taken from organisations that comprised on a mix of private, public and semi-public

organisations. The sample finally included a range of organisations of different sizes. The size of organisations was based on the United States International Trade Commission's criteria (Okun et al. 2010). Access was difficult, which made it challenging to have a quantifiable balance between the small and medium (SME) and larger organisations. Although, there was an inclusion of all small, medium and large organisations. The organisations' demographic information is provided in Chapter 8, section (8.3.1).

In total, thirty individuals from six organisations originally declared interest and agreed to be part of the research. There were certain access difficulties to appropriate organisations. Some organisations refused to participate because of the restricted rules and regulations of discussing their security management to a third party, or to work commitments. The researcher then approached delegates to the 34th IFIP TC-11 International Information Security and Privacy Conference that hosted by University of Lisbon. Delegates were given a one-page invitation flyer that summarised the research project and contained a link that helped to complete the online questionnaire (see Appendix I). The conference delegates then invited relevant individuals from their organisations to participate in this research. Likewise, a member of the supervision team approached delegates to the 13th International Symposium on Human Aspects of Information Security and Assurance (HAISA) and invited them to cooperate in the research by given them the same invitation flyer. From this process, only 160 individuals declared interest in participation and completed the online questionnaire.

As a result of the low level of responses, which could be due to time restrictions and limited access to different organisations, the survey was posted online at https://www.callforparticipants.com. It resulted in a total of 106 respondents who completed the online questionnaire. The final total number of responses in this research was 266 respondents from a mix of the three countries (Saudi Arabia, United Kingdom and United State of America) and other countries such as Australia and South Africa. These respondents worked in different operational, technical positions and departments, comprising operational staff, administrative staff, IT staff, security staff, and managers. A representative sample of organisations was finally achieved. Moreover, the organisations' diversity of locations was considered a positive as it would help in advancing the understanding and improving information security culture comprehension phenomenon from different contexts and environments. Further details of the individual demographics of respondents are presented in the Chapter 8, section (8.3.1).

It is necessary to comprehend the correct sample size for a study to ensure the correct reliability and validity levels (Wolverton 2009). However, to specify the precise sample size is not a simple task. For instance, when the sample size is lower than the estimated size, this can create a greater potential for failure convergence and incorrect solutions, such as an estimation of negative error variance for variable measurements, as well as reduced accuracy of the parameter (Hair et al. 2006). A larger size of sample than required, would not be time effective nor economical, and the process of obtaining all the responses (Bryman & Bell 2007; Hair et al. 2006). Therefore, it is vital that the size of the sample is determined beforehand, in order to create a generalisation for the targeted population that enhances result reliability and validity. This research included a sample size of 266 respondents in order to achieve research objectives.

Nevertheless, it is imperative to reiterate that the method of data analysis for this research stems from Structural Equation Modelling (SEM), which correlates with multiple regression (multivariate analysis) and incorporates statistical techniques that include: Confirmatory Factor Analysis (CFA), structural path analysis (β), total variance extracted (R2), causal modelling with latent variables, analysis of variance and multiple regression. Correspondingly, many researchers such as Chin et al. (2003), and Hair et al. (2006) have stated that it is necessary to estimate approximate sample sizes for studies on SEM. The sample is selected by observing the most cited requirements within multivariate analysis and data analysis techniques, such as SEM using component-based or variance-based (e.g., PLS) techniques, as well as general approaches in the evaluation models that use SEM. For instance, Hair et al. (2006) noted that SEM studies normally use samples that are between 200 and 400 participants, which include 10-15 indicators. This research has examined a total 14 constructs with 58 items within the basic model. Additionally, Comrey and Lee (1992) indicated that a sample size of only 50 participants as very poor, with 100 as poor, 200 as fair, 300 as good, 500 as very good, and 1000 as excellent. The current research included a sample size of 266 respondents in order to examine different paths proposed in the framework for better estimates with reliability.

## 7.5 Questionnaire Process and Administration

Ethical issues were considered in the research methodology. Respondents were advised of reasons for the research and its potential risks and benefits. The questionnaire was included an initial cover letter, which described the research objectives, the time requirement to complete, and advising that participation was completely voluntary and that all details would remain confidential (see Appendix I). The informed consent was provided in the cover letter of a

questionnaire, as this would validate their responses and make the data legitimate. Also, the respondents were informed about the ability to withdraw at any moment without requirement of reason, while the researcher and the school ethics committee's contact details were provided. The respondents were informed that the questionnaire completion and its return would indicate willing consent to be defined as participating in the research. The relevant ethical clearance was obtained from Plymouth University Ethical Principles for Research Involving Human Participants.

The online questionnaire was selected for this research as it provided certain advantages for both the researcher and respondents. The format of an online questionnaire helped to protect privacy and enabled completion of the questionnaire at a convenient time (Singleton et al. 2009). For the researcher, the online questionnaire reduced the number of data-processing activities required and eliminated bias (Van Selm & Jankowski 2006). This research tool was sent as an invitation e-mail to the different organisations to initiate employee participation in the survey. These direct invitation emails detailed the research purpose and contained a link to the online questionnaire with the message written in English. The potential respondents were asked to participate and to invite other relevant employees from their organisations to participate. Six hundred emails were sent to organisations. This questionnaire was posted on the online website of https://www.callforparticipants.com, which resulted in a total of 266 final respondents participated in this research.

The design of the questionnaire and its implementation were conducted through the software and web-hosting service of Qualtrics.com, which enables links to the survey to be shared with all the responses recorded on a spreadsheet (i.e., information on the exact time and date of response). The full English written questionnaire remained open to take responses for a period of twelve months, which started from the day of sending the invitation to the organisations. The allocated time required to answer the full questionnaire was shown as fifteen to twenty minutes, with the respondents able to answer the questions in their own time and convenience. Additionally, the responses were monitored in order to ensure that statistically representative number of responses were achieved, and to ensure that the demographical groups were evident. Subsequently, the obtained data from the information security culture questionnaire was taken and prepared to be analysed.

## 7.6 Conclusion

This chapter presented the development and administrations of the survey instrument with the objective to validate the research framework. The content of survey was developed into four individual sections. The first section for demographics related to respondents. Then, the knowledge section in order to determine and evaluate the security knowledge level and awareness levels of employees. The third section was information security culture practices in order to assess employees' perspectives and perception toward the framework factors. The last section was the personality test using FFM in order to provide a good comprehension of human personality and possess organisational predictive values for security behaviour. Different measurement scales were used in the survey: 5-point Likert scale, Yes/No or Don't know scale and multiple-choice scale. After developing the survey content, a pre-test was utilised using two methods to ensure the validity and reliability of the survey. First, six professional experts in the field of information security culture implementation review the survey and some part of survey was modified based on the reviewer feedback. Then, a pilot study conducted with eleven respondents and the results were analysed. The results of pilot study showed that the survey was clear and easy to understand. The questions were easy to comprehend with a 5-point Likert scale suitably used. The final survey was also revised and developed. Also, the population and survey sample has been detailed. The target population for the present research was individual employees working in an organisation. The size of the sample was selected using non-probability sampling method with convenience and snowball techniques. The survey administration and process were explained. The data collection process is based on e-mail and online questionnaire method. The empirical research's analysis and findings from the quantitative phase are documented in the following Chapters 8 and 9.

# Chapter Eight :

# Empirical Study Analysis and Quantitative Results

## 8.1 Introduction

The empirical results from the survey analyses are detailed in this chapter based on the process described in Chapter 4 (section 4.5.2) and Chapter 7. Following the introduction, the first section presents data screening with statistical forms, and particular output, which includes: missing data treatment, normality, and common method bias. The next section provides demographic characteristics for descriptive statistics, security knowledge results, statistics regarding the factor variables that influence the culture of information security, and the factors that reflect information security culture. Also, this section provides the interpretation of the mean values that obtained from the constructs and variables measured.

An inferential analysis is presented with Partial Least Squares (PLS). This section provides the assessment reliability of the internal consistency and item-total correlations, and validity of the instrument. Factor analyses were applied to determine the structures that demonstrate the framework constructs. The Exploratory Factor Analysis (EFA) was performed to determine the main constructs of the framework. Following this, the subsequent section is vital, and is divided into four sections. The initial section presented the Structural Equation Modelling (SEM) techniques, as well as the practical considerations and justifications for the utilisation of Partial Least Squares (PLS). The second section presents a two-stage process to analyses the developed framework of this research. The measurement model is confirmed for the first stage through Confirmatory Factor Analysis (CFA) in order to improve the structure of the constructs, as this will ensure the reliability and validity levels. After establishing the unidimensionality, the second stage shows an evaluation of the structural equation model with the framework's substantive relations. This stage focuses on the correlation between research framework constructs and research hypotheses tests. The fourth section presents an overview of the Multiple Group Analysis (MGA) process. The last section presents a chapter conclusion.

## 8.2 Data Analysis

Following data collection, data analysis was conducted statistically through specific techniques. In accordance, the Statistical Package for the Social Sciences (SPSS) version 24 and Smart PLS version 3.3.2 were used. The complete collected data was then converted to the SPSS format in order to conduct analysis. SPSS organised the online data and prepared the data to be ready for Structure Equation Modelling analysis that would import Smart PLS. Prior to the data analysis, the data was examined and prepared before the sample's descriptive

statistics were revealed. Subsequently, Exploratory Factor Analysis was undertaken; Confirmatory Factor Analysis was conducted to evaluate the measurement model and structural model. The results as shown from these particular stages are provided in the following subsections.

### 8.2.1 Data Preparation and Screening

Data preparation involves coding responses, data entry to a database, data filtering, and locating missing responses. Data preparation and screening was an important step to ensure the validity of the survey responses. Data screening helps in ensuring the accuracy of collected data, there is no missing data and addressing the issue of response-set, outliers or cases with patterns of scores that are extreme or not normal.

After downloading the survey responses, a screening procedure of the data sets was performed with the use of multiple regression and residual analysis. Data screening was conducted with the SPSS statistical package, which generated exploratory analyses for the variables and checked data entry accuracy, missing values, outliers, normality, response bias and common method bias. The most important step in the data screening process was to show values that were coded incorrectly or out-of-range (Pallant 2011). A frequency test was conducted for the different variables to determine these values. These test results showed no out-of-range or incorrectly coded responses found. For the PLS-SEM analysis purposes, Smart PLS was used to provide an analysis of the measurement and structural models. Data was transferred onto a Microsoft Excel CSV file, which generated raw input. The following section presents the survey data screening procedures that were used to produce the statistical analyses suitability.

#### *8.2.1.1 Missing Data Analysis*

One of the most common issues with data analysis stems from missing values, as questionnaires that are not completed fully could create bias in the results. Indeed, missing data is often found when participants fail to respond to a particular question or when there are omissions in the collected data. Missing data causes problems for the statistical analysis, as reducing the sample size due to missing data lowers the statistical power, and thus, calculated estimates can become biased to generalised (Corderio et al. 2010). Also, Hair et al. (2006) remarked that when solutions of missing data are not applied correctly, there is a resulting reduction in the sample relevance, which produces an insufficient sample from the analysis.

From a substantive perspective, the empirical results from the data that contain non-random missing data could potentially be bias, and consequently result in false results.

The missing data is classified into two types either 'ignorable', which can be part of a survey instrument without the need for remedy, or 'not-ignorable', which is due to either procedural factors. These can include errors during the process of data entry or failures to enter all the entries, or refusal to answer certain items within the instrument. Hair et al. (2006) recommended four stages that would help to overcome the above issues of missing data: firstly, an examination of the type of missing data; secondly, an examination of the amount of missing data; thirdly, an examination of the missing data's randomness; fourthly, apply different remedies, such as the imputation method. An examination of missing data was carried out in this research.

In this research, no items were included as part of the questionnaire that required to be un-answered; hence, ignorable missing data were not a possibility. Through a comparison of the original questionnaires with data entries in SPSS, the data was checked for missing data in order to correct potential incorrect data entries errors. The result indicated that there were no missing values. Missing data were not relevant to this research as the participants were required complete the entire survey.

#### *8.2.1.2 Assessment of Normality*

The assessment of how impactful the violation of the normality assumption was shown to be imperative to the study. Statistical tests, which rely on normality assumptions, could potentially not be valid. The term 'normality' relates to the data distribution shape in regard to it becoming a variable, and the correspondence to 'normal' distribution (Hair et al. 2006). There are two forms of normality: univariate, which show the degree to which the data distribution of a particular variable connects to a normal distribution, such as score distribution at an item-level. The second type is multivariate, which is a normal joint distribution in excess of one variable, such as the score distribution when in excess of two items are combined (Hair et al. 2006).

The assessment of normality is able to be undertaken visually (Hair et al. 2006). The visual process enables a researcher to observe how a variable data histogram connects with a bell-shaped curve. However, a researcher generally adheres to two vital parts of normality (Tabachnick & Fidell 2007): 'skewness', which indicates the distribution symmetry; and 'kurtosis', which provides data in regard to the 'peakedness' or 'flatness' of the distribution

levels in comparison to normal distribution (Hair et al. 2006). When skewness is positive, it indicates that the distribution has moved to the left and tails off to the right; comparatively, negative skewed distribution is in the opposite. In the relation to kurtosis, the negative value indicates a flatter distribution, while the positive shows a peaked distribution level (Hair et al. 2006). Both the distribution's skewness and kurtosis need to become between (-2.00 and +2.00) in order to present a normal distribution level (Hair et al. 2006).

Even though PLS-SEM is a non-parametrical statistical method, and a normal distribution is not a requirement, it is recommended that the normality of data distribution is reviewed. The current research conducted an examination of normality in order to set a preliminary assessment of the data distribution for the different variables. This examination would help to justify the utilisation of particular statistical analysis procedures. The normal distribution tests' results showed that the skewness and kurtosis values for the variables had a range of (0.223 to 1.090) and from (-1.098 to 1.150), respectively. This range is within the previously stated recommendation (-2.00 to +2.00); the results provide support and justification for the data set's normality. The descriptive analysis contained values are presented in Table 8.1 and for all items in Appendix L.

**Table 8.1: Data Distribution Shape Based on Skewness and Kurtosis Values**

| | **N** | **Minimum** | **Maximum** | **Mean** | | **Std. Deviation** | **Skewness** | | **Kurtosis** | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Construct** | **Statistic** | **Statistic** | **Statistic** | **Statistic** | **Std. Error** | **Statistic** | **Statistic** | **Std. Error** | **Statistic** | **Std. Error** |
| Top Management | 266 | 1 | 3.6 | 2.144 | 0.035 | 0.570 | -0.178 | 0.149 | -0.476 | 0.298 |
| Security policy | 266 | 1 | 4 | 2.116 | 0.041 | 0.674 | 0.085 | 0.149 | -0.387 | 0.298 |
| Security education & training | 266 | 1 | 3.67 | 2.216 | 0.037 | 0.610 | -0.214 | 0.149 | -0.394 | 0.298 |
| Risk analysis & assessment | 266 | 1 | 4.33 | 1.905 | 0.036 | 0.589 | 0.626 | 0.149 | 1.150 | 0.298 |

| Construct | N | Minimum | Maximum | Mean | | Std. Deviation | Skewness | | Kurtosis | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Statistic | Statistic | Statistic | Statistic | Std. Error | Statistic | Statistic | Std. Error | Statistic | Std. Error |
| Ethical conduct | 266 | 1 | 4 | 1.662 | 0.041 | 0.675 | 1.090 | 0.149 | 0.997 | 0.298 |
| Job satisfaction | 266 | 1 | 4 | 2.191 | 0.037 | 0.607 | 0.158 | 0.149 | -0.17 | 0.298 |
| Security awareness | 266 | 1 | 3 | 1.747 | 0.032 | 0.523 | 0.163 | 0.149 | -0.472 | 0.298 |
| Security ownership | 266 | 1 | 3 | 1.650 | 0.033 | 0.542 | 0.425 | 0.149 | -0.472 | 0.298 |
| Security compliance | 266 | 1 | 3 | 1.790 | 0.033 | 0.532 | 0.211 | 0.149 | -0.419 | 0.298 |
| Extraversion | 266 | 1.25 | 3.5 | 2.254 | 0.026 | 0.424 | -0.018 | 0.149 | 0.059 | 0.298 |
| Agreeableness | 266 | 1 | 3.78 | 1.970 | 0.029 | 0.470 | 0.663 | 0.149 | 0.939 | 0.298 |
| Conscientiousness | 266 | 1 | 3.67 | 1.912 | 0.029 | 0.477 | 0.808 | 0.149 | 0.719 | 0.298 |
| Neuroticism | 266 | 1.5 | 4.75 | 3.306 | 0.053 | 0.865 | -0.223 | 0.149 | -1.098 | 0.298 |
| Openness | 266 | 1 | 3.2 | 2.010 | 0.027 | 0.433 | 0.279 | 0.149 | 0.012 | 0.298 |

Notes: N: number of Responses, Std. Error: Standard Error, Std. Deviation: Standard Deviation

Further assessment for multivariate normality was undertaken through the residual analysis using normal Probability Plot (P-P plot) for the regression residuals, with a graph displayed between observed and expected values. A variable has a normal distribution level within the P-P plot when the graph's points are clustered around a straight line (Field 2009). In this research, the P-P plot demonstrated a suitable normality level for top management, where the standardised predicted value presented a line with standardised residuals as shown in Figure 8.1 and Appendix K for all constructs.

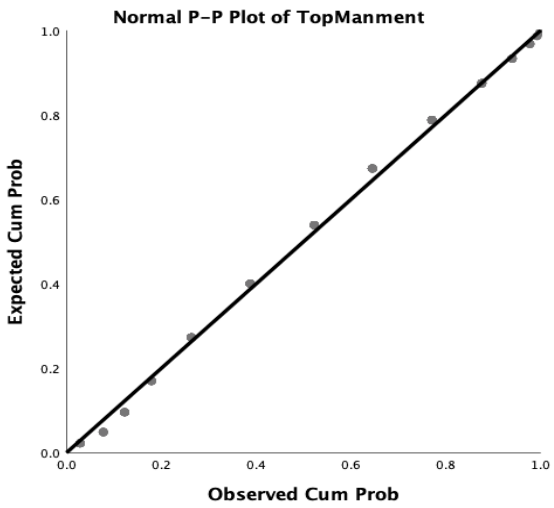



**Figure 8.1: An Example of Multivariate Normal P-P plot of Regression Standardised Residual for Top Management**

### *8.2.1.3 Outlier Screening*

Hair et al. (2006) defines an outlier as a significantly different observation from other ones or with additional characteristics. An outlier is sometimes present within datasets, as a result of incorrect data entries, which is caused by the presence of cases that fail to be part of the intended population (Hair et al. 2006). An outlier can potentially represent a true point of data. Thus, it is vital that screening is undertaken in order to detect the outliers, as these can often result in bias affecting the mean level and increase the standard deviation (Tabachnick & Fidell 2007). Outliers prove detrimental upon data distributions normality and can often be a negative factor upon SEM data analysis (Byrne 2010). Outliers can be either univariate, which is an extreme value observed for a single variable; or multivariate, which is a response with extreme data values for in excess of two different variables (Tabachnick & Fidell 2007). However, there are certain commonly accepted rules that determine a case is outlier within univariate outliers due to two possibilities. Firstly, there is a standard score for a small sample size (<80), which is -2.5 or +2.5 or more, while a standard score for a larger sample size can be considered <=4. Secondly, when a value is in excess of + 3.0 or – 3.0, then the standard deviations that are in excess of the mean may be considered as outliers (Kline 2005).

In this research, a total of sixty-three items were grouped together to represent a single variable, in order to detect such the extreme deviations. The SPSS function of descriptive statistics was used in order to convert the data values of the observations into standardized z-scores. The cases with a total z-score (|z|) value < -3.29 or > 3.29 at $p < 0.01$ were determined to be potential

outliers. For any variable, the number of such an outlier need not exceed 1%, approximately (Tabachnick & Fidell 2007). Three constructs were present in this research (risk analysis and assessment, agreeableness, conscientiousness) had an absolute z score >3.29. There are various ways of how to handle and work with variable outliers. Moderate outliers that have a minimal impact upon a model could be kept, while severe outliers need to be addressed (Chin 2010). The process of trimming can help to deal with severe outliers (Kettaneh et al. 2005). Trimming involves separating the variables and eliminating or changing a small percentage of the extreme ones (commonly 1% to 5%). It is possible to determine whether these variables are noted as acceptable cases, as when an outlier has occurred because of certain measurement errors, it then becomes possible to implement trimming.

In order to ensure that the outliers do not drastically change the data, the evident differences between the mean and the 5% trimmed mean for each variable have been examined and compared to the mean of each component. This 5% trimmed mean is calculated after the removal of the top and bottom 5% from the data set. The differences between the mean and the 5% trimmed need to be ($\leq$0.20), as this will indicate that the data does not include any outliers that can potentially result in a distortion to the data set (Pallant 2010). In this research, all the calculated mean differences ($\Delta$ mean) were small in comparison to 0.20 (ranged from -0.01 to 0.06) as shown in Table 8.2. Therefore, it can be noted that the data sets were not affected detrimentally by the detected outliers.

**Table 8.2: Data Outlier Screening**

| Construct | N | Mean | 5% Trimmed Mean | Δ Mean |
|---|---|---|---|---|
| **Agreeableness** | **266** | **1.97** | **1.95** | **0.020** |
| **Conscientiousness** | **266** | **1.91** | **1.89** | **0.022** |
| Ethical conduct | 266 | 1.66 | 1.60 | 0.062 |
| Extraversion | 266 | 2.25 | 2.25 | 0.004 |
| Job satisfaction | 266 | 2.19 | 2.18 | 0.011 |
| Neuroticism | 266 | 3.31 | 3.32 | -0.014 |
| Openness | 266 | 2.01 | 1.99 | 0.020 |
| **Risk analysis and assessment** | **266** | **1.90** | **1.87** | **0.035** |
| Security awareness | 266 | 1.75 | 1.72 | 0.027 |
| Security compliance | 266 | 1.79 | 1.76 | 0.030 |
| Security education & training | 266 | 2.22 | 2.21 | 0.006 |
| Security ownership | 266 | 1.65 | 1.61 | 0.040 |
| Security policy | 266 | 2.12 | 2.10 | 0.016 |
| Top Management | 266 | 2.14 | 2.14 | 0.004 |

Notes: N: number of Responses, Δ Mean= Mean – 5% Trimmed Mean

Multivariate outliers could be identifiable based on the measurement of Mahalanobis distance $D^2$, which is also known as a multidimensional version of the z-score (Hair et al. 2006). Tabachnick and Fidell (2007) stated that the Mahalanobis distance is a case distance from the centroid of the remaining cases where the centroid is created at the intersection of the different variables' mean levels. This method assisted in measuring the observed distances in the multidimensional space, which is taken from the different observed centre point mean in order to determine a single value (Hair et al. 2006). It has also been stated that if case $D^2/df$ has a great value than 2.5 in a small sample, as well as 3 or 4 in a large sample, then it is considered as a possible outlier (Hair et al. 2006). A conservative statistical test of significance ($p< 0.001$ or $p<0.005$) is used with the Mahalanobis distance measure, where the greater the $D^2$value for a case the smaller the corresponding value of probability is, and thus, considered to be an outlier (Tabachnick & Fidell 2007).

In this research, a liner regression method was used for the calculation of the Mahalanobis $D^2$ value in order to review multivariate outliers. The function of SPSS was used to calculate the *p* value from the *chi*-square distribution with *df* 1-CDF.CHISQ(quant, df), where quant = $D^2$and df=11 in order to ascertain the t-value of significance. This produced results that highlighted cumulative probability as a value from the chi-square distribution level $D^2$ that included relevant freedom with a lower amount than the quant. The *p* values for the computed Mahalanobis $D^2$ are higher than 0.001. The lowest *p* value was 0.002; thus, the variables did not have multivariate outliers at the 0.001 significance level. Consequently, there were no evident outliers that would affect the data and be held for additional analysis.

#### *8.2.1.4 Common Method Bias (CMB)*

The common method variance shows what variance is attributable to the method of measurement, instead of in regard to the constructs that are represented (Podsakoff et al. 2003). Those variances that are due to the measurement can cause problems, as they may result in errors (Podsakoff et al. 2003). The literature on this matter has also shown different causes for the common method bias, as questionnaire misunderstandings, question difficulties, and participants' failure to apply cognitive skills can all prove detrimental (MacKenzie & Podsakoff 2012); as well as fearing being identified; challenges in responding (Podsakoff et al. 2003). Overall, the data was assessed to obtain the potential level of common method bias, and various tests were undertaken to highlight any signs of CMB.

Certain methods exist that can test CMB and Harman Method one of these test (Bagozzi Yi et al. 1991). The Harman method is a single factor test that statistically evaluated whether a common method bias was present. This type of method examines the results of the un-rotated factor solutions, whilst stating the number of factors that accounted for the overall variable variance (Koh & Kim 2004). Two conditions help to determine the level of common method bias (CMB): firstly, when the factor analysis shows a single factor; and secondly, when a single general factor comprises the majority of the co-variance in both independent and criterion variables. When a certain factor can be seen that is >50% of the explained variance, then it can be concluded the data set suffers from CMB (Podsakoff et al. 2003). The Harman test was conducted through SPSS by using Exploratory Factor Analysis with extraction method of principle component analysis (PCA). This helped in the assessment of the CMB issue and examined how most of the model's variances could be explained by one factor. A total of

fourteen factors were indicated that had eigenvalues >1, with the first factor explaining a variance of 20.5%. This confirmed that there was no problem with the CMB, as the study's first factor does not explain a major variance and none of the factor was found apparent. The influence of common latent factor was evaluated in the measurement model. The findings showed no significant changes in the newly tested model, which demonstrates that the CMB is not a problem in this research.

Additional tests such as collinearity test supported results as recommended by Kock (2015), who presented a practical approach that would test the CMB in PLS-SEM. This stems from the variance inflation factors that are produced through a full collinearity test. Kock (2015) showed that the complete collinearity test is beneficial in identifying a model's common method bias which nonetheless adheres to the assessment of standard convergent and discriminant validity criteria based on the confirmation factor analysis. Variance inflation factors (VIFs) are generated with this procedure for all latent variables (LVs) in a model. When the proposed VIF is >3.3, it can be determined as an extreme collinearity, and that the model is potentially contaminated by the common method bias. In this research, VIFs are created for the model's LVs by using SmartPLS during the analysis. In total, all VIFs are <3.3 as shown in Table 8.3, which highlights that common method bias is not evident in the framework. In regard to the structural model of this research, the collinearity level among the predictor constructs was not an issue.

**Table 8.3: Collinearity Assessment**

| Construct | VIF |
|---|---|
| Agreeableness | 1.174 |
| Conscientiousness | 1.177 |
| Ethical conduct | 1.764 |
| Extraversion | 1.054 |
| Job satisfaction | 1.291 |
| Neuroticism | 1.029 |
| Openness | 1.257 |
| Risk analysis & assessment | 1.737 |
| Security education & training | 1.784 |
| Security policy | 1.956 |
| Top Management | 1.805 |

Note: VIF: Variance Inflation Factors

Better and more advanced approaches are also potentially applicable to test common methods bias, which include a leading approach with PLS that incorporates a marker variable in the collection of data which is not connect to the model (Lindell & Whitney 2001). Additionally, common methods bias potentially exists when the data correlations to the marker variable are elevated. In this research, the bivariate correlation matrix was calculated using Pearson's correlation in SPSS (see Table 8.4). The results revealed that there was not any bivariate correlation in excess of 0.8 for independent variables and that multicollinearity was not present.

**Table 8.4: Correlations Among Components of Information Security Culture with Key Factors**

| # | Construct | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Top Management | 1 | | | | | | | | | | | | | |
| 2 | Security Policy | 0.613 | 1 | | | | | | | | | | | | |
| 3 | Security Education & training | 0.38 | 0.426 | 1 | | | | | | | | | | | |
| 4 | Risk Analysis | 0.387 | 0.421 | 0.321 | 1 | | | | | | | | | | |
| 5 | Ethical Conduct | 0.352 | 0.445 | 0.327 | 0.517 | 1 | | | | | | | | | |
| 6 | Job Satisfaction | 0.323 | 0.384 | 0.275 | 0.266 | 0.214 | 1 | | | | | | | | |
| 7 | Agreeableness | 0.18 | 0.143 | 0.119 | 0.18 | 0.221 | 0.071 | 1 | | | | | | | |
| 8 | Conscientiousness | 0.028 | 0.123 | 0.102 | 0.132 | 0.172 | 0.018 | 0.127 | 1 | | | | | | |
| 9 | Extraversion | 0.121 | 0.145 | 0.096 | 0.154 | 0.176 | 0.095 | -0.03 | 0.03 | 1 | | | | | |
| 10 | Neuroticism | 0.037 | -0.003 | 0.051 | -0.02 | 0.022 | -0.031 | 0.026 | -0.128 | 0.058 | 1 | | | | |
| 11 | Openness | 0.136 | 0.26 | 0.163 | 0.218 | 0.26 | 0.235 | 0.169 | 0.192 | 0.12 | 0.017 | 1 | | | |
| 12 | Awareness | 0.527 | 0.563 | 0.393 | 0.49 | 0.485 | 0.244 | 0.22 | 0.107 | 0.154 | -0.03 | 0.232 | 1 | | |
| 13 | Ownership | 0.456 | 0.438 | 0.287 | 0.489 | 0.493 | 0.281 | 0.269 | 0.252 | 0.004 | -0.07 | 0.25 | 0.521 | 1 | |
| 14 | Compliance | 0.528 | 0.5 | 0.356 | 0.54 | 0.569 | 0.351 | 0.237 | 0.209 | 0.187 | -0.05 | 0.28 | 0.54 | 0.588 | 1 |

Note: correlation is significant at the 0.05 level (2-tailed).

## 8.3 Questionnaire Results

This section presents the quantitative results of a survey. The entire data was collected (between December 2018 and December 2019), with an exploratory survey distributed via e-mail with an invitation to 600 different organisations to fill in the questionnaire online. Companies were a range of sizes and geographical locations; the United Kingdom, the United State of America, Saudi Arabia and other countries. The respondents came from a mix of hierarchical levels in their organisations, as well as locations, backgrounds, levels of qualification/education, and age groups. A total of 266 surveys were ultimately completed with valid and useful responses for the research, which were then collated and combined for analysis. The questionnaire quantitative results have been shown through relevant tables and graphs, as shown below.

### 8.3.1 Demographic Data

The demographic information examination has been used to determine whether the sample is able to sufficiently demonstrate characteristics of the survey population, as well as to comprehend the relationship between their individual profiles and information security culture. The following categories were used to classify the participants: firstly, type, industry, size of organisations in which they were employed. Secondly, participants gender, age, country of

residence, background and education in IT field, employment period in their organisation, and job level. Thirdly, the prevalence of induction training, which included information security.

The following sections present the detailed findings of respondents' profiles. It is necessary that the type, industry, organisational size are detailed in order to understand characteristics of the overall population.

### *Type of Organisation*

Organisational type was categorised in three groups. The respondents from various organisations came from both public, private and semi-public sectors (52%, n=139), (43%, n=113), and (5%, n=14) respectively and presented in Figure 8.2. The sample provides a good representation among two categories (public and private). It would be ideal for this research to examine the possible impact of organisations type on relationships between variables in this research, as this could create different knowledge, values and perceptions that may influence information security culture.

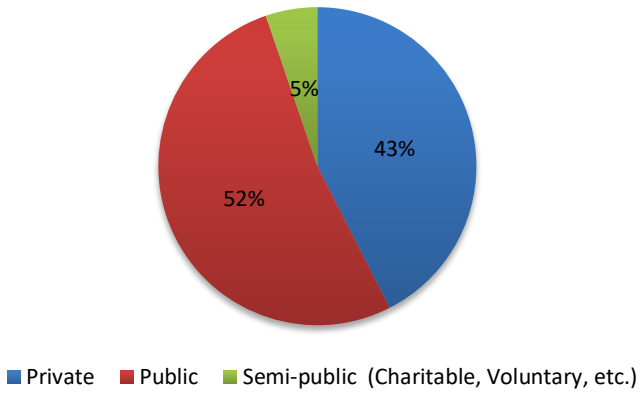



**Figure 8.2: Organisational Types**

### *Industry*

Responses came from various organisational industries, with the largest number coming from education and training industry (46.2%, n=123), and then the medical and healthcare industry (10.6%, n=28) as presented in Table 8.5. The majority of participants were of educational and training institutes, so there is a limited concentration of views or cultural influences from just one major group.

**Table 8.5: The Industries of Organisations**

| Organisation industry | Frequency | Percentage |
|---|---|---|
| Construction | 8 | 3.0% |
| Consultant | 14 | 5.5% |
| **Education/ Training** | **123** | **46.2%** |
| Energy | 2 | 0.8% |
| Finance/ banking | 11 | 4.1% |
| Industrial Tech | 4 | 1.6% |
| Information and communication technology | 14 | 5.3% |
| Insurance | 2 | 0.8% |
| Manufacturing | 3 | 1.2% |
| Medical/Healthcare | 28 | 10.6% |
| Merchandising | 5 | 1.9% |
| Oil/gas | 4 | 1.6% |
| Retail/Wholesale | 14 | 5.5% |
| Telecommunication | 4 | 1.6% |
| Transportation | 6 | 2.4% |
| Utilities | 8 | 3.0% |
| Others | 16 | 6.0% |
| **Total** | 266 | 100% |

### *Number of Employees in Organisations*

The sizes of different organisations that have been reported have appeared to represent a mix of companies. Small, with 250 employees or less (32.3%); medium, 250 to 1000 employees, (23.2%); large with excess of 1000 employees (45.1%), (see Figure 8.3). The sample is a representation across three sizes of organisations. The findings present perspectives from

respondents with a range of work experience and organisational cultural influences. Therefore, it would be interesting for this research to investigate the effect of the organisation size categories on the variables of this research, as this might establish different level of information security culture in each group.

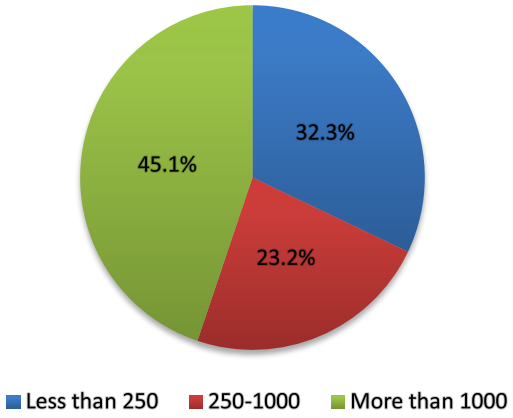



**Figure 8.3: Number of Employees in Organisations**

It is important that gender, age group, country of residence, background and education in IT field, length of employment and their level within organisations are considered.

***Gender***

The sample provided a gender balance with females at 55.3% (n=147) and males at 42.5% (n=112), as displayed in Figure 8.4. This indicates that the sample presents different views and perspectives from participants. However, several studies revealed evidence of gender differences in relation to their beliefs and behavioural intentions for information security (Anwar et al. 2017; McGill &Thompson 2018). Therefore, it was important to examine the impact of gender differences on relationships between variables of this research. This examination might illuminate differences and similarities in knowledge, values and decision-making which may affect the organisational security behaviour and thus the level of information security culture.

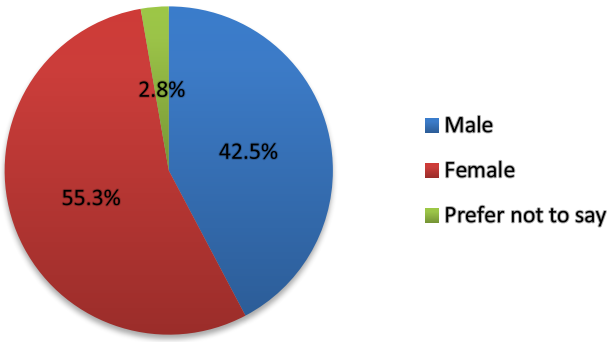



**Figure 8.4: Participants' Genders**

### *Age*

There was an age range of less than 25 years and over 56 years. 20.1% were less than <25 years old; 42.9% between 25 and 35 years old; 23.2% as between 36 and 45 years old; 9.1% as 46-55 years old; and 6.3% were above >56 years of age, (see Figure 8.5). The majority of respondents were between the age of 25 and 35 years. Taking into consideration that the participants seem to dramatically decrease in number as they get older. Thus, it would be interesting to check if the age difference would influence the relationship between key factors and information security culture in this research.

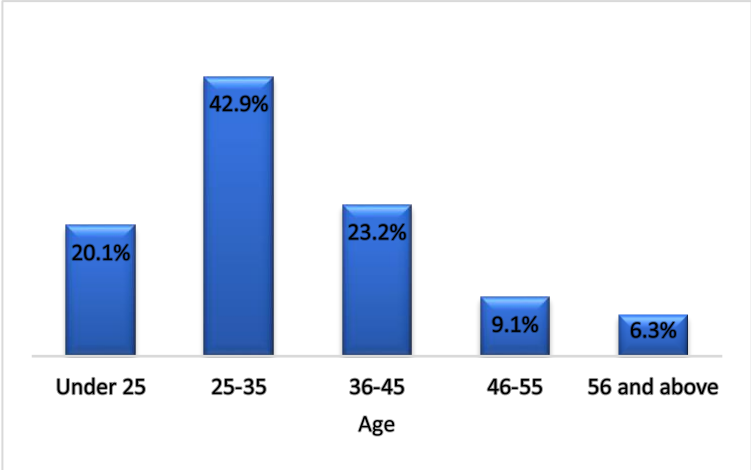



**Figure 8.5: Participants' Ages**

### *Country of Residence*

The sample was split into three categories: respondents from United Kingdom, Saudi Arabia and Other. The response rate from the United Kingdom was (33.4%, n=89), Saudi Arabia (31.5%, n=84) and Other (35.1%, n=93), as displayed in Figure 8.6. The sample provides a

good representation across two countries (United Kingdom and Saudi Arabia). Therefore, it would be interesting for this research to investigate the possible difference effect of these two countries on relationships between key factors of this research. This could create different knowledge, values and perceptions, which may affect the organisational security behaviour and the level of information security culture.

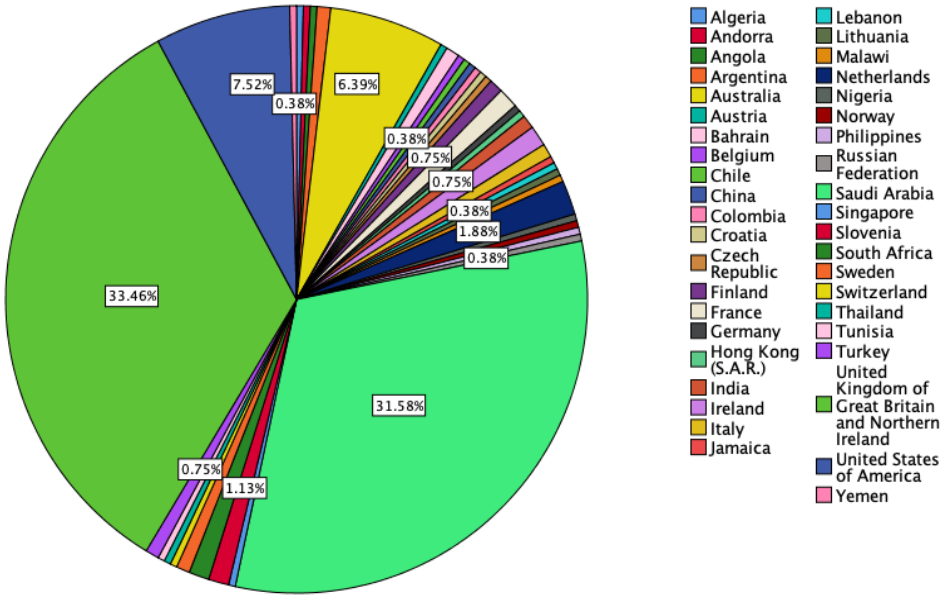



**Figure 8.6: Different Nations**

***Education and Qualification Level in an IT Related Context***

Most of the participants had not received formal education in an IT context (62.4%, n=166). This information might help this research to figure the impact of the participants education background on the security culture and to find any relationship between IT general knowledge and information security culture.

***Length of Employment in Present Organisation***

The participants were of different experience levels in their organisations. The most observed respondents as between 1 to 4 years (35.8%, n=94), then 5 to 10 years (25.2%, n=67); <1 year (21.5%, n=57); and >10 years (18.0%, n=48), as presented in Figure 8.7. The sample presented different views and perspectives with a range of work experience. It also suggests that the respondents have a level of understanding of their organisation and information security practices. However, the years of experience followed the same pattern of age where the number

of respondents tends to decrease as they become older. It would be interesting to examine the possible impact of different experience levels on correlations between variables in this research. As this could create different knowledge and decision which may affect the organisational security behaviour and the level of information security culture.

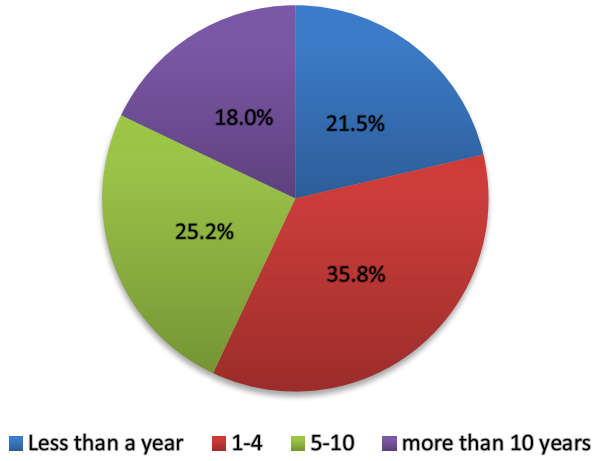



**Figure 8.7: Length of Employment in the Organisation**

***Job Level***

The structure of job levels for the participants was as follows: operational staff (administrative, clerical, etc.) 23.2% (n=60); middle management 20.9% (n=55); and security staff 4.3% (n=11), (see Figure 8.8). The respondents had different views and perceptions at different job levels. This might help this research to check the possible differences between job levels that would have potential influences on security knowledge levels and relationship between key factors and information security culture.

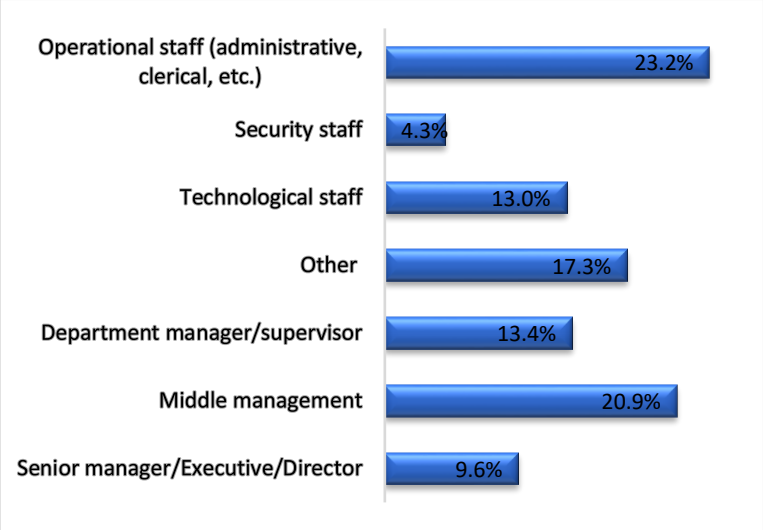



**Figure 8.8: Respondents' Employment Level**

***Did you have an induction training when you started work with the organisation?***

The majority of respondents said that their organisations provided inductions (69.7%, n=185). This information might help this research to investigate the effect of the respondents who had an induction training on the information security culture.

***Did the induction training include security information awareness about using and protection of data and the organisation's information?***

The majority of respondents stated that their induction sessions included information security, as well protection of the organisation's data (69.7%, n=129). This information would support this research to figure the impact of respondents who had a security induction training on information security culture.

### 8.3.2 Information Security Knowledge

The questionnaire included nineteen statements that helped to determine the level of knowledge that employees possess in regard to information security and their own awareness levels regarding this topic. This assisted in developing background information, in order to analyse the questions on the information security culture, and to identify organisational strengths or areas requiring development areas. The frequency of those to agree with the different statements has been analysed, as represented in Table 8.6. In the Table, the first column presents the numbered statements; with the second column providing the actual statement; and the third as the number of respondents who responded to that particular statement.

Additionally, the following three columns provided how many respondents (percentage %) who choose “Yes”, “No” or “Do not know”.

**Table 8.6: Information Security Knowledge Statements**

| No. | Statement | No. of Response | %Yes | %No | %Don’t Know |
|---|---|---|---|---|---|
| 1 | The organisation has formal documents for information security policies. | 266 | 61.60 | 13.69 | 24.71 |
| 2 | I have read the information security policy section that is applicable to my job. | 165 | 80.61 | 15.76 | 3.64 |
| 3 | Are there disciplinary consequences if employees do not comply with the information security policies in the organisation? | 165 | 70.91 | 13.33 | 15.76 |
| 4 | The organisation consistently reviews and updates the information security policies on a periodic basis. | 165 | 69.09 | 9.70 | 21.21 |
| 5 | I am informed regularly about information security requirements and updates. | 266 | 65.04 | 26.32 | 8.65 |
| 6 | Are your security responsibilities and roles clear? | 266 | 66.92 | 23.31 | 9.77 |
| 7 | Does the organisation have a person/team that is assigned for assessing the risk of information assets? | 266 | 66.17 | 13.53 | 20.30 |
| 8 | I am regularly informed and updated information about risks associated with security breaches such as scam email attachments, unknown senders, etc. | 266 | 66.54 | 26.69 | 6.77 |
| 9 | Does the organisation consistently assess and generates a report for the information security risk analysis on a periodic basis? | 266 | 36.84 | 25.94 | 37.22 |

| No. | Statement | No. of Response | %Yes | %No | %Don't Know |
|---|---|---|---|---|---|
| 11 | The organisation has the ethical code of conduct. | 266 | 63.91 | 9.02 | 27.07 |
| 12 | Does the organisation have an ethics committee/advisory that is responsible for the code of conducts? | 170 | 62.35 | 17.65 | 20.00 |
| 13 | Is the organisation's code of conducts clear and easy to understand? | 170 | 81.18 | 9.41 | 9.41 |
| 14 | I am informed by my organisation about information relevant legislation and regulations, such as of intellectual property and copyright laws. | 170 | 72.94 | 20.59 | 6.47 |
| 15 | Is there a procedure to ensure the safety of data at the end of each working day? For example, not leaving confidential documents on the desk when you leave the working area. | 170 | 72.94 | 17.65 | 9.41 |
| 16.a | Do you as an employee know where to find/access the organisational information security policies? | 266 | 61.28 | 28.20 | 10.53 |
| 16.b | Do you as an employee know where to find/access the organisation's ethical code of conduct? | 266 | 54.51 | 28.57 | 16.92 |
| 16.c | Do you as an employee know where to find/access the security-related training programs? | 266 | 50.38 | 34.59 | 15.04 |
| 16.d | Do you as an employee know where to find/access the update information/materials regarding the organisation's security? | 266 | 48.87 | 33.08 | 18.05 |
| 17 | Have you attended any security training in the organisation such as Induction training or Web based training? | 266 | 51.50 | 44.36 | 4.14 |

| No. | Statement | No. of Response | %Yes | %No | %Don't Know |
|---|---|---|---|---|---|
| 18 | I would like to receive information security awareness and training sessions. | 266 | 61.65 | 27.07 | 11.28 |
| **Overall average** | | 231.65 | 63.26% | 21.92% | 14.82% |

Notes: N: number of Responses

The data shows that the average of general awareness and knowledge amongst respondents is 63.26%. The majority of respondents were well informed of security policies. For instance, 80.61% of respondents stated that they had read their company security policies applicable to their jobs and roles, although 38.73% did not know how to obtain a policy document. 69.09% of respondents agreed that their organisations reviewed and updated the security policies consistently. 70.91% of respondents stated that their particular organisations have disciplinary consequences for employees who fail to adhere to security policies. In addition, 66.92% of respondents stated that they knew and were aware of their security responsibilities; while 65.04% of respondents stated that they were regularly informed in regard to security requirements. However, 51.13% of respondents did not know how to obtain updated material on their organisation security policy.

66.17% of respondents stated that their organisations include a team that assessed information asset risk levels. These teams also regularly provided updates related to security risks and breaches. However, 63.16%, of respondents were unaware whether their organisations provided a security risk analysis report periodically. Moreover, 63.91% of respondents noted that they are aware of the code of ethics, although 45.49% of respondents added that they were unaware of how to obtain a copy of this. Meanwhile, 62.35% of respondents answered that they know that an ethics committee is part of their organisations, that is responsible for this code. 81.18% of respondents agreed that the code of conduct is clear and understandable. While 72.94% of respondents remarked that they do receive information regarding relevant legislation/regulations and have procedures that ensure data safety.

49.63% of respondents did not know how to locate and find the security training programme from their organisation, which can correlate with their lack of knowledge. 48.50% of respondents had never attended any security training session. Nonetheless, 61.65% of respondents stated that security awareness and security training sessions would be beneficial.

Also, respondents asked to whom they should report information security incidents (see Figure 8.9). In total, 50% of respondents noted that they should report these incidents to the IT department, while 44% believed that it was to their immediate manager; 26% and 25% of respondents selected group information security officer and help desk, respectively; as well as human resources (9%), the whistle-blowing process (7%) or do not know (6%).

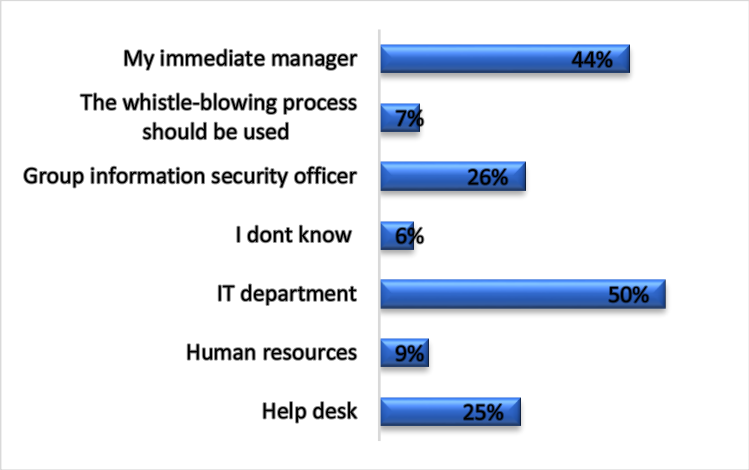



**Figure 8.9: Reports in Organisations of Information Security Incidents**

Respondents reported whether they had attended any security training program in their organisations. 137 of respondents selected “yes”, as they have attended a security training session in their organisations. These respondents selected the type of sessions provided (see Figure 8.10) induction training, hands-on training session, web-based training, and all of them. The majority of respondents chose web-based training (60.7%), with an induction training session (49.7%).

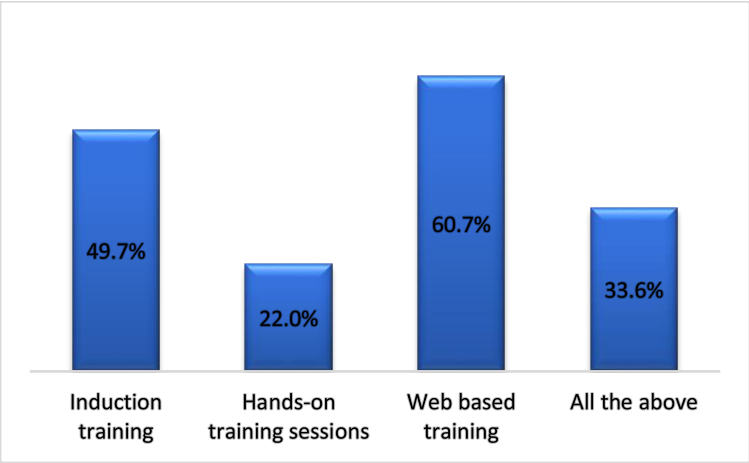



**Figure 8.10: Training Session Type Provided in Organisations**

A majority of 164 respondents stated their interest to receive information security awareness and security education and training sessions. Respondents indicated how they would prefer to receive information in regard to security awareness and training messages. There was a preference of information to be received via email (65.7%); received through induction training (44%); through hands-on training sessions (42%); web-based training sessions (41%) and via videos (32%). The respondents also stated discussion groups (24.7%), SMS (23.5%), posters (18.1%), business unite presentation (13.3%), and articles in new frontiers (8.4%), (see Figure 8.11).

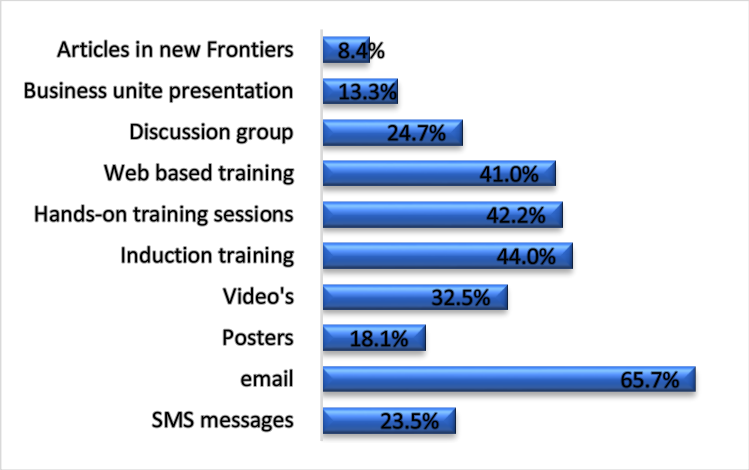



**Figure 8.11: Preference of How to Receive Information Regarding Security Awareness and Training Messages**

There was an analysis of how influential demographical categories were. This would determine the potential external influences on security knowledge levels among employees in an organisation. Various tests were used, which included the Independent Sample T-test and ANOVA at a significance level of 0.05. T-test is a parametric method that compare the means of two independent groups. This test would show whether statistical evidence exists of the mean level from the associated population being noticeably different, in order to test the contrasts between the categories and security knowledge levels, as this would determine the overall effect level (Saunders et al. 2009).

The ANOVA test is a non-parametric method, which equates to the one-way analysis of variance. This is used in order to test whether samples stem from the same forms of distribution and are able to be compared to in excess of two independent samples that may have different sizes (Saunders et al. 2009). When using ANOVA to test the equality of at least three group

means, sometimes statistically significant results show that not all of the group means are equal (Saunders et al. 2009). The results of ANOVA test do not recognise which specific differences between group of means are significant (Saunders et al. 2009). In order to find exactly which groups are different from each other, the researcher have to conduct a post- hoc test (Saunders et al. 2009). A post-hoc test is known as a multiple comparison test, which allows investigation of the difference between multiple groups means and determines where exactly the difference is (Saunders et al. 2009). The most common and simplest post-hoc test is a Bonferroni post-hoc test. Bonferroni post hoc test is a set of t-tests performed on each pair of groups at the same time, in order to investigate the group difference on multiple variables and to reduce the instance of a false positive (Saunders et al. 2009).

Different demographical groups were compared, and certain ones were shown to have a base of demographic variables that would have considerable sized samples, which included: organisation type, number of employees in organisation, gender, age, country, background education in IT field, years of experiences, induction training and security induction training. There were only two groups that failed to apply the comparison tests (organisation industry and job level), as the sample size was insufficient in size and not equal to provide a comparison. The statistical tests used for testing and results are summarised in Table 8.7.

**Table 8.7: Analysis of the Correlation between Knowledge and Demographical Information**

| **Variable name** | **Test** | **Sig ($p<0.05$)** | **Comment** |
|---|---|---|---|
| Organisation type | Independent sample T-test | 0.014 | There is significant difference between organisation type and average knowledge because sig<0.05 |
| Number of employees (size of organisation) | ANOVA | 0.948 | There is no significant difference between size of organisation and average knowledge because sig>0.05 |
| Gender | Independent sample T-test | 0.180 | There is no significant difference between gender and average knowledge because sig>0.05 |

| Variable name | Test | Sig (p<0.05) | Comment |
|---|---|---|---|
| Age | ANOVA | 0.105 | There is no significant difference between age and average knowledge because sig>0.05 |
| Geographical area (between United Kingdom and Saudi Arabia) | Independent sample T-test | 0.002 | There is difference between two countries and average knowledge because sig<0.05 |
| Education background in IT | Independent Sample T-test | 0.754 | There is no significant difference between background education in IT and average knowledge because sig>0.05 |
| Years' experience in organisation | ANOVA | 0.007 | There is difference between years of experience and average knowledge because sig<0.05 |
| An induction training | Independent Sample T-test | 0.002 | There is difference between employees that had an induction training and average knowledge because sig<0.05 |
| Security induction training | Independent Sample T-test | 0.002 | There is difference between the induction training include security information and average knowledge because sig<0.05 |

Notes: Sig = significant, p = p-value; * p < 0.05.

Four demographic groups presented no significance difference in the level of knowledge: number of employees in an organisation, gender, age, and IT educational background. However, various differences exist among five other demographic groups: organisation type (p=0.014), country (p=0.002), years of experiences (p=0.007), job level (p=0.004), induction training (p=0.002) and security induction training (p=0.002).

Organisational type was measured in three groups: public, private and semi-public. Initially, for semi-public, the total was minimal (approximately 5%). Thus, it was removed from the final analysis. The types were compared between only two groups (public and private). The independent sample T-test examined the differences in organisation types in regard to

knowledge level. A statistically significant difference exists between the types of organisations and levels of knowledge (p=0.014) (see Table 8.8). Subsequently, this demonstrates that employees in public organisations have slightly better levels of knowledge on information security.

**Table 8.8: T-test Statistics Demonstrating Organisational Type Differences Regarding Knowledge**

| | **Public (n=139)** | | **Private (n=113)** | | **T-value** | **p** |
|---|---|---|---|---|---|---|
| Variable | Mean | St. Deviation | Mean | St. Deviation | 2.46 | 0.014 |
| Knowledge | 1.65 | 0.43 | 1.51 | 0.42 | | |

Notes: p = p-value at $p < 0.05$

The country variable was categorical and unambiguous. As a result of the lower number of respondents from different countries, the research focused on the contrasts between only two countries: Saudi Arabia (n= 84) and the United Kingdom (n= 89). The Independent sample T-test helped to determine whether there were differences among two groups. The results show a statistically significant correlation between two countries and level of knowledge (p=0.002), as displayed in Table 8.9.

**Table 8.9: T-test Statistics Showing Countries Differences in Knowledge**

| | **United Kingdom (n=89)** | | **Saudi Arabia (n=84)** | | **T-value** | **p** |
|---|---|---|---|---|---|---|
| Variable | Mean | St. Deviation | Mean | St. Deviation | 3.185 | 0.002 |
| Knowledge | 1.65 | 0.39 | 1.70 | 0.45 | | |

Notes: p = p-value at $p < 0.05$

In order to examine the differences between employees' years of experiences and their levels of knowledge, the research used the one-way ANOVA test among four different groups. A post-hoc test was implemented to show where differences originate (see Table 8.10).

**Table 8.10: ANOVA Statistics Demonstrating Years of Experiences and Differences in Knowledge Levels**

| Variable | Years of experiences | No. of Response | Mean | St. Deviation | f | p |
|---|---|---|---|---|---|---|
| Knowledge | Less than 1 year | 57 | 1.6 | 0.39 | 4.136 | 0.007 |
| | 1- 4 | 94 | 1.6 | 0.47 | | |
| | 5-10 | 67 | 1.4 | 0.36 | | |
| | More than 10 years | 48 | 1.5 | 0.41 | | |

Notes: p = p-value at $p < 0.05$

The contrasts between the levels of knowledge among groups was shown to be significantly different ($F(3,262) = 4.136$, $p=0.007$). A Bonferroni post hoc-test showed that employees with 5 to 10 years of experiences had marked differences in knowledge from those with less than 12 months (mean difference= -2.15, $p=0.030$) and for those with 1 to 4 years' experiences (mean difference= -2.15, $p=0.01$). However, from the 5 to 10 years' experience group, there was no significant difference between respondents of in excess of 10 years' experience. The research also examined whether differences existed in knowledge levels, between the group that had received an induction training and who had not. This question was measured in two distinct groups: employees who selecting that they had and had not received induction training. An independent sample T-test was conducted, which showed that the respondents who had received induction training were noted as having a better level of knowledge. It can be concluded that a clear statistically significant difference between two group existed in employees' knowledge levels ($p=0.002$) as shown in Table 8.11.

**Table 8.11: T-test Statistics that Show Induction Training Differences in Knowledge**

| | Yes (n=185) | | No (n=81) | | T-value | p |
|---|---|---|---|---|---|---|
| Variable | Mean | St. Deviation | Mean | St. Deviation | 3.635 | 0.002 |
| Knowledge | 1.72 | 0.42 | 1.52 | 0.40 | | |

Notes: p = p-value at $p < 0.05$

In order to determine whether the inclusion of information security in induction training can affect employees' knowledge, an independent sample T-test was conducted, with groups of employees who stated that they had received information regarding security in induction training and those who had not. The t-statistics' results demonstrate that employees who had received information on security through induction training had a greater level of knowledge; while the differences between the groups was noticeably significant (p=0.002), as displayed in Table 8.12.

**Table 8.12: T-test Statistics that Show Induction Training Differences in Levels of Knowledge**

| | **Yes (n=129)** | | **No (n=56)** | | **T-value** | **p** |
|---|---|---|---|---|---|---|
| Variable | Mean | St. Deviation | Mean | St. Deviation | | |
| Knowledge | 1.70 | 0.44 | 1.40 | 0.30 | -6.331 | 0.002 |

Notes: p = p-value at $p < 0.05$

### 8.3.3 The Statistical Analysis of the Research's Framework Dimensions

This section focuses on the evaluation and interpretation of the variables, and mean values calculated from the whole sample. In order to obtain the complete mean level for the different constructs, the components' items scores were shown through their average, which comprised: top management, security policy, security education and training, security risk analysis and assessment, ethical conduct, job satisfaction, personality traits that include (agreeableness, conscientiousness, extraversion, neuroticism, openness), security awareness, security ownership and security compliance that were calculated in order to create fourteen composite variables. The mean values were shown to represent the variables' responses, and the mean values ranged between (1.65 and 3.30), as presented Table **8.13**. This indicated a general tendency for the numerically coded responses to demonstrate a value that is between neither 'disagreeing' nor 'agreeing' with the individual items (score = 3) and merely 'agreeing' with the items (score = 2). For the detailed analysis of the different statements and distribution frequency regarding the respondent's perceptions see Appendix L.

**Table 8.13: Research Framework Constructs Results Statistical Analysis Summary**

| Construct | N | Mean | Std. Error | Std. Deviation |
|---|---|---|---|---|
| Top Management | 266 | 2.144 | 0.035 | 0.570 |
| Security Policy | 266 | 2.116 | 0.041 | 0.674 |
| Security Education & Training | 266 | 2.216 | 0.037 | 0.610 |
| Risk Analysis & Assessment | 266 | 1.905 | 0.036 | 0.589 |
| Ethical Conduct | 266 | 1.662 | 0.041 | 0.675 |
| Job Satisfaction | 266 | 2.191 | 0.037 | 0.607 |
| Security Awareness | 266 | 1.747 | 0.032 | 0.523 |
| Security Ownership | 266 | 1.650 | 0.033 | 0.542 |
| Security Compliance | 266 | 1.790 | 0.033 | 0.532 |
| Extraversion | 266 | 2.254 | 0.026 | 0.424 |
| Agreeableness | 266 | 1.970 | 0.029 | 0.470 |
| Conscientiousness | 266 | 1.912 | 0.029 | 0.477 |
| Neuroticism | 266 | 3.306 | 0.053 | 0.865 |
| Openness | 266 | 2.010 | 0.027 | 0.433 |

Notes: N: number of Responses, Std. Error: Standard Error, Std. Deviation: Standard Deviation

The mean level of neuroticism, extraversion, security education and training, job satisfaction, top management, security policy and openness were in excess of 2, which indicates a quality

reflection for those variables. The low average for the weighted mean was for security ownership, ethical conduct, security awareness, security compliance, security risk analysis and assessment, conscientiousness and agreeableness, which indicated that requires more attention and improvements. In general, the organisations displayed moderate levels of involvement from management in regard to information security programmes, with the mean value at 2.14. Indeed, 58% of respondents stated and believed that their top-level manager provided consistent support to their organisation's security programme, as well as all levels of leaderships being involved in activities of information security. Security policy has a mean value of 2.11. While 62.7% of respondents stated that the security policy was clear and understandable from their organisation. Security education and training support was a clear concern for the different organisations. Security education and training has a mean value of 2.21. Furthermore, 86.8% of respondents in this research remarked that it is imperative to receive security refresher training, while 48.5% of respondents showed that they received training programme that focused on their daily duties.

There was a mean value of 1.90 for the security risk analysis and assessment. A total of 62.7% of respondents noted that the process of a security risk analysis in their organisations was sufficiently capable of identifying risk levels that would impact upon information security. Ethical conduct received a score of 1.66 on average. 89% of respondents also remarked that taking care was important when mentioning work or confidential information whilst in public places. Additionally, 84.9% of respondents had the perception that indicated the importance of considering ethical conduct in the creation of beneficial information security culture. The results also showed that respondents were satisfied with their job in their organisations, with an average score of 2.19. It was evident that 40.9% of respondents were satisfied with the opportunity for promotion and rewards that their organisations presented them.

The average score for security awareness was 1.74. 75% of respondents perceived their levels of security awareness to be moderate, which showed that they understood the continual initiatives in relation to their organisations' security awareness. Security ownership receives the lowest average score of all the constructs with the average of 1.65. Meanwhile, 89% of respondents added that they felt a sense of elevated security ownership; while 92.8% of respondents indicated that the information security protection is the responsibility of all employees inside the organisation. The mean value for security compliance and adherence to the security policy was 1.79. 92.4% of respondents stated that it was imperative to adhere to

security policies, in order to improve the organisation's information security cultures; while 74% of respondents believed that their organisations enforced employee adherence to their security policies. In addition, the mean score range of 1.91 to 3.30 for the categories of agreeableness (1.90), conscientiousness (1.91), openness (2.01), extraversion (2.25), and neuroticism (3.30). The mean value of neuroticism and extraversion were the highest average of all constructs. The normal for an individual mean is close to the midpoint for conscientious, agreeable and openness, yet much closer to the neuroticism (emotional stability) and extraversion, respectively.

The Standard Deviation (SD) and Standard Error (SE) of all variables were calculated. The Standard Deviation (SD) is a measure of how well the mean demonstrates the observed data (Field 2009). When the SD is larger this shows that the cluster of scores is generally closer to the mean value, which suggests that the mean value is not a valid indication of the data. Contrastingly, when the SD is small, there are fewer data statistics in relation to the mean value, which demonstrates that the mean value adequately represents the overall data.

Standard Error (SE) is the indication of how well the particular sample represents the population (Field 2009). SE demonstrates the sample mean variability level. Separately, when the SE is large, this shows significant variation between various samples' mean values, and thus, a sample commonly fails to represent the full observed population. Comparatively, when the SE is small this indicates that the majority of sample means coincide with the population mean; hence, the sample is a vital indication of the overall population.

For all the variables in this research, the SD had a range of 0.42 to 0.86, as shown in Table 6.13. The SD values indicated a minimal distance from the mean score, which demonstrates clear and specific results among organisational members, as well as ensuring that the mean value functions as a quality representative for the data sets. Similarly, for the various variables, the SE had a range of 0.026 to 0.053, as displayed in Table 6.13. The SE value shows that the sample means correlate with the population mean value. Thus, the SE's minimal values present an understanding that the used sample was a sufficient representation of the overall population. For the entire variables, the SD and SE were at a relatively small level in comparison to the means levels. Therefore, it is possible to determine that the mean value can be used as a representative score for the variables in the data sets. The SE's minimal values indicate that the used sample functioned as a sufficient representative of the overall population.

## 8.4 The Research Instrument Levels of Reliability and Validity

Following an analysis of the participants' demographic data and the descriptive characteristics presented, the next stage examined how these individual responses had answered the questions/items on the survey in regard to the conceptual framework different dynamics. This is also known as an analysis of the data's psychometric aspects that need sufficient levels of reliability and validity for the measurement (Hair et al. 2006). The ideal situation within research is present when the data scores produce reliability and validity (Creswell 2008). Creswell (2008) stated that scores are required to remain stable and consistent in order to demonstrate reliability prior to them gaining meaning (i.e., valid). The research gains validity when a particular instrument used by an individual produces valid and meaningful scores (Creswell 2008). Therefore, an analysis of both reliability and validity was implemented through the development of this research questionnaire, as this helped to construct a beneficial survey.

### 8.4.1 Reliability of the Instrument

A scale is viewed as valid when it can be used practically and functions with reliability (Pallant 2005). Reliability is defined as how an instrument is able to measure in the same way at different moments when implemented with the same conditions and subject matter (Pallant 2011). Reliability commonly has two reasons of relevance, as it evaluates consistency between the number of items measured through a single variable (Hair et al. 2006); and it forms the connections between respondents' scores from the same item measured at two different stages (Ticehurst & Veal 2000). Generally, accuracy levels and consistency of measures are directed from the reliability of scale, which help to avoid bias (error free), and thus, enable the reproducibility of measurement tools for different samples and time horizon. A scale reliability analysis was performed in this research, in order to make sure that the measurement scales were able to accurately capture the current constructs. The scale reliability analysis was performed through an assessment of internal consistency and inter-total correlations.

#### *8.4.1.1 Internal Consistency*

Internal consistency is an assessment of the reliability of survey or test items designed to assess the same construct, in order to ensure that the various items measuring the different constructs produce consistent scores (Tabachnick & Fidell 2007). The most commonly used measurement

instrument for internal consistency is Cronbach's alpha coefficient. This measures the estimated correlation of a set group of items and actual recorded scores. In this research, Cronbach's α coefficient method was selected for the items of the different constructs in order to test the level of validity from the questionnaire and how its internal consistency measured. Cronbach's α coefficient (inter-item consistency reliability) was selected, as it functions in a simple manner to produce calculations and is often used in academic research (Tabachnick & Fidell 2007). Specifically, Cronbach's alpha value has a range of one (perfect reliable) to zero (unreliable), with values higher than 0.50 shown to be acceptable (Gliem & Gliem 2003). There was a high correlation between all the constructs in this research through the Cronbach's alpha values, which ranged from 0.55 to 0.91. Indeed, the recommended value of the Cronbach's α was 0.50, and it was higher in this research, which indicates good scale internal consistency and reliability, as demonstrated in Table 8.14. Therefore, Cronbach's alpha coefficient consists of consistent variables that help to capture the framework's meaning in this research.

**Table 8.14: Cronbach's Alpha Attribute Value and the Result of Analysis**

| Factor | No of Statement | Cronbach's Alpha | Analysis |
|---|---|---|---|
| Top Management (TM) | 5 | 0.680 | Acceptable |
| Security Policy (SP) | 4 | 0.797 | Good |
| Security Education & Training | 3 | 0.557 | Acceptable |
| Risk Analysis & Assessment (RA) | 3 | 0.636 | Acceptable |
| Ethical Conduct (EC) | 3 | 0.860 | Good |
| Job Satisfaction (JS) | 5 | 0.791 | Good |
| Security Awareness (SA) | 3 | 0.664 | Acceptable |
| Security Ownership (SO) | 3 | 0.760 | Good |
| Security Compliance (SC) | 3 | 0.630 | Acceptable |
| Agreeableness (Agr) | 7 | 0.848 | Good |
| Conscientiousness (Con) | 7 | 0.845 | Good |
| Extraversion (Ext) | 6 | 0.863 | Good |
| Neuroticism (Neu) | 5 | 0.912 | Good |
| Openness (Ope) | 7 | 0.842 | Good |

Note: No of statement: number of statements

#### *8.4.1.2 Item-Total Correlation*

Various researchers have recommended that item-total correlation analysis for complete groups of items needs to be performed in order to improve the measurement process by removing unnecessary items before deciding on the factors that represent the constructs (Lu et al. 2007). This enables the prevention more factors be produced that have no value to the study. A variable of interest score is excluded through corrected item-total correlation when the composite score is calculated (Koufteros 1999). When the corrected item-total correlation has a value of lower than 0.30, this highlights that something different is being measured from the actual construct (Pallant 2011). In this research, the results of item-total correlations demonstrate that the majority of variables within the constructs provide a measurement of the construct itself, as there was a higher correlation value than 0.30. Nonetheless, a total of ten variables were less than 0.30 that are: TM3, SET2, RA1, JS3, Agr6, Agr7, Ext6, Ext7, Ope9, Ope10. In particular, a method that has been shown to increase the α-value is to delete the items that have lower Squared-Multiple-Correlations (SMC) or to remove the items with lower corrected-item-total correlation (Pallant 2011). For instance, item SET2 (corrected item-total correlation = 0.09) within the Security Education and Training (SET) construct was deleted in order to increase the α-value. However, these items were maintained in order to better examine the constructs through the use of exploratory factor analysis method of convergent validity. The results of item-total correlations are presented in Appendix M.

### 8.4.2 Validity

The measurement scale's validity enables the findings to be shown as a real representation of the researched concept (Hair et al. 2006). The validity test should be able to confirm that the concept has been known already. Commonly in research within the fields of business and social, there are two methods of validity testing that are applied in the measurement of an instrument quality, which are content validity and construct validity.

#### *8.4.2.1 Content Validity*

Content validity is referred to as face validity, which presents an assessment of the relationship between items and constructs through rating systems by experts, judges, and pre-tests with numerous sub-populations (Hair et al. 2006). Content validity needs to be the first step to establish the constructs' relationship and to measure the items. If measurement scales fail to

include content validity, then they are unable to include construct validity, even though the statistical analysis may indicate something to the contrary (Graver & Mentzer 1999).

In this study, the researcher used items from previous studies, such as Alhogail (2016) and Da Veiga (2018), in order to establish content validity (see survey development in this Chapter 7, section 7.2.1). Subsequently, the researcher asked experts in information systems, who were more familiar with the topic to evaluate the measurement items and state what items appeared to be logical and valid. The experts provided minor typographical suggestions, which were incorporated into the final questionnaire (see Chapter 7, section 7.3).

#### *8.4.2.2 Construct Validity*

The construct validity is referred to as the external validity of an instrument. This is quantitatively calculated through the use of observations of the relationship between theoretical sets of measurement items (Hair et al. 2006). The construct validity is defined as how a group of items are measured against their original intend measurement (Garver & Mentzer 1999). Construct validity is able to be measured through convergent validity, discriminant validity and nomological validity (Campbell et al. 1959). In this research, the objective was to examine the overall validity of the survey instrument. Therefore, convergent and discriminant validities were analysed and are detailed later in this chapter.

## 8.5 Factor Analysis (FA)

Factor Analysis (FA) is the most beneficial way to comprehend the underlying structure of a particular theory, as well as the variables through analysis (Tabachnick & Fidell 2007). Factor Analysis (FA) has been used as a tool to examine different factors' structures and/or correlations (Williams et al. 2012). Factor analysis generally aims to lower the information that is contained in various measuring items into a reduced set of innovative composite factors. FA was implemented in this research to determine the overall construct validity. FA was carried out to produce a better examination of the current study's measurement items.

There are two individual techniques in factor analysis that help to determine the variables of interest from the subsets that all function independently: Exploratory Factor Analysis (EFA); and Confirmatory Factory Analysis (CFA) (Hair et al. 2006). EFA explores the data and provides information in regard to various possible factors that represent the data (Hair et al. 2006). CFA validates and confirms the factors of measurement that are present within sets of

variables involved in the theoretical form. Accordingly, the current research aimed at this stage to check the survey instrument validity. First, EFA was applied, which tested the measurement items. CFA was applied as a second method in evaluation for the construct items, which ensured a better level of reliability and validity and confirm the theoretical perspective of the latent variables.

### 8.5.1 Exploratory Factor Analysis (EFA)

Exploratory Factor Analysis (EFA) was undertaken in order to examine the measurement items' structure that corresponded to the variables in the study framework. EFA is beneficial as a preliminary analysis tool when there is insufficient detailed theory in regard to the correlation between variables and the main constructs (Gerbing & Anderson 1988). EFA was shown to be necessary in this research, even though all the variables from the constructs were taken from previous studies, such as Alhogail and Mirza (2015) and Da Veiga (2018), as can be seen from the literature review and expert feedback.

#### *8.5.1.1 Factorability of Data*

Factorability of data refers to how suitable the data is in regard to the inter-correlation between different variables (Tabachnick & Fidell 2007). A factorable correlation matrix was required to include sizable values for the correlation, as the variables from the analysis were shown to measure the same main construct (Tabachnick & Fidell 2007). To achieve relevant results from the factor analysis, it has been recommended to apply that the Kaiser-Meyer-Olkin (KMO) test and Bartlett's test of Sphericity should be calculated (Norusis 1992). The KMO provided measurements of sampling adequacy, while Bartlett's test of sphericity is normally used to show the factorability of data (Pallant 2011). When the KMO has a value in excess of 0.60, this suggests that the relationship between items is statistically significant and has the suitability for EFA to provide set of factors (Tabachnick & Fidell 2007). Comparatively, Bartlett's test of sphericity shows the correlation between the measured items to be in excess of 0.30, which again provides a suitability level for EFA (Hair et al. 2006).

In this research, seventy-seven items were examined through the use of EFA, which contributed to fourteen constructs (see Table 8.15). The results shown that KMO value was 0.790 higher than the lowest acceptable level (0.60). The test of Bartlett's was significant at $p<0.001$, as this adhered to the initial assumptions for EFA (Kaiser 1974; Bartlett 1954). The results confirmed the factorability of the EFA conducted for each construct (Hair et al. 2006).

**Table 8.15: KMO and Bartlett's Test of Sphericity**

| | | Bartlett's Test of Sphericity | | |
|---|---|---|---|---|
| **Construct** | **KMO** | **Approx. Chi-square** | **df** | **Sig.** |
| Information Security Culture framework | 0.790 | 11310.484 | 3103 | .000 |

Notes: KMO: Kaiser-Meyer-Olkin, Approx. Chi-Square: Approximately Chi-square, Sig: Significant

### *8.5.1.2 Factor Extraction and Rotation*

EFA requires the process of following two essential steps that help to produce a valid solution to explain a relevant number of factors that represent a certain construct. These two steps are factor extraction, and factor rotation and interpretation (Pallant 2011). Factor extraction has the goal of determining the factors and criteria from a particular method, as well as their relevance; while factor rotation and interpretation aim to improve how a factor solution is interpreted and understood (Tabachnick & Fidell 2007).

There are numerous extraction methods that can be used, which include Principal Component Analysis (PCA), Principal Axis Factors (PAF), Maximum Likelihood Factoring (MLF), image factoring, alpha factoring and unweighted and generalised weighted lest squares factoring (Tabachnick & Fidell 2007). In this research, Principal Component Analysis (PCA) with SPSS Statistics was used in the examination of correlation patterns from the questions to provide measurements of respondents' perceptions in regard to information security. PCA maximises the extracted variance from a set of data, as the initial component takes the highest variance and the last component taking the lowest variance (Tabachnick & Fidell 2007). PCA is able to identify and reduce large sets of variables into small number of components through the transformation of interrelated variables into different unrelated linear composite variables (Hair et al. 2006). The correlation matrix factorability was investigated through the use of Pearson's product-moment correlation coefficient in this research. Pearson correlation coefficient is a statistical formula that measure the strength of the linear relationship between two variables (Tabachnick & Fidell 2007). When the correlation patterns between the set of observed variables were detailed, factor analysis assisted in determining the main factors and helped to identify the factors that were represented in a conceptual manner.

There are various forms of criteria used to attain the number of factors that can describe the main correlation among variables in the best manner: latent root criterion; Catell's scree test; a priori criterion; and percentage of variance criterion (Hair et al. 2006). The Latent root criterion provides a suggestion that the factors are significant when factors have Eigenvalues higher than 1, and those that are lower than 1 should not be used in analysis and disregarded (Pallant 2011). Separately, the Catell's scree test uses a graphic plot of Eigenvalues, which is measured against the number of factors in their extraction sequence, while the curve shape within the plot helps to determine the cut-off point (Hair et al. 2006). The plot shape starts to decrease after the initial factor, which has its highest Eigenvalue towards the lowest one until it is at its last factor with the lowest Eigenvalues (Tabachnick & Fidell 2007). When there is a change in the slope in the curve, this indicates what should be the maximum number of factors for extraction (Pallant 2011). This change in the shape of the plot, (which is commonly in the shape of an elbow shape) shows an evident distinction among the factors of interest that have Eigenvalue>1, and the disregarded factors that has an Eigenvalue<1 (Hair et al. 2006).

A priori criterion is a criterion that has the number of factors taken before implementing the factor analysis. The priori criterion is considered beneficial when testing a theory or hypothesis in regard to the number of extracted factors (Hair et al. 2006). This criterion attempts to replicate work from different researchers and extracts the same number of factors found previously (Hair et al. 2006). The variance criterion percentage shows practical relevance of the factors, as it confirms specific amounts of variance (Tabachnick & Fidell 2007). Hair et al. (2006) also stated that it is often common for a solution to be considered when it shows >60% cumulative variance that satisfies the percentage variance of criterion, which is also known as the score variability. In this research, three criterions: latent root criterion, Catell's scree test and percentage of variance criterion were used to assess the adequacy of extracted factors.

Communality is the term given to the total variance of any original variable that is shared with different variables (Hair et al. 2006). Communality is set at 1 to the variance does not exists, while a communality of 0 is given to variables that share nothing with different variables (Field 2009). Items are also considered weak when they exhibit communality that is lower than 0.50 (Hair et al. 2006). For example, certain variables are accepted with a 0.30 cut-off value of communality depending on their overall sample size (Pallant 2011).

Factor loadings present the level that variables load onto factors following the factor extraction (Field 2009). In general, the initial factor solution fails to provide a relevant interpretation, as

the majority of variables have high loading rates on the main factor, whilst they only have small loadings on others, regardless of which method of extraction is used (Tabachnick & Fidell 2007). Consequently, factor rotation was used in order to produce easier and more directly usable solutions.

The preferred used method was the orthogonal varimax rotation, as it was the easiest and most common form of rotation (Tabachnick & Fidell 2007). It is also the most common variance maximising procedure with a high level of generalisability and is more replicable in comparison to oblique rotation (Tabachnick & Fidell 2007). A specific criterion was used to show the factor loadings' relevance following the factor rotation. The factor loading was shown to be significant at >0.50 with the 0.05 level able to obtain an 80% level of power from a sample of 266 (Hair et al. 2006). Whereas the variables from the factor loading that were <0.50 were removed.

### *8.5.1.3 Factor Analysis Results*

It can be determined from the aforementioned techniques and criteria that EFA was performed for the seventy-seven items through the use of SPSS program. Subsequently, fourteen components were extracted that had Eigenvalues >1 with a complete variance of 59.36%. In this research, the inspection of the Scree plot demonstrates correlating number of factors that were extracted by using Kaiser's latent root criterion (Eigenvalue higher than 1) as shown in Figure 8.12. The graph clearly showed changes in the shape through components 13 and 14, while 1 to 14 provided detail of more variance than the later components.

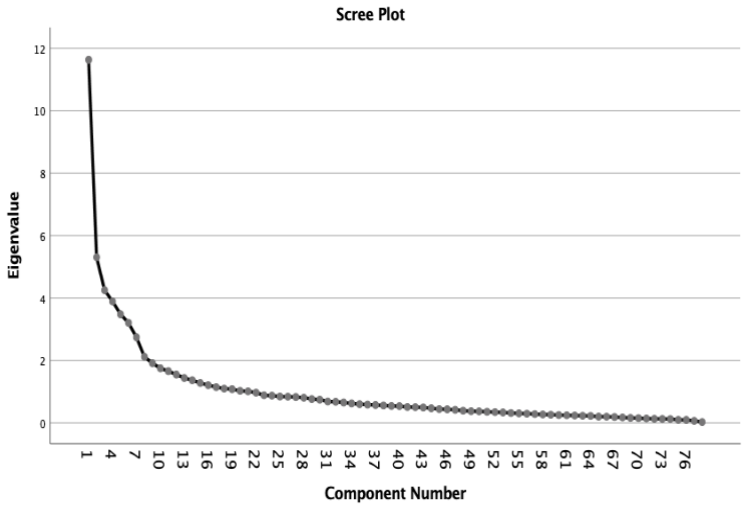



**Figure 8.12: Scree Plot**

The rotated pattern matrix presented fourteen solutions (see Table 8.16), which demonstrate how items were loaded onto fourteen different factors with a range of 0.501 to 0.863. Each of the seventy-five items had a loading of at least or very close to 0.50 with the primary factor, which indicated a practical significance and satisfied to the minimum factor loadings' criterion. When a sample has a size that exceeds 100, loadings that are above >0.50 are shown to be the most significant (Hair et al. 2006). Comparatively, the items with a factor loading of less than 0.40 or cross-loading with higher than 0.40 show weak consistency within scales and are beneficial to not be deleted (Hair et al. 2006). In this research, in relation to the factors, two items (SET2 and JS3) had the possibility of either high cross-loads or low loading. Moreover, it was clear in construct of Security Education and Training (SET), that item SET2 with a high cross load into the construct Security Awareness (SA) (cross load= 0.61 > 0.50) created the removal of the item. It is possible that cross loading occurred due to the similarity between these constructs.

**Table 8.16: Factor Loading (Pattern Matrix)**

| | Component | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| **SP1** | 0.80 | | | | | | | | | | | | | |
| **SP2** | 0.85 | | | | | | | | | | | | | |
| **SP3** | 0.80 | | | | | | | | | | | | | |
| **SP4** | 0.69 | | | | | | | | | | | | | |
| **TM1** | | 0.76 | | | | | | | | | | | | |
| **TM2** | | 0.75 | | | | | | | | | | | | |
| **TM4** | | 0.67 | | | | | | | | | | | | |
| **TM5** | | 0.66 | | | | | | | | | | | | |
| **SO1** | | | 0.82 | | | | | | | | | | | |
| **SO2** | | | 0.81 | | | | | | | | | | | |
| **SO3** | | | 0.84 | | | | | | | | | | | |
| **SA1** | | | | 0.80 | | | | | | | | | | |
| **SA2** | | | | 0.71 | | | | | | | | | | |
| **SA3** | | | | 0.80 | | | | | | | | | | |
| **SC1** | | | | | 0.82 | | | | | | | | | |
| **SC2** | | | | | 0.74 | | | | | | | | | |
| **SC3** | | | | | 0.70 | | | | | | | | | |
| **SET1** | | | | | | 0.66 | | | | | | | | |
| **SET3** | | | | | | 0.74 | | | | | | | | |
| **SET4** | | | | | | 0.79 | | | | | | | | |
| **RA1** | | | | | | | 0.51 | | | | | | | |
| **RA2** | | | | | | | 0.88 | | | | | | | |
| **RA3** | | | | | | | 0.86 | | | | | | | |
| **JS1** | | | | | | | | 0.78 | | | | | | |
| **JS2** | | | | | | | | 0.71 | | | | | | |
| **JS4** | | | | | | | | 0.71 | | | | | | |
| **JS5** | | | | | | | | 0.78 | | | | | | |
| **JS6** | | | | | | | | 0.71 | | | | | | |
| **Neu1** | | | | | | | | | 0.51 | | | | | |
| **Neu2** | | | | | | | | | 0.88 | | | | | |
| **Neu3** | | | | | | | | | 0.85 | | | | | |
| **Neu4** | | | | | | | | | 0.82 | | | | | |
| **Neu5** | | | | | | | | | 0.86 | | | | | |
| **Neu6** | | | | | | | | | 0.50 | | | | | |
| **Neu7** | | | | | | | | | 0.85 | | | | | |
| **Neu8** | | | | | | | | | 0.51 | | | | | |
| **Ope1** | | | | | | | | | | 0.84 | | | | |
| **Ope2** | | | | | | | | | | 0.59 | | | | |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Ope3** | | | | | | | | | | 0.51 | | | | |
| **Ope4** | | | | | | | | | | 0.73 | | | | |
| **Ope5** | | | | | | | | | | 0.73 | | | | |
| **Ope6** | | | | | | | | | | 0.71 | | | | |
| **Ope7** | | | | | | | | | | 0.62 | | | | |
| **Ope8** | | | | | | | | | | 0.76 | | | | |
| **Ope9** | | | | | | | | | | 0.51 | | | | |
| **Ope10** | | | | | | | | | | 0.51 | | | | |
| **Agr1** | | | | | | | | | | | 0.81 | | | |
| **Agr2** | | | | | | | | | | | 0.81 | | | |
| **Agr3** | | | | | | | | | | | 0.70 | | | |
| **Agr4** | | | | | | | | | | | 0.55 | | | |
| **Agr5** | | | | | | | | | | | 0.66 | | | |
| **Agr6** | | | | | | | | | | | 0.50 | | | |
| **Agr7** | | | | | | | | | | | 0.50 | | | |
| **Agr8** | | | | | | | | | | | 0.76 | | | |
| **Agr9** | | | | | | | | | | | 0.75 | | | |
| **Con1** | | | | | | | | | | | | 0.72 | | |
| **Con2** | | | | | | | | | | | | 0.73 | | |
| **Con3** | | | | | | | | | | | | 0.69 | | |
| **Con4** | | | | | | | | | | | | 0.68 | | |
| **Con5** | | | | | | | | | | | | 0.64 | | |
| **Con6** | | | | | | | | | | | | 0.77 | | |
| **Con7** | | | | | | | | | | | | 0.73 | | |
| **Con8** | | | | | | | | | | | | 0.50 | | |
| **Con9** | | | | | | | | | | | | 0.51 | | |
| **EC1** | | | | | | | | | | | | | 0.86 | |
| **EC2** | | | | | | | | | | | | | 0.90 | |
| **EC3** | | | | | | | | | | | | | 0.90 | |
| **Ext1** | | | | | | | | | | | | | | 0.72 |
| **Ext2** | | | | | | | | | | | | | | 0.77 |
| **Ext3** | | | | | | | | | | | | | | 0.75 |
| **Ext4** | | | | | | | | | | | | | | 0.80 |
| **Ext5** | | | | | | | | | | | | | | 0.80 |
| **Ext6** | | | | | | | | | | | | | | 0.50 |
| **Ext7** | | | | | | | | | | | | | | 0.51 |
| **Ext8** | | | | | | | | | | | | | | 0.75 |
| **Eigen Value** | 11.6 | 5.3 | 4.2 | 3.9 | 3.5 | 3.2 | 2.7 | 2.1 | 1.9 | 1.7 | 1.7 | 1.5 | 1.4 | 1.4 |
| **Variance (%)** | 14.9 | 6.8 | 5.4 | 5.0 | 4.5 | 4.1 | 3.5 | 2.7 | 2.4 | 2.2 | 2.1 | 2.0 | 1.8 | 1.7 |
| **Cumulative Variance explained** | 14.9 | 21.7 | 27.2 | 32.2 | 36.6 | 40.7 | 44.2 | 47 | 49.4 | 51.6 | 53.8 | 55.8 | 57.6 | 59.4 |

The majority of items shared above 0.50 communalities with their components. For instance, communalities were seen to be less than 0.50 in only the construct Job Satisfaction item JS3. As detailed earlier lower levels of communality show that an item is unable to connect correctly with different items within the same component, thus, in order to improve the scale, it is often beneficial to remove items with minimal communality (Hair et al. 2006). There is also the suggestion to observe the factor loading prior to the removal of the items with low levels of communality (Pallant 2011). The items with a factor loading lower than 0.40 should also be deleted (Hair et al. 2006). It was also observed that item JS3 has a lower level of communality (0.38) with its corresponding component, and thus, the item was removed.

As a result, in EFA's second round, the remaining seventy-five items were run in the data reduction purpose, excluding one cross-loaded item and one lower loading item. This option has been noted to be the most conducive option, as the scree plot and the Eigenvalue have indicated that the items could be placed naturally into fourteen factor solutions. In total, all constructs' items loaded as had been predicted previously, except two items related to Security Education and Training (SET2) and Job Satisfaction (JS3). Separately, the Cronbach's alpha coefficients for the scales had elevated levels (>0.50), which ranged between 0.55 and 0.91; hence, highlighting internal consistency. The results also confirmed that the developed scales included items with reliability and validity, which emphasised the model constructs' relevance and connecting factors. Nonetheless, validation techniques, which include Confirmatory Factor Analysis (CFA), can improve the research framework level of validation.

## 8.6 Assessment and Evaluation of the Model

The model's assessment was conducted after the model's validity and reliability were defined earlier in this chapter (section 8.4). Structural Equation Modelling (SEM) has been used in this research. It included a two-stage process: to assess the measurement model and the structural model. The model validation goal was to define whether both the measurement and the structural model adhered to the determined quality criteria for the empirical research. Subsequently, guidelines are presented in the following sections that were used when assessing the research model.

### 8.6.1 Structure Equation Modelling (SEM) Overview

Structure Equation Modelling (SEM) tools are used for the purpose of research in regard to correlations between modelling complexes and the multivariate sets of data that rely on various

measures to be implemented for the constructs (Hair et al. 2006). SEM is considered to present an extension to the multivariate techniques that enable numerous indicators to provide measurements of unobserved variables, such as constructs, and facilitate the acquisition of data and combined theory (Hair et al. 2006). SEM is used to determine whether there is any validity in the possibility of a theoretical (*a priori*) model, which specifies, estimates and evaluates the linear relationships among a certain group of variables both observed and unobserved (Shah & Goldstein 2006). The causal links are implied by linear relationships, which can have their estimated path coefficients used as the structural base for hypothesis testing (Shah & Goldstein 2006). SEM enables to model multiple layer relationship for multiple independent and dependent variables simultaneously. Additionally, SEM improves upon initial statistical tools. SEM enables a researcher to model complex correlations, deal with multicollinearity, implement CFA, utilise both unobserved and observed variables, and to provide an estimation of explicit measurement error variance in order to avoid bias (Hair et al. 2006).

The analysing techniques of SEM include covariance-based modelling (i.e., LISREL, AMOS) and variance-based or component-based modelling (i.e., Partial Least Squares (PLS)), which are known as analytical methods for second generation data (Bagozzi & Fornell 1982). Specifically, before model evaluation occurs, it is vital to demonstrate the importance and rationale in adopting component -based or variance-based SEM technique in data analysis. For this purpose, it is imperative that a comparison is provided between two broad families of SEM analysis techniques, such as covariance-based SEM (CBSEM) e.g., AMOS, LISREL, EQS, and variance-based or component-based SEM e.g., Smart PLS, PLS Graph. This comparison and differentiation merely aim to present their individual relevance to the current research.

The main aim of covariance-based SEM (CBSEM) is to show that the data supports the items taken from theory. The model that is examined by using CBSEM creates a covariance matrix that functions within the observed matrix's sampling variation, as well as being commonly accepted as a fit model (Hair et al. 2006). CBSEM applies most commonly Maximum Likelihood (ML) method of estimation method in order to compare the observed and estimated covariance matrix (Hair et al. 2006). Maximum Likelihood (ML) is a method that estimating the parameters of distribution probability (Hair et al. 2006). It is necessary for the sample of data within CBSEM to be higher, with a minimum of 100-150, which is understood to be normal from a multi-variance perspective in order to achieve the goodness-of-fit indices, which include chi-square, CFI, REMSE, and GFI (Hair et al. 2006; Tabachnick & Fidell 2007).

Normal distribution and a large sample size from the data are required when using CBSEM. The results will not be accurate if the assumptions are not adhered to (Hair et al. 2011).

The main aim of component-based SEM is to test the theoretical model as devised from the relevant literature, as well as to potentially predict it, but not to test the alternate model that best functions with the data (Sosik et al. 2009). The component-based SEM technique such as PLS applies Ordinary Least Squares (OLS) for estimation method in order to explain the complete level of variance (Gefen et al. 2000). Ordinary Least Squares (OLS) is a type of linear least squares method that estimates the parameters in a regression model (Gefen et al. 2000). PLS implements an OLS iterative sequence, which is factor analysis in conjunction with path difference. This helps in the analysis of single construct in a manner that minimises the residual variance level of the dependent variables in the structural model, which can withstand until the construct's average $R^2$ (coefficient of determination) is not significant anymore. As a result, this is less susceptible to the sample size and the requirements of the multivariate distribution levels (Gefen et al. 2000).

This research used component-based SEM (SmartPLS version 3.3.2) to assess the ISCFF framework. The rational for use this technique because it is commonly used in various forms of literature, while being relevant for theory building research (Vinzi et al. 2010). It is deemed to be appropriate for complex cause-effect-relationship models (Lowry & Gaskin 2014). It is also non-parametric and has fewer restrictions in relation to data distribution and the sample (Vinzi et al. 2010). Correspondingly, SEM-PLS is able to estimate how different residuals correspond and to assess their effects on the framework. Thus, PLS is the best option for the current research, as it not only creates the possibility to predict the path relations but can assist in validating the theories with CFA without using a set sample size or any data set of multiple variables (Gefen et al. 2000).

SEM includes two interrelated models: measurement model and structural model (Gefen et al. 2000). The measurement model is also referred to as Confirmatory Factor Analysis (CFA), which defines the constructs/latent variables, as well as allocating observed variables to each. It also shows the correlation between the variables and constructs, which are able to be used to show whether the constructs are measured accurately. Comparatively, the structural model, which is often referred to as regression or path analysis provides details on the hypothetical relationship between the constructs (Hair et al. 2006; Gefen et al. 2000). It is vital to clarify that the constructs or latent variable represent the theoretical construct, which is not able to be

observed directly and is able to produce an exogenous form, such as an independent variable in the model, or an endogenous form, such as a dependent variable (Hair et al. 2006).

Generally, the SEM analysis followed the two stages of establishing validity through an assessment of the entire measurement model, and to test the structure model in order to assess the constructs' relationships (Tabachnick & Fidell 2007). The ISCFF framework in Chapter 5 was evaluated through a two-step approach of the measurement model and structural model based on hierarchy basis. Initially, the psychometric reliability and validity tests were assessed by examining the measurement model for the constructs. The next step was to assess the structure model through testing research hypotheses, which focused on the hypothetical relationships based on sign, magnitude and significance levels.

### 8.6.2 Measurement Model Assessment

The measurement model presents various sequenced relationships which depict the way that measured variables show a construct (reflective or formative) that is not directly measured (Hair et al. 2016). This approach began through the model's specifications and uses CFA in the reliability assessment (Cronbach's α, indicator reliability and composite reliability) and validity (convergent and discriminant). The measurement model used factor analysis in the assessment of the observed variables and how they are loaded in their underlying construct (Hair et al. 2016). CFA is referred to as a statistical approach that is used in the mind of testing pre-determined relationships between observed measured variable and latent factors (Elsheikh 2012; Byrne 2010).

In the measurement model, the constructs can be either reflective or formative. In regard to a reflective construct, the construct causes the indicators with the arrows directing to the indicators form the construct, which shows that the indicators can interchange. Contrastingly, indicators fully constitute a formative construct, with arrows pointing to the construct from the indicators. Hence, the meaning of the construct can be altered by a change or removal of an indicator (Ringle et al. 2012). In this research, the measurement model presents only reflective constructs. The validity and reliability assessment of a reflective measurement model includes: Composite Reliability (CR) that evaluates internal consistency reliability; individual indicator reliability; Average Variance Extracted (AVE) to evaluate convergent validity; and discriminant validity (Hair et al. 2016). Table 8.17 provides the criterion for the measurement model fitting.

**Table 8.17: Measurement Model Fitting Criterions**

| Criterion | Description | Acceptable fit |
|---|---|---|
| Indicator Reliability | This shows the total standardised outer loading, which is evaluated in accordance with the loadings or indicators and measures' correlations to relevant constructs. | Item's loading >0.50 and significant at least at the 0.05 level (Hair et al. 2006) |
| Internal Consistency: Composite Reliability (CR) | This measures the level to which the measurement model's constructs are detailed by the indicators. | CR >0.60 (Hair et al. 2006) |
| Internal Consistency: Cronbach's α | The indicators' uni-dimensionality (inter-correlation) is measured with the Cronbach's α in relation to their latent construct. | α Value >0.50 (Hair et al. 2006) |
| Convergent Validity | Convergent validity defines how measured variables of certain constructs share an elevated variance proportion. This is shown by the uni-dimensionality that utilises an Average Variance Extracted (AVE). | AVE >0.50 (Fornell & Larcker 1981) |
| Discriminant Validity<br><br>Construct-level | This takes assessments by calculating each constructs' square root of the AVE, which is higher than other correlations (Hair et al. 2006). This makes sure that the latent variables connect through more variance and their specific form of indicators than in comparison to other latent variables. | $\sqrt{AVE}$>latent variable correlation (Fornell & Larcker 1981) |
| Discriminant Validity<br><br>Item-level | This shows how two apparent concepts, which are theoretically similar, contrast (Hair et al. 2006).<br><br>A construct's AVE's square root needs to be higher than the correlation that exists from one construct to another (Fornell & Larcker 1981).<br><br>The item's cross-loading for the indicators is highest for the set construct. | Loading of each indicator >cross loadings<br><br>Cross loading <0.4 (Hair et al. 2006) |
| Model Fit | The fit indices provide a direct measurement of the level that a specified model creates observed data (Hair et al. 2006). SRMR is utilised to determine the level of model fit. NFI shows an index comparison from the proposed and base model (Hair et al. 2006). | SRMR < 0.08 (Hair et al. 2006)<br><br>NFI > 0.9 (Hair et al. 2006) |

### *8.6.2.1 Reliability Assessment*

For the assessment of the measurement model, the first step was to assess the reliability of the measuring observed variables/items. The reliability of the measurement model was evaluated in this research by assessing the indicator reliability and internal consistency reliability. The

following subsections present and discuss the results for analysis in order to evaluate the reliability of the measurement model.

*8.6.2.1.1 Indicator Reliability*

The indicator reliability is measured by examination of items loadings. The purpose of assessing indicator reliability is to evaluate how variables or sets of variables are consistent with the measurement intention (Urbach & Ahlemann 2010). A higher outer-loading level on a variable shows how an associated measure connects strongly with the variable measured (Hair et al. 2016), factor loading for the items needs to be 0.50 or above (Hair et al. 2016). A measurement model is shown to present adequate indicator reliability when the item loading estimates are above 0.70, as this highlights the connection strength between the latent variable and the item (Hair et al. 2017).

The measurement of indicator reliability was conducted in this research through factor loadings (outer loading) for each item. The factor loading of items ranged from lower bound 0.51 to upper bound 0.89 (see Table 8.20). All items were shown as significant with a level of 0.001. Although when the loading is between 0.50 and 0.70, it is able to be kept based upon how these items contribute to the AVE and CR. Also, indicators exhibiting factor loadings of less than 0.50 need to be removed (Hair et al. 2017). In total, there were twelves items from the constructs of agreeableness, conscientiousness, extraversion, openness and neuroticism were removed due to their low level of loading (see Appendix N). Two items, which failed to meet the EFA criteria test were deleted as a result of high cross-load in relation to other constructs, and the low loading that was analysed again in the CFA test. Consequently, the results indicated that SET2 and JS3 from Security Education and Training and Job Satisfaction constructs had a loading less than 0.50. They were removed, which resulted in CR and AVE increasing to above the recommended threshold (0.70 and 0.50) (Hair et al. 2016). As a result, the measurement model items displayed loadings of above 0.50, and provided sufficient indicator reliability.

*8.6.2.1.2 Internal Consistency*

Internal consistency provides reliability, which helps to determine results' consistency levels among items with the replicable variables (Hair et al. 2016). This showed that items with the same constructs presented higher correlations between them. In regard to the measurement model, internal consistency is able to be assessed with Cronbach's *a*, which measured the

unidimensionality of internal constancy of various item scales. This method helped this research to provide an estimate for the levels of reliability as shown by indicator inter-correlations. Constructs that presented elevated Cronbach's *a* value shown that the construct's items present the same range (Cronbach 1971). The internal consistency was measured through the use of Composite Reliability (CR) within PLS, which provided a measurement of how the assigned items measured the constructs (Fornell & Larcker 1981). A value between 0.70 and 0.90 should be presented by CR values between 0 and 1. The higher values, and in particular above 0.95, indicate a level of indifference from the indicator's measurement (Hair et al. 2017).

In general, both Composite Reliability (CR) and Cronbach's *a* measure internal consistency, although composite reliability does consider how indicators present alternative loading levels. In the current research, Cronbach's α and composite reliability have examined (see Table 8.18). It has been shown that Cronbach's α value was higher than the requirement value of 0.50 (Hair et al. 2006). This demonstrates the values of CR for the current research's constructs, which ranges from 0.77 to 0.93; indeed, the values were all above 0.70 (Hair et al. 2006). Therefore, it can be observed that the items used to represent the constructs have adequate levels of internal consistency reliability.

**Table 8.18: Convergent Validity and Reliability for the Constructs**

| Construct | Cronbach's Alpha | Composite Reliability (CR) | Average Variance Extracted (AVE) |
|---|---|---|---|
| Agreeableness | 0.848 | 0.885 | 0.526 |
| Conscientiousness | 0.845 | 0.877 | 0.505 |
| Ethical conduct | 0.860 | 0.915 | 0.781 |
| Extraversion | 0.863 | 0.895 | 0.587 |
| Job satisfaction | 0.791 | 0.856 | 0.543 |
| Neuroticism | 0.912 | 0.930 | 0.727 |
| Openness | 0.842 | 0.879 | 0.512 |
| Risk analysis & assessment | 0.636 | 0.802 | 0.586 |
| Security awareness | 0.664 | 0.815 | 0.596 |
| Security compliance | 0.630 | 0.799 | 0.572 |
| Security education & training | 0.557 | 0.773 | 0.533 |
| Security ownership | 0.760 | 0.862 | 0.676 |
| Security policy | 0.797 | 0.869 | 0.625 |
| Top Management | 0.680 | 0.804 | 0.507 |

#### *8.6.2.2 Assessment of Construct Validity*

After assessing the reliability of measurement model, a second step was to assess the validity of the measuring observed variables/items. In this research, the validity of the measurement model was evaluated by assessing convergent validity and discriminant validity. The following subsections present the results for analysis to evaluate the validity of measurement model.

##### *8.6.2.2.1 Convergent Validity*

Convergent validity incorporates how individual items reflect a construct that converges when compared to items that measuring different constructs. It demonstrates that a particular set of items can represent a singular main construct, which is able to be shown through its uni-dimensionality. This can be assessed through the use of the Average Variance Extracted (AVE) value. When a construct's AVE value is at a minimum of 0.50, the adequate convergent validity is achieved (Fornell & Larcker 1981). In this research, all the constructs have an AVE range from 0.50 to 0.78, as shown in the Table 8.18. All constructs have the potential to explain, on average, in excess of 50% of the variance to its measuring items, which is shown by an adequate convergent validity presented by the measurement model. The findings also shown that a convergent validity and good internal consistency were present in the measurement model, and thus, it can be understood that the measurement indicators from each construct measured sufficiently and focused purely on that particular construct.

##### *8.6.2.2.2 Discriminate Validity*

Discriminate validity complements convergent validity, as it presents two conceptually alternate constructs that are exhibited in different ways, such as when a set of measurement items are believed to not be in unidimensional form (Henseler 2009). This form of validity test focuses on the construct variances, which require knowledge of how one construct has an elevated level of variance through its particular items in comparison to other constructs (Hair et al. 2017). Two forms of measuring discriminant validity that commonly used are: Fornell-Larcker's criterion at construct-level (Fornell & Larcker 1981); and the cross-loading at the item level (Chin 1998).

Fornell and Larcker's criterion compares the square root of the AVE against the latent construct correlation (Hair et al. 2016). A latent variable is required to share more variance with the assigned indicators than in relation to different latent variables. As a result, each construct AVE

square root needs to present a higher value than what is shown from the correlations of different latent constructs (Hair et al. 2016). At the item level, the second assessment for discriminant validity analyses cross-loading within the process of factor loading. It examines the indicators and compares them to the different correlations of constructs. The factor loading indicators on the assigned construct need to be at a greater level than the loading levels on constructs (Chin 1998).

The measurement model discriminant validity in this research was assessed through the use of two different measurements: Fornell and Larcker's criterion; and cross-loadings. The measurement model has adequate discriminant validity levels if the square root of the AVE is in excess of the correlations between what is measured and the other measurements, as well as when an indicator's loading is higher for its respective construct when compared to different constructs. In this research, from corresponding rows and columns, the AVE's square root is higher than the off-diagonal elements. There are no inter-construct correlation values in excess of the AVE's square root of the AVE, as displayed in Table 8.19. The **bolded** elements in the table represent the square root of the AVE and the inter-correlation's non-bolded values between constructs.

**Table 8.19: Discriminant Validity-Fornell Larcker Criterion**

| | Agr | Con | EC | Ext | JS | Neu | Ope | RA | SA | SC | SET | SO | SP | TM |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Agr** | **0.725** | | | | | | | | | | | | | |
| **Con** | 0.222 | **0.710** | | | | | | | | | | | | |
| **EC** | 0.274 | 0.196 | **0.884** | | | | | | | | | | | |
| **Ext** | 0.002 | 0.084 | 0.176 | **0.766** | | | | | | | | | | |
| **JS** | 0.116 | 0.100 | 0.253 | 0.065 | **0.737** | | | | | | | | | |
| **Neu** | 0.013 | -0.107 | -0.029 | 0.045 | -0.044 | **0.853** | | | | | | | | |
| **Ope** | 0.259 | 0.268 | 0.284 | 0.119 | 0.270 | 0.003 | **0.716** | | | | | | | |
| **RA** | 0.224 | 0.198 | 0.559 | 0.106 | 0.288 | -0.059 | 0.237 | **0.766** | | | | | | |
| **SA** | 0.287 | 0.181 | 0.500 | 0.153 | 0.321 | -0.076 | 0.257 | 0.525 | **0.772** | | | | | |
| **SC** | 0.301 | 0.281 | 0.597 | 0.202 | 0.416 | -0.091 | 0.342 | 0.602 | 0.578 | **0.756** | | | | |
| **SET** | 0.208 | 0.255 | 0.510 | 0.061 | 0.290 | -0.104 | 0.243 | 0.546 | 0.547 | 0.528 | **0.730** | | | |
| **SO** | 0.335 | 0.304 | 0.500 | 0.025 | 0.340 | -0.116 | 0.318 | 0.537 | 0.554 | 0.632 | 0.480 | **0.822** | | |
| **SP** | 0.150 | 0.193 | 0.451 | 0.127 | 0.404 | -0.022 | 0.258 | 0.415 | 0.560 | 0.504 | 0.483 | 0.447 | **0.790** | |
| **TM** | 0.185 | 0.098 | 0.412 | 0.063 | 0.359 | 0.007 | 0.157 | 0.422 | 0.513 | 0.534 | 0.455 | 0.476 | 0.587 | **0.712** |

The cross-loading within factor loading was examined for the item-level discriminant validity and results are presented in Table **8.20**. This enables the measuring items within a construct to be higher than the cross-loadings shown. In the column and row, it can be seen that indicator variables for Job Satisfaction (JS) were presented by JS1, JS2, JS4, JS5 and JS6 with loadings (0.77, 0.70, 0.70, 0.78, and 0.70, respectively), which are higher than indicator variables that include Ethical Conduct (EC) and Risk Analysis (RA) in the same block. Furthermore, all measurement items used had higher loaded levels measured against their intended latent variable in comparison to different variables that had no cross-loadings and a lack of connecting measurement errors. The measurement model discriminant validity is confirmed by the output of cross-loading.

**Table 8.20: Factors/Outer-Loading with Cross-Loading**

| | Agr | Con | EC | Ext | JS | Neu | Ope | RA | SA | SC | SET | SO | SP | TM |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Agr1** | **0.81** | 0.22 | 0.21 | 0.01 | 0.11 | 0.05 | 0.24 | 0.21 | 0.24 | 0.32 | 0.21 | 0.33 | 0.16 | 0.22 |
| **Agr2** | **0.81** | 0.17 | 0.23 | 0.00 | 0.08 | -0.01 | 0.26 | 0.15 | 0.23 | 0.22 | 0.16 | 0.24 | 0.07 | 0.13 |
| **Agr3** | **0.70** | 0.19 | 0.17 | 0.07 | 0.08 | -0.04 | 0.21 | 0.13 | 0.16 | 0.18 | 0.08 | 0.24 | 0.04 | 0.08 |
| **Agr4** | **0.55** | 0.05 | 0.16 | 0.06 | 0.16 | -0.04 | 0.15 | 0.10 | 0.18 | 0.14 | 0.11 | 0.14 | 0.14 | 0.07 |
| **Agr5** | **0.66** | 0.16 | 0.18 | -0.04 | 0.06 | 0.03 | 0.05 | 0.24 | 0.19 | 0.18 | 0.14 | 0.21 | 0.17 | 0.09 |
| **Agr8** | **0.76** | 0.15 | 0.21 | -0.06 | 0.10 | 0.04 | 0.16 | 0.17 | 0.19 | 0.25 | 0.18 | 0.27 | 0.13 | 0.19 |
| **Agr9** | **0.75** | 0.16 | 0.23 | -0.01 | 0.02 | 0.00 | 0.23 | 0.13 | 0.26 | 0.19 | 0.16 | 0.23 | 0.06 | 0.11 |
| **Con1** | 0.26 | **0.72** | 0.27 | 0.09 | 0.18 | -0.03 | 0.40 | 0.24 | 0.21 | 0.32 | 0.28 | 0.33 | 0.21 | 0.12 |
| **Con2** | 0.16 | **0.73** | 0.18 | 0.09 | 0.10 | -0.02 | 0.20 | 0.17 | 0.11 | 0.19 | 0.14 | 0.20 | 0.11 | 0.00 |
| **Con3** | 0.07 | **0.69** | 0.11 | 0.07 | 0.06 | -0.10 | 0.15 | 0.08 | 0.09 | 0.14 | 0.16 | 0.16 | 0.11 | 0.00 |
| **Con4** | 0.04 | **0.68** | 0.05 | -0.02 | 0.05 | -0.13 | 0.09 | 0.09 | 0.09 | 0.15 | 0.13 | 0.21 | 0.11 | 0.08 |
| **Con5** | 0.06 | **0.64** | 0.01 | 0.02 | -0.03 | -0.14 | -0.01 | 0.01 | 0.00 | 0.07 | 0.11 | 0.16 | 0.08 | 0.03 |
| **Con6** | 0.16 | **0.77** | 0.07 | 0.07 | 0.01 | -0.15 | 0.08 | 0.10 | 0.13 | 0.19 | 0.19 | 0.18 | 0.14 | 0.09 |
| **Con7** | 0.22 | **0.73** | 0.12 | 0.05 | 0.01 | -0.04 | 0.17 | 0.14 | 0.15 | 0.18 | 0.15 | 0.17 | 0.11 | 0.11 |
| **EC1** | 0.20 | 0.17 | **0.86** | 0.14 | 0.19 | 0.01 | 0.24 | 0.46 | 0.42 | 0.53 | 0.40 | 0.41 | 0.32 | 0.38 |
| **EC2** | 0.23 | 0.12 | **0.90** | 0.18 | 0.21 | -0.05 | 0.20 | 0.49 | 0.45 | 0.54 | 0.45 | 0.47 | 0.41 | 0.34 |
| **EC3** | 0.30 | 0.23 | **0.90** | 0.15 | 0.27 | -0.04 | 0.32 | 0.53 | 0.45 | 0.52 | 0.50 | 0.45 | 0.46 | 0.38 |
| **Ext1** | -0.02 | 0.04 | 0.11 | **0.72** | 0.06 | 0.11 | 0.07 | 0.12 | 0.10 | 0.14 | 0.03 | 0.03 | 0.10 | 0.06 |
| **Ext2** | 0.07 | 0.11 | 0.10 | **0.77** | 0.05 | -0.04 | 0.08 | 0.06 | 0.07 | 0.16 | 0.02 | 0.02 | 0.03 | 0.06 |
| **Ext3** | -0.01 | 0.06 | 0.09 | **0.75** | 0.02 | 0.04 | 0.13 | 0.06 | 0.11 | 0.12 | 0.05 | -0.06 | 0.12 | 0.00 |
| **Ext4** | 0.01 | 0.09 | 0.20 | **0.80** | 0.06 | 0.03 | 0.09 | 0.06 | 0.11 | 0.19 | 0.06 | 0.04 | 0.10 | 0.10 |
| **Ext5** | 0.00 | 0.05 | 0.15 | **0.80** | 0.06 | 0.06 | 0.09 | 0.12 | 0.21 | 0.15 | 0.07 | 0.03 | 0.15 | 0.03 |
| **Ext8** | -0.05 | 0.04 | 0.13 | **0.75** | 0.02 | 0.04 | 0.14 | 0.02 | 0.03 | 0.13 | 0.03 | 0.00 | 0.07 | 0.04 |
| **JS1** | 0.08 | 0.10 | 0.20 | 0.05 | **0.78** | -0.02 | 0.24 | 0.20 | 0.32 | 0.32 | 0.23 | 0.28 | 0.33 | 0.30 |
| **JS2** | 0.16 | 0.07 | 0.19 | 0.04 | **0.71** | -0.07 | 0.15 | 0.22 | 0.29 | 0.29 | 0.23 | 0.27 | 0.28 | 0.28 |
| **JS4** | 0.06 | 0.04 | 0.18 | 0.11 | **0.71** | 0.01 | 0.11 | 0.25 | 0.18 | 0.27 | 0.19 | 0.21 | 0.21 | 0.25 |
| **JS5** | -0.02 | 0.04 | 0.20 | 0.05 | **0.78** | 0.01 | 0.21 | 0.23 | 0.12 | 0.33 | 0.19 | 0.22 | 0.34 | 0.28 |
| **JS6** | 0.12 | 0.10 | 0.16 | -0.01 | **0.71** | -0.08 | 0.27 | 0.18 | 0.23 | 0.32 | 0.22 | 0.26 | 0.32 | 0.21 |
| **Neu2** | 0.06 | -0.11 | -0.02 | -0.11 | -0.02 | **0.88** | 0.04 | -0.03 | -0.03 | -0.09 | -0.11 | -0.09 | -0.01 | -0.01 |
| **Neu3** | 0.05 | -0.09 | -0.04 | 0.01 | 0.02 | **0.85** | 0.00 | -0.03 | -0.07 | -0.08 | -0.06 | -0.06 | -0.01 | 0.01 |
| **Neu4** | -0.05 | -0.11 | 0.03 | 0.04 | -0.06 | **0.82** | 0.02 | 0.05 | -0.02 | -0.03 | -0.06 | -0.07 | 0.05 | 0.03 |
| **Neu5** | -0.02 | -0.08 | -0.07 | 0.08 | -0.06 | **0.86** | 0.04 | -0.08 | -0.15 | -0.07 | -0.12 | -0.12 | -0.10 | -0.01 |
| **Neu7** | 0.03 | -0.05 | 0.08 | 0.06 | -0.03 | **0.85** | 0.04 | -0.04 | 0.00 | -0.02 | -0.09 | -0.06 | -0.01 | 0.09 |
| **Ope1** | 0.22 | 0.14 | 0.21 | 0.08 | 0.23 | -0.03 | **0.84** | 0.19 | 0.18 | 0.25 | 0.17 | 0.25 | 0.15 | 0.13 |
| **Ope2** | 0.26 | 0.46 | 0.29 | 0.15 | 0.22 | 0.04 | **0.59** | 0.24 | 0.25 | 0.38 | 0.27 | 0.30 | 0.21 | 0.16 |
| **Ope4** | 0.15 | 0.16 | 0.20 | 0.09 | 0.15 | 0.02 | **0.73** | 0.15 | 0.20 | 0.20 | 0.15 | 0.19 | 0.23 | 0.10 |
| **Ope5** | 0.19 | 0.05 | 0.09 | 0.05 | 0.18 | 0.04 | **0.73** | 0.11 | 0.10 | 0.13 | 0.08 | 0.15 | 0.12 | 0.02 |
| **Ope6** | 0.11 | 0.09 | 0.23 | 0.10 | 0.19 | -0.05 | **0.71** | 0.17 | 0.14 | 0.21 | 0.19 | 0.16 | 0.25 | 0.14 |
| **Ope7** | 0.13 | 0.10 | 0.15 | 0.04 | 0.12 | 0.02 | **0.62** | 0.07 | 0.17 | 0.20 | 0.13 | 0.20 | 0.15 | 0.10 |
| **Ope8** | 0.17 | 0.13 | 0.15 | 0.05 | 0.22 | -0.04 | **0.76** | 0.16 | 0.16 | 0.20 | 0.14 | 0.24 | 0.15 | 0.08 |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Ope10** | 0.11 | 0.16 | 0.30 | 0.08 | 0.13 | -0.11 | **0.51** | 0.17 | 0.12 | 0.24 | 0.19 | 0.16 | 0.26 | 0.03 |
| **RA1** | 0.11 | 0.03 | 0.22 | 0.08 | 0.14 | 0.07 | 0.23 | **0.51** | 0.26 | 0.28 | 0.25 | 0.21 | 0.31 | 0.28 |
| **RA2** | 0.17 | 0.17 | 0.52 | 0.10 | 0.26 | -0.06 | 0.15 | **0.88** | 0.49 | 0.54 | 0.48 | 0.49 | 0.39 | 0.37 |
| **RA3** | 0.22 | 0.21 | 0.48 | 0.07 | 0.22 | -0.10 | 0.21 | **0.86** | 0.42 | 0.52 | 0.48 | 0.47 | 0.28 | 0.33 |
| **SA1** | 0.24 | 0.16 | 0.37 | 0.12 | 0.26 | -0.01 | 0.21 | 0.36 | **0.80** | 0.45 | 0.36 | 0.43 | 0.52 | 0.45 |
| **SA2** | 0.12 | 0.07 | 0.31 | 0.12 | 0.23 | 0.02 | 0.14 | 0.33 | **0.71** | 0.34 | 0.36 | 0.28 | 0.42 | 0.39 |
| **SA3** | 0.28 | 0.17 | 0.46 | 0.12 | 0.25 | -0.16 | 0.23 | 0.51 | **0.80** | 0.52 | 0.53 | 0.54 | 0.36 | 0.36 |
| **SC1** | 0.25 | 0.25 | 0.58 | 0.14 | 0.33 | -0.18 | 0.27 | 0.62 | 0.54 | **0.82** | 0.48 | 0.64 | 0.38 | 0.40 |
| **SC2** | 0.24 | 0.22 | 0.37 | 0.16 | 0.30 | 0.02 | 0.29 | 0.38 | 0.40 | **0.74** | 0.35 | 0.41 | 0.48 | 0.47 |
| **SC3** | 0.19 | 0.15 | 0.36 | 0.17 | 0.31 | -0.01 | 0.22 | 0.31 | 0.33 | **0.70** | 0.35 | 0.32 | 0.29 | 0.34 |
| **SET1** | 0.19 | 0.17 | 0.28 | 0.02 | 0.28 | 0.00 | 0.13 | 0.27 | 0.41 | 0.35 | **0.66** | 0.35 | 0.47 | 0.45 |
| **SET3** | 0.10 | 0.17 | 0.37 | 0.09 | 0.14 | -0.11 | 0.16 | 0.39 | 0.40 | 0.39 | **0.74** | 0.32 | 0.27 | 0.24 |
| **SET4** | 0.17 | 0.22 | 0.46 | 0.02 | 0.21 | -0.11 | 0.24 | 0.52 | 0.40 | 0.42 | **0.79** | 0.38 | 0.32 | 0.30 |
| **SO1** | 0.27 | 0.30 | 0.49 | 0.10 | 0.33 | -0.10 | 0.28 | 0.52 | 0.51 | 0.60 | 0.47 | **0.82** | 0.41 | 0.43 |
| **SO2** | 0.27 | 0.22 | 0.38 | -0.08 | 0.25 | -0.08 | 0.24 | 0.38 | 0.43 | 0.49 | 0.34 | **0.81** | 0.37 | 0.38 |
| **SO3** | 0.29 | 0.22 | 0.35 | 0.03 | 0.26 | -0.10 | 0.26 | 0.41 | 0.42 | 0.45 | 0.37 | **0.84** | 0.32 | 0.36 |
| **SP1** | 0.12 | 0.12 | 0.39 | 0.11 | 0.34 | 0.00 | 0.19 | 0.30 | 0.49 | 0.39 | 0.37 | 0.37 | **0.80** | 0.44 |
| **SP2** | 0.07 | 0.14 | 0.32 | 0.04 | 0.35 | -0.04 | 0.20 | 0.33 | 0.43 | 0.38 | 0.33 | 0.34 | **0.85** | 0.53 |
| **SP3** | 0.08 | 0.13 | 0.28 | 0.16 | 0.33 | -0.04 | 0.17 | 0.23 | 0.42 | 0.34 | 0.37 | 0.31 | **0.80** | 0.47 |
| **SP4** | 0.19 | 0.22 | 0.41 | 0.10 | 0.26 | 0.00 | 0.25 | 0.43 | 0.42 | 0.46 | 0.44 | 0.38 | **0.69** | 0.42 |
| **TM1** | 0.14 | 0.11 | 0.37 | 0.10 | 0.27 | -0.02 | 0.13 | 0.37 | 0.45 | 0.47 | 0.32 | 0.44 | 0.49 | **0.76** |
| **TM2** | 0.10 | 0.04 | 0.29 | 0.09 | 0.27 | 0.00 | 0.10 | 0.25 | 0.31 | 0.37 | 0.25 | 0.31 | 0.46 | **0.75** |
| **TM4** | 0.12 | 0.00 | 0.21 | -0.04 | 0.23 | 0.01 | 0.10 | 0.21 | 0.31 | 0.32 | 0.31 | 0.27 | 0.38 | **0.67** |
| **TM5** | 0.17 | 0.11 | 0.28 | 0.00 | 0.25 | 0.05 | 0.12 | 0.34 | 0.36 | 0.34 | 0.41 | 0.31 | 0.32 | **0.66** |

#### *8.6.2.3 Goodness of Model Fit*

CFA is able to show how a particular factor model represents the data set, through an examination of the model fit indices. The model is invariably accepted when the fit indices prove to be good. Certain model-fit criteria, which include SRMR and NFI for PLS models are provided by SmartPLS. The available model fit assessment criteria in PLS-SEM remain not to be fully explored and understood, when comparing with CBSEM criteria (Henseler et.al. 2010)

Fit indices are shown to be one of two concepts: absolute or incremental. Absolute fit indices demonstrate a direct measure of the way a specified model reproduces observed data sets (Hair et al. 2016). Specifically, the main absolute fit index is a Chi-square (X2) statistic; this normally incorporates the value of X2, degree of the freedom (df) and significance level (p-value). However, absolute indices can potentially be negatively affected by the size of a sample (Kline

2005). Consequently, various indices have been developed to quantify the degree of model fit (Shah & Goldstein 2006). Standardised Root Mean Square Residual (SRMR) is a main index that is created to quantify how a model fit best function. The SRMR is shown to be the difference between a predicted correlation and one that is observed. It enables the average magnitude of the discrepancies between the correlations (anticipated and observed) to be a total measurement of (model) fit criterion. A value less than 0.10 and of 0.08 are considered as values with a good fit (Hair et al. 2017).

Incremental fit indices are referred to the degree of how the model of interest is better than the subsequent different baseline models (Hair et al. 2006). The most commonly found baseline model is a 'null-model', which presents the complete observed variables to not be correlated. Normed-fit-index (NFI) is a popular incremental fit index. NFI represents a comparative index between a baseline model and what was predicted. This is achieved by calculating the model's Chi-square value and comparing it against a relevant target. The NFI results are measured in values of 0 to 1. The fit is determined to be better when it is closer to 1 (Lohmöller 1989). According to Hair et al. (2014) standards for acceptable fit, SRMR is required to be <0.08; with an NFI' value at >0.90.

The SRMR and NFI were used in this research to evaluate the model fit, as the SmartPls was used in the analysis. The results indicate that fit statistics for the research model demonstrate a good fit. The value of SRMR (0.076<0.08) and NFI (0.91 > 0.90), as shown in Table 8.21. The saturated model presents an assessment of correlation between constructs, while the estimated model is based on the complete effect scheme, which relates and connects to the model structure.

**Table 8.21: Model Fit Indices**

| SEM | Saturated Model | Estimated Model |
|---|---|---|
| SRMR | 0.076 | 0.078 |
| NFI | 0.91 | 0.92 |

### 8.6.3 Final Measurement Model

For the final measurement model, the two methods of EFA and CFA were applied. Although CFA was principally used, due to the fact that the study's constructs had been developed. EFA was used as additional analysis in order to demonstrate that the constructs had been developed

in a good manner. Correspondingly, the security antecedents' results showed that fourteen constructs had been developed well, which the EFA analysis results for each construct. The findings also highlighted that these constructs were suitable for CFA utilisation.

The research framework constructs were redeveloped from the CFA restructured by the removal of fourteen items which had a total factor loading of <0.50 in the development of CR and AVE. Construct validity was obtained for the constructs, as the variables were loaded substantially onto their corresponding factors with a sufficient reliability level. The measurement model presents acceptable and satisfactory indicator reliability, convergent validity, and discriminant validity tests. Overall, it can be determined from this research, the measurement items for the constructs are valid and able to be used in providing an estimation of the parameters in the structural model. The CFA model shows a sequence correlation which suggests the way that measured variables demonstrate an indirectly measured construct (Hair et al. 2006).

The measurement model in the current research was developed by implementing the constructs into one single model (see Figure 8.13). This particular model includes a total of fourteen reflective constructs and a second-order construct that has latent variable scores for the three dimensions that constitute the culture of information security. The second-order models are commonly able to be applied in research contexts where measurement tools provide an assessment of various connected constructs, which numerous items measure. The second-order model presents a hypothesis that apparent distinct. But related constructs can be accounted for by in excess of one commonly related main higher order construct.

The indicators of the construct's lower-order factors (security awareness, security ownership and security compliance) were used to estimate the second-order construct security culture. This research focused on security culture as theoretically connected to security awareness, security ownership and security compliance. There were strong correlations between security culture and its levels of reflection: security awareness (0.824), security ownership (0.860) and security compliance (0.871). This indicates a strong existing correlation among the constructs. The measurement model consisted of three layers: firstly, the indicators (sixty-three items), which signified the measured factors; secondly, first-order factors, which signified the main fourteen constructs; and thirdly, second-order factors (security culture), which signified the underlying three constructs (security awareness, security ownership and security compliance). This was formed as a result of their greater correlation levels and the relationship strength

between the first- and second-order models. The results from the measurement model highlight that the constructs are at an adequate level, as presented in Figure 8.13.

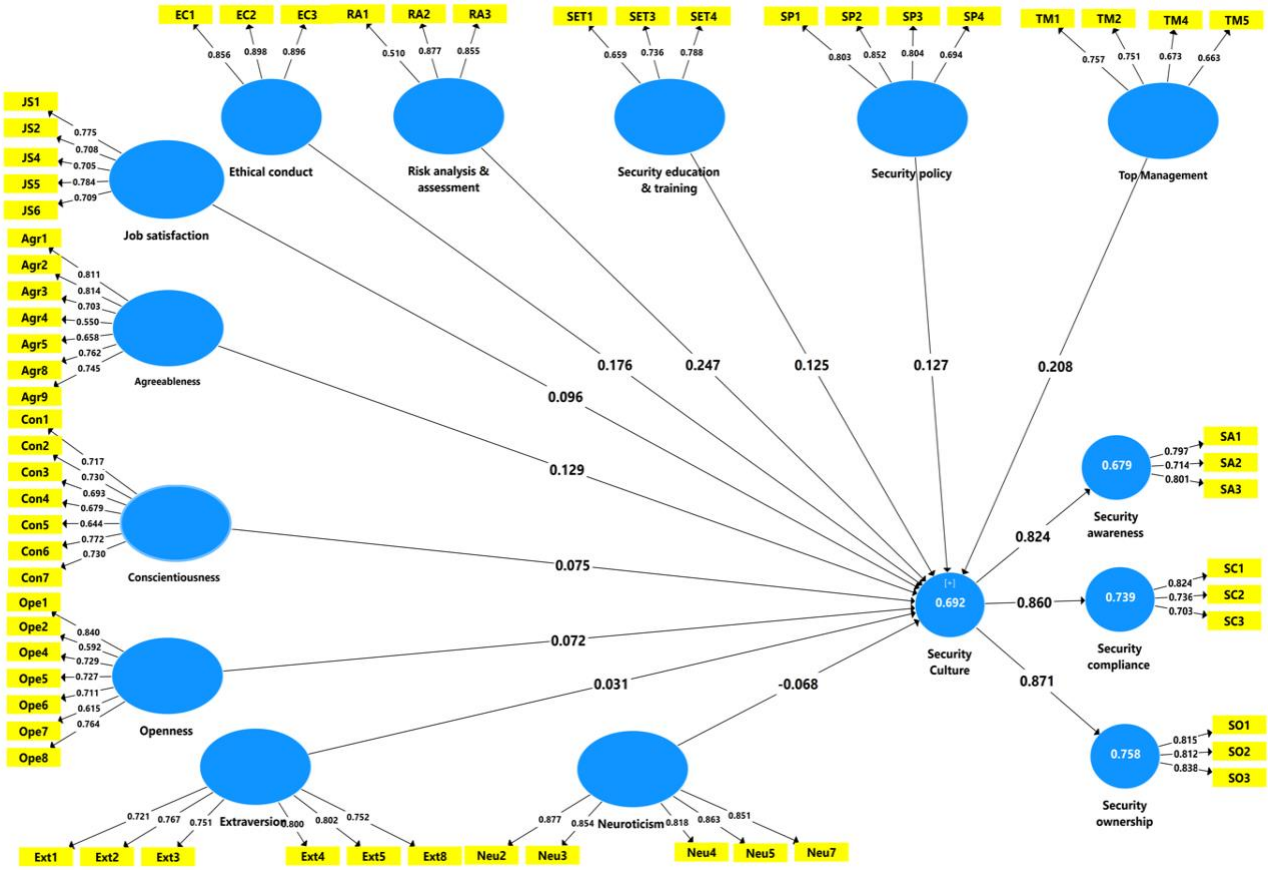



**Figure 8.13:Measurement Model for Information Security Culture**

### 8.6.4 Structure Model Assessment

Once a reliable measurement model is established and validated, the following stage is to provide an estimation of the assumed causal and covariance linear relationship among both latent variables (independent and dependent). The structural model enables evaluation of the inner-model or path model, which is produced through a series of structural equations that demonstrate the theoretical model (Chin 2010). PLS is not able to support statistical evaluation of the model's overall goodness of fit, which is based on the assumption of distribution-free variance (e.g., GFI, AGFI, CFI). Therefore, non-parametric statistical tests were used in the evaluation of the model fitting. In particular, the main criteria to conduct the structural model assessment in this research were as follows: coefficient of determination ($R^2$) for dependent variable, estimation of path coefficient (β), effect size (*f2*) and prediction relevance (*q2*) and significance is tested with the help of t-value and P-Value. A bootstrapping procedure was used

to examine the value of all the correlations, which included 1000 iterations and not a single change in sign. The bootstrap confidence intervals were measured from the base of a two-tailed test that had an important level at 1% (Hair et al. 2017). Table 8.22 below shows the threshold value for the criteria.

**Table 8.22: Structure Model Assessment Criteria**

| Criterion | Description | Acceptable Fit |
|---|---|---|
| Coefficient of determination: $R^2$ of dependent (endogenous) latent variable | The coefficient of determination measures the level of variability in outcome and how it relates to the independent observed variables (Tabachnick & Fidell 2007; Hair et al. 2006). | Value 0.67 is substantial<br>Value 0.333 is moderate<br>Value 0.190 is weak (Chin 1998) |
| Estimate for β path coefficient | This estimate measures various correlation coefficients between both variables (independent and dependent) (Tabachnick & Fidell 2007). The value needs to be a minimum of 0.100 and adhere to the correct algebraic sign (+ or -), at <= 0.05. | Significance using t-statistics and p-value<br>> 1.96 at p< 0.05<br>>2.58 at p < 0.01<br>>3.30 at p< 0.001<br>(Hair et al. 2006) |
| Effect size *f*2 | This effect measures the ratio representation of the improvement in predicting the model fitting results (Tabachnick & Fidell 2007). | Value 0.35 is large<br><br>Value 0.15 is medium<br><br>Value 0.02 is weak (Chin 1998) |
| The Stone-Geissers Q2 | The Stone-Geissers measure the predictive nature of the model through the use of sample cross-validation (Geisser 1974). | Q2> 0 |

### *8.6.4.1 Path Estimation (β)*

The structural model analysis depends on evaluating the structural coefficients statistical significance that is shown in the PLS model. A hypothesis is represented by each path in the structural model that creates a relationship between two latent variables. The path estimation, referred to as nomological validity, was performed in order to examine the significance of the path relations in the inner-model (Chin 1998). Path coefficients enable researchers to confirm a hypothesis or not, and to gain better understanding of the strength of the correlations between both types of variables (dependent and independent). Path coefficients are calculated in

ordinary least squares regression, which are able to be interpreted as standardised beta coefficients. The different path correlations in the model were examined through the regression coefficient (β). For the path coefficients, there values are shown as measured from -1 to +1, while positive values present positive reactions, and contrastingly for negative ones. The closer the value is to +1 or -1, the stronger the effect becomes (Hair et al. 2017). These coefficients should be at a minimum of 0.1 to account for a particular impact within the model, and to be significant at the 0.05 level of significance.

The utilisation of the PLS Bootstrap process can be determined in order to obtain the significance of regression coefficient β, which is based on t-value. Bootstrapping has been defined as "a re-sampling approach that draws random samples (with replacements) from the data and uses these samples to estimate the path model multiple times under slightly changed data constellations" (Hair et al. 2016, (p.162)). Bootstrapping is used to measure coefficient estimate standard errors that can produce an examination of statistical relevance (Vinzi et al. 2010). Bootstrapping produces a large, pre-determined sample; for example, 1000 or 5000. The bootstrap procedure, from the initial sample, creates cases at random that replace parts of that sample. The bootstrapping analysis enables hypotheses statistical validating, which are based on the relationships between the model's variables.

The significance of direct correlations between the constructs and security culture were tested by the structural model, as it examines the path coefficients β among the different constructs, as displayed in Figure 8.14. A two-tailed test was computed for t- and p-values at a significance level of 1%, in order to test the significance of the path coefficients. Additionally, the bootstrapping procedure of the SmartPLS has been used with a total of 500 cases and 2000 samples. The results yield t-values 1.96 and p-values <0.05, which indicate that a significant relationship exists between the model's security culture and the other constructs at a 1% level of significance.

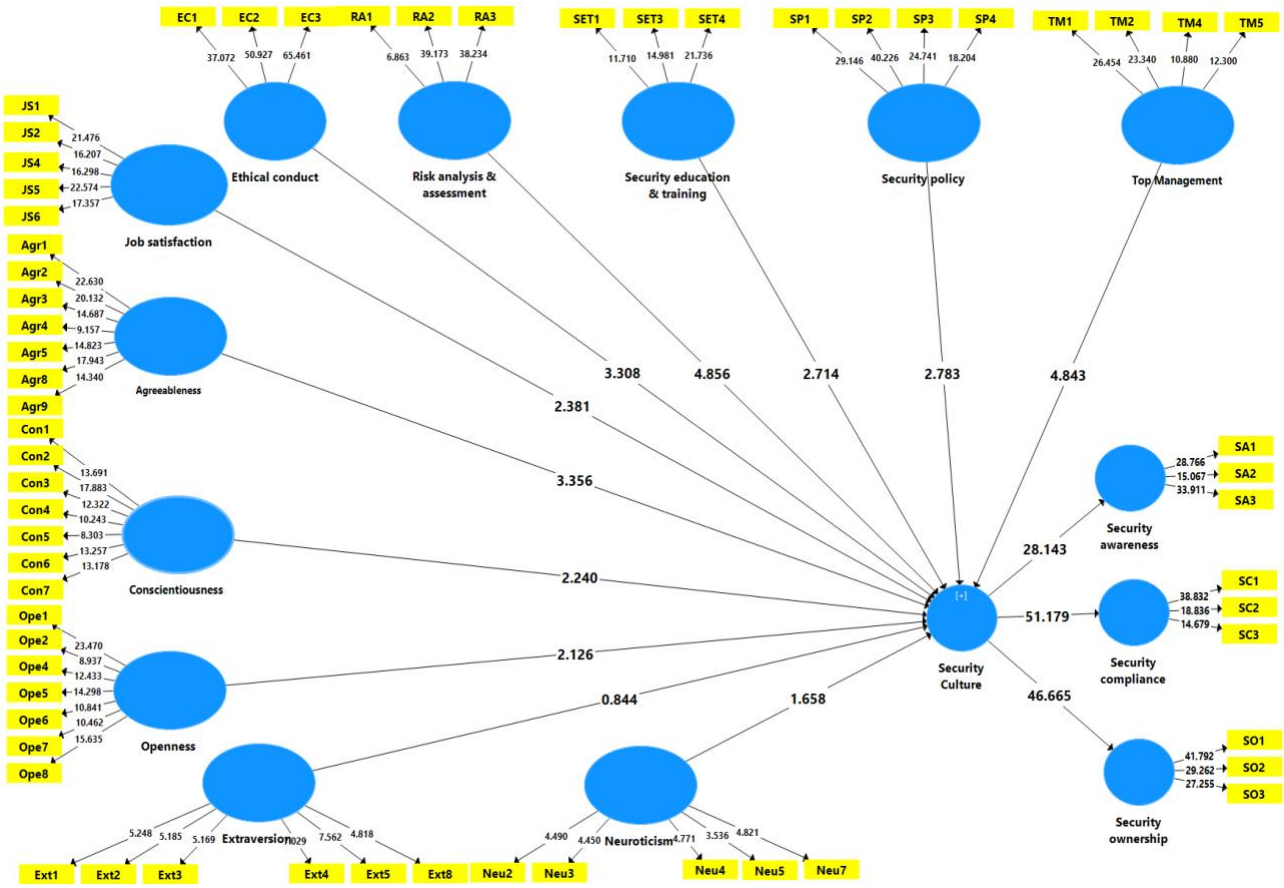



**Figure 8.14: Evaluation of the Information Security Culture Structure Model**

Table 8.23 presents the path coefficients β results, *t*-statistics, and significance level p-value for all hypothesised relationships.

**Table 8.23: Hypothesised Paths' Coefficients, Observed T-Statistics, Significant Level P-value**

| Hypothesis | Path | β | T-value | P-Values | Sig | *f*2 |
|---|---|---|---|---|---|---|
| **H1** | **TM -> ISC** | 0.208 | 4.843 | 0.000 | Yes | 0.081 |
| **H2** | **SP -> ISC** | 0.127 | 2.783 | 0.006 | Yes | 0.028 |
| **H3** | **SET -> ISC** | 0.125 | 2.714 | 0.007 | Yes | 0.028 |
| **H4** | **RA -> ISC** | 0.247 | 4.856 | 0.000 | Yes | 0.114 |
| **H5** | **EC -> ISC** | 0.176 | 3.308 | 0.001 | Yes | 0.057 |
| **H6** | **JS -> ISC** | 0.096 | 2.381 | 0.018 | Yes | 0.023 |
| **H7a** | **Agr -> ISC** | 0.129 | 3.356 | 0.001 | Yes | 0.046 |
| **H7b** | **Con -> ISC** | 0.075 | 2.240 | 0.025 | Yes | 0.016 |
| **H7c** | **Ope -> ISC** | 0.072 | 2.126 | 0.034 | Yes | 0.014 |

| Hypothesis | Path | β | T-value | P-Values | Sig | *f*2 |
|---|---|---|---|---|---|---|
| **H7d** | **Ext -> ISC** | 0.031 | 0.844 | 0.399 | No | 0.003 |
| **H7e** | **Neu -> ISC** | -0.068 | 1.658 | 0.098 | No | 0.015 |

Notes: β: Path coefficient, t: t-value, p: p-value; * p < 0.05, *f*2: effect size.

The complete path coefficients present positive, significant, direct, effects in this research framework (apart from extraversion and neuroticism). The nine hypotheses were relevant and significant from a total of eleven path relations. Supported hypotheses are significant at 0.05, as they show relevance to anticipated directions, and include a path coefficient value (β) with a range of 0.075 to 0.247. All constructs (Agr, Con, EC, JS, Ope, RA, SET, SP, TM) were positively significant and met the proposed theoretical suggestions, as the paths' results in regard to dependent variable Security Culture (SC) demonstrated. Top Management (TM) creates a significant positive influence on a model's security culture (ß =0.208; p=0.000), as it supports H1 (see Table 8.23). Security Policy (SP) presents a positive connection with the security culture (ß =0.127; p =0.006), which supports H2. Security Education and Training (SET) have a positive effect in the model's security culture in relation to the support of H3 (ß =0.125; p =0.007). To support H4, Risk Analysis and Assessment (RA) have relevant positive influences upon a model's security culture (ß =0.247; p =0.000). Ethical Conduct (EC) positively effects upon a model's security culture (ß = 0.176; p =0.001), which supports H5. Finally, Job Satisfaction (JS) creates a positive effect upon a model's security culture (ß = 0.096; p =0.018), and thus, supporting H6.

In regard to the constructs of personality traits, the results show that Agreeable personality (Agr) has a positive influence on security culture (ß = 0.129; p =0.001), which supports H7a. Similarly, the conscientious personality (Con) positively influences security culture (ß = 0.075; p =0.025), which supports H7b. Openness personality (Ope) has a relevant positive influence upon security culture (ß = 0.072; p =0.034), which supports H7c. Nevertheless, Extraversion (Ext) and Neuroticism (Neu) do not have any effect on a security culture and do not have any support. Extraversion has insignificant relevant positive influences on security culture (β=0.03, p = 0.399); thus, there was no support for H7d. Likewise, Neuroticism has insignificant negative influences upon a security culture (β=-0.06, p=0.098); this, H7e was not supported.

The strength of the effects exhibits a high level of variation, despite the effect of the majority of correlations being at a significant level. The most prominent significant path (p<0.001) was found between risk analysis and assessment and the security culture (β=0.247, t=4.85); this

was followed by top management and security culture (β=0.208, t=4.84). Meanwhile, two constructs demonstrate a weak effect on the security culture. A low significance of ($p<0.005$) was shown between openness and security culture (β=0.072, t= 2.12), which was followed by conscientious and security culture (ß=0.075; t =2.240). It can, therefore, be suggested that the context of security culture generally has a positive influence through risk analysis and assessment, top management, ethical conduct, agreeableness, security policy, security education and training, job satisfaction, conscientiousness and openness. The results demonstrated that two paths that worked in relation to dependent variable security culture did not have relevant levels: extraversion and neuroticism. Overall, nine of hypothesised relationships (H1-H7c) have been confirmed (see Table 8.24).

**Table 8.24: Results of the Research Hypotheses**

| **Research Hypothesis** | | **Supported** |
|---|---|---|
| **H1** | Top management support has a positive influence on the effectiveness of the security culture. | Yes |
| **H2** | Security policy has a positive influence on the effectiveness of the security culture. | Yes |
| **H3** | Security education and training has a positive influence on the effectiveness of the security culture. | Yes |
| **H4** | Security risk analysis and assessment has a positive influence on the effectiveness of the security culture. | Yes |
| **H5** | Ethical conduct has a positive influence on the effectiveness of the security culture. | Yes |
| **H6** | Job satisfaction has a positive influence on the effectiveness of the security culture. | Yes |
| **H7a** | Agreeableness has a positive influence on the effectiveness of the security culture. | Yes |
| **H7b** | Conscientious has a positive influence on the effectiveness of the security culture. | Yes |
| **H7c** | Openness has a positive influence on the effectiveness of the security culture. | Yes |

| Research Hypothesis | | Supported |
|---|---|---|
| **H7d** | Extraversion has a positive influence on the effectiveness of the security culture. | No |
| **H7e** | Neuroticism has a negative influence on the effectiveness of the security culture. | No |

H: Hypothesis

The results indicated that three dimensions that reflect the security culture have positive and significant paths; these are: security awareness, security ownership and security compliance. Subsequently, this shows that the three first-order constructs present a unique contribution to the second one. Hence, they provide justification in accepting the security culture as the second- order factor. In forming security culture, security ownership presented the greatest level of the path coefficients, which suggests a greater level of relevance to this dimension, followed by security compliance and security awareness.

Correlation coefficients were assessed through SPSS, with Pearson two-tailed correlation used that had a significance level of 1%. This offered a better examination of the correlation between the components of factors that influence information security culture and factors that constitute information security culture. The correlation values provide support to both the framework and the research hypotheses. The results show that the correlations between factors (except extraversion and neuroticism) that influence information security culture, and those that constitute information security culture are significantly positive. Hence, the absence of multicollinearity was confirmed, as all the correlation values are lower than the value of .80 (Pallant 2011). The results are presented in Table 8.25.

**Table 8.25: Correlations Among Components of Security Culture with the Key Factors**

| # | Construct | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **1** | Top Management | 1 | | | | | | | | | | | | | |
| **2** | Security Policy | 0.613 | 1 | | | | | | | | | | | | |
| **3** | Security Education & training | 0.38 | 0.426 | 1 | | | | | | | | | | | |
| **4** | Risk Analysis | 0.387 | 0.421 | 0.321 | 1 | | | | | | | | | | |
| **5** | Ethical Conduct | 0.352 | 0.445 | 0.327 | 0.517 | 1 | | | | | | | | | |
| **6** | Job Satisfaction | 0.323 | 0.384 | 0.275 | 0.266 | 0.214 | 1 | | | | | | | | |
| **7** | Agreeableness | 0.18 | 0.143 | 0.119 | 0.18 | 0.221 | 0.071 | 1 | | | | | | | |
| **8** | Conscientiousness | 0.028 | 0.123 | 0.102 | 0.132 | 0.172 | 0.018 | 0.127 | 1 | | | | | | |
| **9** | Extraversion | 0.121 | 0.145 | 0.096 | 0.154 | 0.176 | 0.095 | -0.03 | 0.03 | 1 | | | | | |
| **10** | Neuroticism | 0.037 | -0.003 | 0.051 | -0.02 | 0.022 | -0.031 | 0.026 | -0.128 | 0.058 | 1 | | | | |
| **11** | Openness | 0.136 | 0.26 | 0.163 | 0.218 | 0.26 | 0.235 | 0.169 | 0.192 | 0.12 | 0.017 | 1 | | | |
| **12** | Awareness | 0.527 | 0.563 | 0.393 | 0.49 | 0.485 | 0.244 | 0.22 | 0.107 | 0.154 | -0.03 | 0.232 | 1 | | |
| **13** | Ownership | 0.456 | 0.438 | 0.287 | 0.489 | 0.493 | 0.281 | 0.269 | 0.252 | 0.004 | -0.07 | 0.25 | 0.521 | 1 | |
| **14** | Compliance | 0.528 | 0.5 | 0.356 | 0.54 | 0.569 | 0.351 | 0.237 | 0.209 | 0.187 | -0.05 | 0.28 | 0.54 | 0.588 | 1 |

Note: correlation is significant at the 0.05 level (2-tailed).

### *8.6.4.2 Coefficient of Determination ($R^2$)*

The determination of coefficient ($R^2$) provides the variation percentage in dependent variable(s) explained by independent variable(s) (Keil et al. 2000). It is the data variability percentage that is explained by a measurement model. As with the simple regression, the coefficient is represented by the values of squares multiple correlation ($R^2$), which represents the level of latent construct's explained variance. This provides a measurement of regression function's fit level (goodness of fit), which is measured against the empirically obtained observed items (Bakhaus et al. 2016). $R^2$ values vary in accordance with the measurement of independent variables, which can include a greater number of independent variable requirement to produce a value of $R^2$ that is at a higher level, as well as with the opposite (Chin 1998). The value of $R^2$ value is from 0 to 1, and it specifies the exogenous variables' accuracy in predicting a particular construct (Hair et al. 2017). The model with $R^2$ is deemed to be measured as substantial (0.67), moderate (0.33), and weak (0.19) (Chin 1998). The value needs to be at a high level in order to determine the variance well of endogenous latent variable. Thus, a greater level of $R^2$ value augments the potential to predict the structural model. In this research, the Smart PLS algorithm function was used to obtain the values of $R^2$. While the bootstrapping function helps to produce 2000 samples from 500 cases and is used to create

values for t-statistics. In this research, security culture is an endogenous variable. Table 8.26 demonstrates that the security culture shared a high level of variance at $R^2$=0.69. All the different constructs present and detail 69% of security culture's variance. Also, by examining the endogenous variables' predictive power, it has been shown that there are substantial $R^2$ values. Overall, it is possible to conclude that this research framework has a substantial prediction power for the endogenous constructs.

**Table 8.26: The Constructs' Coefficient Determinations**

| Construct | R Square | R adjust | Q2 |
|---|---|---|---|
| Security Culture (SC) | 0.692 | 0.679 | 0.297 |
| Security Awareness (SA) | 0.679 | 0.677 | 0.394 |
| Security Compliance (SC) | 0.739 | 0.738 | 0.410 |
| Security Ownership (SO) | 0.758 | 0.757 | 0.504 |

Note: R Square: determination of coefficient ($R^2$), Q2: Stone-Geissers (predictive relevance).

The endogenous variable security culture is higher order factor with a total of three dimensions: SA (0.67), SO (0.75) and SC (0.73) as the $R^2$ values. It can be noted that the model principally presented the highest variation in security ownership, which subsequently showed a variation through security compliance. Security awareness explained a total of 67% variation. This shows that the structural model developed has the potential to predict.

### *8.6.4.3 Effect Size (f2)*

The effect $f^2$ size effect provides an evaluation of the development in $R^2$ values when a specific independent (exogenous) variable is removed. It shows the effect of predictor latent variable on a particular dependent (endogenous) variable. The effect size function *f* (similar to the partial F-test) assists in examining how the $R^2$ value becomes higher in variance percentage in relation to the dependent variable that is not explained (Gotz et al. 2010). *f2* does not provide a reference to the sample size, in contrast to the traditional F-test, but refers to the analysis population in general. Hence, no freedom was required in order to calculate the *f2* value. The *f2* values for the significant independent variables are shown with their effect size as: small (0.02), medium (0.15), and large (0.35) (Cohen 2013).

In this research, the function of *f* by Cohen (2013) calculates the changes in the inner model in regard to the effect size. In previous Table 8.23 in section ( 8.6.4.1), the last column *f2* size effect has a variety from small to large (range 0.023 to 0.114) for the exogenous variables in explaining the Security Culture. All paths towards the Security Culture were shown to be significant in the specified framework. The *f2* for the Risk Analysis and Assessment (0.114), Top Management (0.081), Ethical Conduct (0.057), Agreeableness (0.046), Security Policy (0.028), Security Education and Training (0.028) and Job Satisfaction (0.023). There is only a relationship between the assessment on Security Culture and Risk Analysis and Assessment that shows a medium significant effect (*f2* = 0.114, p = 0.000).

The minimal impact from the size indicates that by including an additional path or independent variable, there is no effect that can be observed on the shared variance of dependent variable. In regard to the substantive effect on Security Culture from the significant paths, the *f2* values were 0.016 for Conscientiousness and 0.014 for Openness. This indicates that path coefficient (β) has an approximate medium level effect on security culture that functions beyond the contributions that are created from Conscientiousness and Openness. Additionally, it is worth noticing that *f2* of some paths had an effect size that was negative or below the accepted range for Extraversion 0.003 and Neuroticism 0.015. The lack of significant impact on the dependent variable defined the negative or zero effect of these paths.

#### *8.6.4.4 Prediction Relevance ($Q^2$)*

It has been suggested by Hair et al. (2017) to examine the Stone-Geissers Q2 value (Geisser 1974), which measures the predictive potential of the model. This statistic is used to access the endogenous variable's predictive relevance, through a stage of blindfolding (Tenenhaus et al. 2005). Predictive relevance is often shown as a type of model fit indicator. While the $R^2$ value is used to measure the predictive strength of the in-sample, and the Q2 value shows the potential predictive strength of the out-of-sample model (Hair et al. 2017). Chin (1998) specifically states that the $Q^2$ depicts a measurement of how the model reconstructs the observed values and the estimates of the parameter. It has also been stated that predictive relevance is shown within models that have a $Q^2 > 0$ (Hair et al. 2017); while the higher level positive $Q^2$ value models are seen to present a stronger level of predictive relevance.

The $Q^2$ cross-valid redundancy is calculated from the blindfolding procedure, which omits a section of data matrix in order to enable the construct to be examined and produce model

parameter estimates (Chin 1998). For this to be accomplished, a set of omission distance parameters is required to ensure the correct execution of the algorithm, which needs to be a prime integer between the number of indicators and the total cases (Henseler & Fassott 2010). Subsequently, with the remaining data points, all the *d*th data from the endogenous constructs are omitted and an estimation of parameters provided. A greater level of predictive accuracy is produced, with a recommendation of omission distance D between (5 and 10) (Hair et al. 2017). Small differences between the original and predicted values show a greater value of $Q^2$ value. In this research, blindfolding was used and run with an omission distance D= 8. The SC has a $Q^2$ value of 0.297 >0, and thus, the model has a predictive relevance for endogenous variable. Table 8.26 in section ( 8.6.4.2) provides the Q2 values of all the endogenous constructs.

### 8.6.5 Multi-group Analysis with Demographic

Following the examination of direct path relationships in the central model, the next stage was to analyse the structure model from a variety of contexts by focusing on the demographic variables and determining whether the differences between path coefficients of certain groups were statistically significant. One of the main concerns in the process of comparing model estimates between groups is to make sure that construct measurements are invariant and unchanging between the groups. There are various ways of examination for the moderate effect within structural models. But there are two that are used most frequently: examination using interaction effect (product term), and examination using Multiple-Group Analysis (MGA).

In the interaction-effect or product-term effect approach, moderating effects within a structural path model is represented from a structural relationship perspective (Henseler & Fasssott 2010). The proposed model requires examination through a moderate effect that is made up of: firstly, the main considered effect (a); secondly, the moderator variable's main effect on criterion variable (b), thirdly, there is an interaction in the effect of the variable (c) (predictor x moderator). In addition, if path (c) is significantly different from zero, where a null hypothesis is potentially rejected, then it represents a moderation effect (Baron & Kenny 1986). This form does not have negative consequences until the predictors and moderator variables are shaped from the reflective indicators (Chin et al. 2003; Eberl 2010).

The Multiple-Group Analysis (MGA) tests and provides comparisons to the effect of each structural path across a variety of groups and their significance level. MGA is commonly the recommended technique of analysis, if an independent or moderator variable function

categorically (Aguinis et al. 2017). MGA enables a researcher to be able to assess in excess of two variables are impactful (same or different) between groups (MacKinnon 2011). Normally this type of group analysis is commonly accepted into the CBSEM methods as a way of determining the moderating effect; this has also been seen to be relevant to the PLS environment (Chin 2010). However, this approach is not all positive as it is necessary to test the t-value with the assumption that the data is classed as 'normal'. To overcome this issue with the PLS, it has been suggested by Dibbern and Chin (2005) that a distribution free approach and a random permutation method could be applied. MGA is performed via univariate analysis and this procedure is able to be completed by comparing between at least two groups. The moderators are examined in the MGA through data-sample division into smaller samples, which are comprised of moderating variable and the same PLS model is run for both subsamples (Chin 1998). The differences in the paths between the groups are compared by providing an examination of the t-test significance.

MGA was subsequently used for this research to investigate how impactful the demographic variables were upon the independent variables influence on the dependent ones. The reasons to select MGA approach in this research are as follows: first, the MGA approach is common in CBSEM methods, as the obtained results using PLS will assist in developing future research in the re-examination and comparison of the moderating effects that use CBSEM. Second, the majority of the demographic variables that were analysed in this research discrete and/or formed categorically, with all the predictors measured on reflective indicators; thus, adhering to Eberl's (2010) assumption that MGA is the most relevant approach in relation to the interaction effect.

The MGA could be performed by using traditional MGA method tests: ANOVA and MANOVA. The intent is to assess the significant contrasts in regard to the dependent variable's means scores between groups (Hair et al. 2006). Therefore, the measured variables in these tests require observation and analysis. The main concerns for these tests were to view the dependent variables contrasts, instead of for the latent variables, as they may not be able to be observed (Tabachnick & Fidell 2007). Nevertheless, ANOVA and MANOVA were less preferred methods when comparing the SEM techniques, as this research emphasised that dependent or criterion variables were unobserved in nature and the means of predictors or independent variables were indirectly supported on their indicator loadings.

There has been a total of four approaches to the MGA analysis within a PLS path modelling framework. The first one is the parametric approach (Henseler 2007), which is a parametric significance test for the difference of group-specific PLS-SEM results that function on the assumption of equal variances across groups. Keil et al. (2000) was first to introduce this approach. This approach involves the estimation model parameters for each group individually, and used standard error obtained from bootstrapping as the form of input for a parametric test. The next approach was introduced by Chin (1998), which is a distribution-free data permutation test (Chin & Dibbern 2010). This approach is used as the distributional assumptions from the parametric approach do not function with the distribution-free character of the PLS path modelling. The distribution-free data permutation aims to scale the observed differences between the different groups through a comparison of the data found between the randomly chosen groups.

For the third approach, Henseler (2007) proposed a nonparametric procedure that directly compares group-specific bootstrap estimates from the bootstrap samples (Henseler et al. 2009). This approach is a non-parametric significance test that measures the differences of specific results from the groups that that builds on PLS-SEM bootstrapping results. The fourth approach is the Partial Least Squares Multi-Group Analysis (PLS-MGA), which extends upon the Henseler original nonparametric MGA method. This approach is a non-parametric significance measure based on the difference of group-specific results that builds on PLS-SEM bootstrapping results. The result is significant at the 5% level of error probability, when the p-value is lower than the level of 0.05 or larger than of 0.95 for specific differences in group-specific path coefficients (Henseler et al. 2009). Generally, the multi-group analysis enables the researcher the possibility of examination for predefined data groups that have significant differences in their specific parameter estimates, such as outer weights, outer loadings and path coefficients. Moreover, PLS provides outcomes of the aforementioned approaches, which are based on the bootstrapping results from each group (Hair et al. 2017).

This research used the PLS-MGA, as part of the methods to compare two data groups. The PLS-MGA approach provides a comparison of the bootstrap estimate from a particular group against all the other bootstrap estimates of same parameter in different groups (Henseler et al. 2009; Hair et al. 2017). By counting the number of occurrences where the first group bootstrap estimate is larger than those of the second, the approach produces a probability value for a one-tailed test. Specifically, PLS-MGA involves various comparisons of bootstrap estimates, such

as 25,000,000 comparisons for each parameter in a case of 5,000 bootstrap samples, and reliably tests for group differences. Simultaneously, the tests are directed towards the function of a one-sided hypothesis testing.

An assessment of model variables was undertaken with demographic variables by adhering to the following steps: firstly, the sample was split into specific smaller groups (subsample); and subsequently the independent variable(s)' path-relationships are regressed with dependent variable(s) that use one subsample at a time. Each model was considered to be acceptable in term of goodness of fit, which include: validity (discriminant and convergent); reliability (Cronbach α and composite reliability); and explanatory power in dependent variable ($R^2$). Then, bootstrapping is applied in order to re-sample the data that will obtain the structural paths standard errors in subsamples that are under consideration. Finally, for the significance of t-test, the path estimator differences are tested.

The PLS-MGA requires a sufficient sample size in order to ensure reliable results (Henseler et al. 2009; Hair et al. 2017). Therefore, there are only few comparisons among different demographical groups that are able to be conducted in this research. Following the data collection, the definitions for certain groups were provided based on demographic variables, as this helped to obtain considerable size samples, which included: organisation type, gender, country and background education in IT. The sample sizes for industry, size of organisation (number of employees in the organisation), age groups, years of experiences and different job level groups, were not sufficiently large enough and equal in group for a PLS-MGA to be performed.

Before conducting the PLS-MGA analysis, the researcher evaluated a reliability and validity assessment for the items in each group. As recommended by Wong (2013), the results demonstrated that the indicators' reliability met the threshold level of a minimum of 0.4; while the composite reliability values are in excess of 0.7 (Hair et al. 2016). The discriminant validity test demonstrated that discriminant validity existed, as AVE's square root for the latent variables was larger than the latent variables' correlation (Hair et al. 2017). The multi-group analysis examined the statistical significance of the comparable sub-samples' path coefficients. The different sub-samples' path coefficients have enabled the possibility to view the alternative paths, and to determine whether there is a difference in path direction. The PLS-MGA results show that three differences are able to be identified for the relationships that exist in regard to

security culture between job satisfaction, risk analysis and assessment, ethical conduct, security policy and security education and training.

#### *8.6.5.1 Organisation Type*

The nature of the variable organisation type was categorical and comprised three categories: public (n=113), private (n=139) and semi-public (n=14). As there was a lower number of respondents from the semi-public, the sample was split into public and private. The differences between the subsamples of the public and private organisations calculated. The standardised estimation path values of the connections between the overall sample and the two subsamples were determined. Table 8.27 provides the standardised estimation path values of relations in two subsample models and overall sample. It can also be determined that a statistically significant difference in the relationship between Job Satisfaction (JS) and Security Culture (ISC) exists among employees who are not part of the same organisation type (β diff=-0.21, p=0.01). There was a positive relationship and high significance between Job Satisfaction and Security Culture (β=0.20, t=3.18) in the public organisation group; with a nonsignificant (β=-0.01, t=0.25) level for the private organisation group. The relationship is noticeably stronger for respondents who work in a public organisation, which implies that job satisfaction is better able to predict security culture levels. Therefore, job satisfaction is a vital determinant of security culture effectiveness for public organisation employees, although remains less relevant in private organisations.

**Table 8.27: Differences of Organisation Type in PLS-MGA and Path Coefficients**

| | **Private vs Public** | | **Private** | | | **Public** | | |
|---|---|---|---|---|---|---|---|---|
| **Path** | **diff** | **p-Value** | **β** | **t-Value** | **p-Value** | **β** | **t-Value** | **p-Value** |
| Agr -> ISC | 0.05 | 0.533 | 0.135 | 2.559 | 0.011 | 0.085 | 1.457 | 0.146 |
| Con -> ISC | 0.04 | 0.569 | 0.096 | 1.74 | 0.082 | 0.055 | 1.182 | 0.238 |
| EC -> ISC | -0.052 | 0.602 | 0.117 | 1.63 | 0.104 | 0.169 | 2.488 | 0.013 |
| Ext -> ISC | 0.149 | 0.28 | 0.068 | 1.402 | 0.162 | -0.081 | 0.726 | 0.468 |
| **JS -> ISC** | **-0.214** | **0.01** | **-0.014** | **0.25** | **0.803** | **0.2** | **3.184** | **0.002** |
| Neu -> ISC | -0.116 | 0.255 | -0.111 | 1.357 | 0.175 | 0.004 | 0.083 | 0.934 |
| Ope -> ISC | 0.028 | 0.698 | 0.101 | 2.273 | 0.023 | 0.073 | 1.35 | 0.178 |
| RA -> ISC | 0.077 | 0.469 | 0.291 | 4.218 | 0 | 0.214 | 2.642 | 0.009 |
| SET -> ISC | 0.059 | 0.557 | 0.175 | 2.617 | 0.009 | 0.116 | 1.569 | 0.117 |
| SP -> ISC | -0.077 | 0.402 | 0.082 | 1.382 | 0.168 | 0.158 | 2.162 | 0.031 |
| TM -> ISC | 0.126 | 0.176 | 0.277 | 4.7 | 0 | 0.152 | 2.097 | 0.036 |

Notes: β: Path coefficient, t: t-value, p: p-value; * p < 0.5

### *8.6.5.2 Gender*

The gender variable has one category to represent the females (n=147,) and second category for males (n=112). After the observation of test values, it was determined that one significant difference between the gender groups related to the relationship between Security Culture (ISC) and Risk Analysis and Assessment (RA) (β diff= -0.26, p=0.004). The results presented in Table 8.28. The path from Risk Analysis and Assessment to Security Culture for male respondents shows a significant positivity (β=0.37, t=4.96); although insignificant positivity and moderate effects for the female group (β=0.113, t=1.98). Men can therefore be shown to be more concerned with risk analysis when evaluating an information security culture.

**Table 8.28: Differences of Gender in PLS-MGA and Path Coefficients**

| | **Female vs Male** | | **Female** | | | **Male** | | |
|---|---|---|---|---|---|---|---|---|
| **Path** | **diff** | **p-Value** | **β** | **t-Value** | **p-Value** | **β** | **t-Value** | **p-Value** |
| Agr -> ISC | 0.098 | 0.213 | 0.189 | 3.537 | 0 | 0.091 | 1.538 | 0.125 |
| Con -> ISC | 0.035 | 0.629 | 0.084 | 1.791 | 0.074 | 0.05 | 0.931 | 0.352 |
| EC -> ISC | -0.073 | 0.453 | 0.164 | 2.289 | 0.023 | 0.237 | 3.564 | 0 |
| Ext -> ISC | 0.076 | 0.342 | 0.054 | 1.087 | 0.277 | -0.022 | 0.337 | 0.736 |
| JS -> ISC | -0.025 | 0.75 | 0.084 | 1.729 | 0.084 | 0.109 | 1.729 | 0.085 |
| Neu -> ISC | 0.228 | 0.008 | 0.117 | 1.465 | 0.144 | -0.111 | 2.12 | 0.034 |
| Ope -> ISC | 0.021 | 0.787 | 0.074 | 1.309 | 0.191 | 0.053 | 1.047 | 0.296 |
| **RA -> ISC** | **-0.265** | **0.004** | **0.113** | **1.886** | **0.06** | **0.378** | **4.964** | **0** |
| SET -> ISC | 0.171 | 0.085 | 0.208 | 3.331 | 0.001 | 0.037 | 0.48 | 0.632 |
| SP -> ISC | 0.093 | 0.306 | 0.154 | 2.497 | 0.013 | 0.061 | 0.893 | 0.372 |
| TM -> ISC | -0.023 | 0.803 | 0.198 | 3.239 | 0.001 | 0.22 | 3.508 | 0 |

Notes: β: Path coefficient, t: t-value, p: p-value; * p < 0.5

### *8.6.5.3 Country*

The nature of country variable was categorical. The country variable included a lower number of respondents from different countries, as this research only examined the difference between two specific countries: Saudi Arabia (n=84) and United Kingdom (n=89). Three effect path coefficient differences were revealed through these comparisons, which show the comparison estimate differences, and also provide the results of multi-group comparisons as presented in Table 8.29. The first difference was taken in regard to path Ethical Conduct (EC) and Security Culture (ISC) (β diff=-0.21, p=0.04). In the United Kingdom group, the path was moderate positively significant (β=0.161, t=2.10), whereas in Saudi Arabia it was not significant (β=0.14, t=1.79). Therefore, it can be determined that the sample creates a positive impact upon

information security culture. The second path between the Security Education (SET) and Security Culture (ISC) functioned in different ways across the two groups (β diff=-0.28, p=0.01). For the United Kingdom group, the structural dimension's effect was shown to be moderate positive significant (β=0.180, t=2.25), whereas in Saudi Arabia group it was non-significant (β=0.151, t=1.76). As a result, the security education and training can be seen to connect positively with an information security culture in United Kingdom group.

Another difference path was found between Security Policy (SP) and Security Culture (ISC) (β diff= -0.15, p=0.04). The path presents a high level of positive significance (β=0.20, t=2.68) from the United Kingdom respondents; while in relation to Saudi Arabia respondents, there was a non-significant positive and weak effect (β=0.044, t=0.518). The relationship is shown to be positive and significant for those who live in the United Kingdom group, in relation to the security policy, ethical conduct, security education and training and security culture, which indicates that these are important predictors of information security culture for those in the United Kingdom. The gender balance in both countries was reviewed in order to make sure that there is no conflict that relates to gender differences. With 37 male respondents and 51 female respondents from United Kingdom and 32 male respondents and 50 female respondents from Saudi Arabia, it can be assumed that these gaps are indeed valid.

**Table 8.29: Differences of Country in PLS-MGA and Path Coefficients**

| | **SA vs UK** | | **SA** | | | **UK** | | |
|---|---|---|---|---|---|---|---|---|
| **Path** | **diff** | **p-Value** | **β** | **t-Value** | **p-Value** | **β** | **t-Value** | **p-Value** |
| Agr -> ISC | -0.053 | 0.589 | 0.129 | 1.82 | 0.069 | 0.182 | 2.672 | 0.008 |
| Con -> ISC | -0.015 | 0.888 | 0.038 | 0.455 | 0.65 | 0.053 | 0.696 | 0.487 |
| **EC -> ISC** | **-0.21** | **0.04** | **0.14** | **1.794** | **0.073** | **0.161** | **2.105** | **0.036** |
| Ext -> ISC | 0.014 | 0.945 | 0.088 | 1.289 | 0.198 | 0.074 | 0.887 | 0.376 |
| JS -> ISC | -0.051 | 0.607 | 0.045 | 0.558 | 0.577 | 0.096 | 1.553 | 0.121 |
| Neu -> ISC | -0.013 | 0.894 | -0.099 | 1.261 | 0.208 | -0.086 | 1.002 | 0.317 |
| Ope -> ISC | 0.024 | 0.794 | 0.077 | 1.163 | 0.245 | 0.053 | 0.855 | 0.393 |
| RA -> ISC | 0.061 | 0.604 | 0.329 | 3.889 | 0 | 0.268 | 3.093 | 0.002 |
| **SET -> ISC** | **-0.28** | **0.01** | **0.151** | **1.76** | **0.079** | **0.18** | **2.257** | **0.024** |
| **SP -> ISC** | **-0.158** | **0.04** | **0.044** | **0.518** | **0.605** | **0.203** | **2.685** | **0.007** |
| TM -> ISC | 0.122 | 0.24 | 0.253 | 3.175 | 0.002 | 0.131 | 1.964 | 0.05 |

Notes: β: Path coefficient, t: t-value, p: p-value; * $p < 0.5$

### *8.6.5.4 Background Education in IT*

The background education in IT variable was measured with a two-point scale of "yes" and "no" in this research. The background education in IT variable has also been categorical. The first category was for "yes" in regard to IT education background (n=100); and the second category was for "no" and non-IT education background (n=166). The results showed that there were no statistically significant differences between the two group of with or without background education in IT, which indicates that background education in IT is not effectual, as shown in Table 8.30.

**Table 8.30: Difference of Background Education in IT in PLS-MGA and Path Coefficients**

| | **Background Education IT (Yes vs No)** | | **No** | | | **Yes** | | |
|---|---|---|---|---|---|---|---|---|
| **Path** | **diff** | **p-Value** | **β** | **t-Value** | **p-Value** | **β** | **t-Value** | **p-Value** |
| Agr -> ISC | 0.064 | 0.460 | 0.099 | 2.089 | 0.037 | 0.163 | 2.249 | 0.025 |
| Con -> ISC | -0.138 | 0.106 | 0.121 | 3.06 | 0.002 | -0.017 | 0.225 | 0.822 |
| EC -> ISC | -0.138 | 0.199 | 0.241 | 4.28 | 0.000 | 0.103 | 1.122 | 0.263 |
| Ext -> ISC | 0.031 | 0.723 | 0.027 | 0.496 | 0.620 | 0.058 | 0.799 | 0.424 |
| JS -> ISC | -0.017 | 0.854 | 0.104 | 2.263 | 0.024 | 0.088 | 1.272 | 0.204 |
| Neu -> ISC | -0.03 | 0.72 | -0.075 | 1.227 | 0.221 | -0.105 | 1.259 | 0.209 |
| Ope -> ISC | 0.072 | 0.351 | 0.055 | 1.42 | 0.156 | 0.126 | 1.887 | 0.06 |
| RA -> ISC | 0.09 | 0.400 | 0.207 | 3.334 | 0.001 | 0.297 | 3.362 | 0.001 |
| SET -> ISC | -0.067 | 0.482 | 0.134 | 2.057 | 0.040 | 0.067 | 0.90 | 0.369 |
| SP -> ISC | 0.037 | 0.716 | 0.096 | 1.698 | 0.090 | 0.133 | 1.424 | 0.155 |
| TM -> ISC | -0.029 | 0.781 | 0.234 | 4.500 | 0.000 | 0.205 | 2.256 | 0.024 |

Notes: β = Path coefficient, t = t-value, p = p-value; * $p < 0.5$

## 8.7 Conclusion

The current research developed ISCFF that was used in the implementation of valid information security culture which include factors that are imperative in the establishment or measurements of information security culture. One of the main objectives of this research was the assessment and validation of ISCFF, which was achieved with the use of Structural Equation Modelling (SEM) technique that gathered data from practical situations. The quantitative study has the goal of validating the framework factors and testing the hypotheses

and potential relationships among the factors influential on information security culture and those that constitute the culture of information security. The specific framework of information security culture was tested in an empirical study that evaluated the levels of validity and reliability, which helped to address the objective of research.

The data analysis has been presented in this chapter, which has focused on the full investigation and results for the research framework. The analysis through quantitative data was evaluated comprehensively, which included a questionnaire that ascertained quantitative data and findings from the individual employees. This helped to measure their attitudes, opinions and perceptions in regard to the information security culture in their organisations. There was a total of 266 respondents who took part in the questionnaire and came from a variety of organisations and several countries. An analysis of questionnaires was conducted in order to validate the research framework and to determine the relevant factors that positively affect and improve the level of organisational security culture.

In the first part of this chapter, a pre-analysis of the data was screened before the statistical analyses, in order to increase the levels of data accuracy as collected from the Web-based questionnaire. This data screening included an evaluation of missing data, multivariate normality, multivariate outliers and common method bias. It was subsequently determined that the data screen demonstrated no missing data, as the participants had completed the full survey. The data screening helped to determine a distribution level without extreme outliers, which was deemed to be ‘normal’. The P-P plot, along with the findings of skewness and kurtosis showed that the data were classified as normal at both univariate and multivariate level. The z-scores and 5% trimmed mean process demonstrated that the sets of data were negatively unaffected by the external outliers. Additionally, no outliers were shown to be present through the computed Mahalanobis Distance (*D2*) values.

The Harman method and bivariate Pearson correlation were used to examine the multicollinearity assumption, which highlighted that VIF, and the effect of tolerance fell within the range of acceptability, which suggested the absence of multicollinearity. Following this, preliminary statistics were taken from the reports of descriptive statistics of demographic data, which develops a better level of comprehension of characteristics of data collected from questionnaires. It could be seen that the 266 respondents provided opinions and perspectives that produced reliable information in accordance with their organisations and employment positions within them and their levels of qualifications.

In the analysis of security knowledge statements, frequency distribution was used. The data demonstrates that the general awareness and knowledge levels average at 63.26%. Thus, additional attention is required in employees' acquisition of information security comprehension. Indeed, the security knowledge of employee is required to be improved, and particularly for targeted security education and training, and for the advancement of security awareness that will help to improve information security culture. These findings also highlighted a failure in the access to recent and relevant material regarding security policies, ethical codes and security training programmes, which can ultimately result in inadequate levels of security awareness and security compliance by employees.

Various tests were used, including the Independent Sample T-test and ANOVA, to test the differences between the demographic categories and security knowledge levels of employees. The findings show that four different demographic groups that presented no significance difference in the level of knowledge, which are: number of employees in the organisation, gender, age, and IT educational background. However, there are numerous contrasts found among six of demographic groups: organisation type, country, years' experiences, job level, induction training and security induction training. The results showed that employees from public organisations possess slightly better knowledge levels regarding information security. Similarly, years of experience made a significant different in knowledge level, with 5 to10 years' experiences marking a clear difference from those who have less than an employee with 0 to 4 years' experience. This was also true in relation to induction training, as higher knowledge levels were noted in the employees who had received it in the past. Similarly, levels of knowledge would often contrast between different countries due the different implementation strategies, standards and cultural differences between different countries.

It could be seen that the research framework variables were measured through the use of descriptive statistics, including the mean, standard error and standard deviation. It was also noted by the standard deviation and standard mean's error that the mean value could be used as a variable representative, with the sample adequately representing the population. Subsequently, the data was considered suitable input for the multivariate analyses (EFA, CFA and SEM analyses). The reliability and validity of questionnaire were evaluated. Cronbach's $\alpha$ reliability tests were used for the different constructs in order to stipulate how the items on the questionnaire were consistent with each other. There was also the scale reliability assessment, which demonstrated the different measurement scales, as used to capture the framework

constructs' meanings, reliability levels, and the high Cronbach's $\alpha$ value for the constructs. The total variables' item-total correlations were substantial, which showed that the variables sufficiently measured the base concept of model.

Survey items from previously validated scales helped in the content validity, with the construct validity determined through both convergent validity and discriminant validity. The Exploratory Factor Analyses was performed to inform a scale validity evaluation, and to group the multiple items from the same construct. EFA was used for the individual constructs, as this helped to present the relevant number of factor structures. A total of fourteen components were extracted based on Kaiser's criterion of eigenvalue (59.36% variance). The items of SET2 and JS3 were deleted during the process of EFA, as there were low-loading and cross-loading levels with other components. Factor extracted based on the EFA were also analysed through the use of a Scree plot method. As a result, the EFA provided evidence of quality measurement scales for factors that reflect and influence an information security culture, with high levels of reliability, validity and concept understanding.

The research framework assessment was performed with the use of Structural Equation Modelling (SEM) through a two-stage process. Initially, the Confirm Factor Analysis (CFA) evaluated the measurement model in order to determine the reliability, discriminant validity and convergent validity of items and constructs. Subsequently, a total of twelves items removed from agreeableness, conscientiousness, extraversion, openness and neuroticism were removed, as they had low-loading levels. The instruments of measurement framework also presented reliability and composite reliability (CR) estimates for quality indicators. Also, the findings showed that the model's constructs fitted well with the base items of measurements. The assessment results indicated that the measurement model included sufficient levels of model fit, convergent validity, and discriminant validity, with an adequate range of AVE values. It has also been suggested by the level of goodness of fit indices (GoF) that the model and data fitted at a moderate level.

The following stage was the evaluation of structural model in order to present the framework hypothetical relations. The variables' relationships strengths were analysed through the use of bootstrapping technique. The structure model produced quality level of reliability estimates, which indicated that the model supported the coefficient of determination (R2), path significance (β value), effect size (*f2*), and prediction relevance (*q2*). The nine path coefficients within the framework demonstrate present positive significant direct effects, apart from

extraversion and neuroticism were two clear paths that failed to be supported. The nine proposed relationships had $\beta$ values >0.070, with a significance at 0.05 level. The context of information security culture in general has a positive influence through security risk analysis and assessment, top management, ethical conduct, agreeableness, security policy, security education and training, job satisfaction, conscientiousness and openness. Also, there is positive correlation among the different factors, which help to support the validity levels of information security culture framework. These are consistent with the assumptions on factors that are positively influential and able to predict organisational security culture. In addition, the determination of coefficient fitting (R2) and effect size ($f2$) showed that the model and the data fitted substantially. The predicative relevance of path significance with a sample-to-population through the Stone-Geisser criterion was also satisfied.

The subsequent stage was an analysis of structure model from various forms by focusing on the demographic variables to determine whether the path coefficients' contrasts between groups are relevant statistically. Four demographic variables were evaluated as moderators between the framework's path relations: organisation type, gender, country, and background education in IT. The PLS-MGA method was used to examine the moderators' impacts. The findings highlighted that the moderators were significantly supported. However, the demographic variable of background education in IT fails to have an effect on information security culture predictions.

It was shown from the demographic characteristics' moderation effect results that job satisfaction levels are a more comprehensive way of predicting public organisational security culture and its effectiveness for employees and remains less relevant in private organisations. The findings also indicated that male employees had higher levels of concern in regard to risk analysis and assessment in information security culture evaluation comparing to female employees. The current research analysed the moderating effect in relation to two countries (the United Kingdom and Saudi Arabia), which demonstrated a clear positive correlation of security policies, ethical conduct, security education and training, and security culture with employees working in the United Kingdom. Therefore, it can be noted that these are factors are able to predict organisational security culture and relevance in the United Kingdom. The next Chapter 9 will provide the discussion of findings and results presented in this chapter.

# Chapter Nine :

# Discussion and Implications of Quantitative Results

## 9.1 Introduction

This this chapter presents and discusses the justifications for the proposed conceptual framework. In particular, the significance and insignificance of relationships between factors identified in the ISCFF. The main findings are highlighted and discussed. The findings obtained from the research hypotheses tests are compared with other research studies. Furthermore, this chapter details the findings of an examination of a moderating impact of different demographic characteristics and how these characteristics may influence organisational security culture through organisation type, gender, country and background education in IT. Finally, a summary of chapter is presented.

## 9.2 Reflecting upon The Results

This research aimed to achieve the objectives outlined in chapter 1. The main aim was assessing and validating the ISCFF using Structural Equation Modelling (SEM) using data from practical-based situations. The lack of reliability and validity in security culture measurements (see Chapter 3) prompted an exploratory survey to obtain more reliable and valid findings. The aim of quantitative phase was to provide validity to the identified factors in the framework, to test the reliability and validity of a framework and to test the hypotheses.

The exploratory survey provided information that supported the identified factors of ISCFF as found from both the literature review and interviews. The framework was used in data collection from employees. The ISCFF helped the understanding of different values, perspectives, opinions, knowledge levels and forms of practising information security. It was also possible to investigate the efforts of organisations in improving employee development in information security. Therefore, the current research was beneficial in providing details of how the framework and hypotheses could be validated.

In order to analyse the measurement factor structure in this research, factor analysis EFA, CFA and SEM techniques were used, which also provided validity to the assessment and in testing the research hypotheses. The questionnaire was adopted from previous studies, such as Alhogail (2016) and Da Veiga (2018). Therefore, it was crucially important to do an assessment of validity and reliability levels. EFA was initially conducted in order to detail the correlations among the observed variables. EFA helped to present the main factors, as well as to identify

what factors represent conceptually. The structures ascertained from the EFA helped to guide a factor structure based on empirical evidence for CFA tests.

Both CFA and SEM were conducted to confirm the existence of a specific factor structure that was derived by the EFA. In general, the findings from the measurement and structure model developed quality reliability estimates. The findings also shown that the ISCFF supported the content validity, discriminant validity, convergent validity, explanatory power of model (R2), path significance (β value), effect size (*f2*), and goodness of fit indices (GoF). Also, the influential factors upon information security culture in ISCFF framework were determined as positively predicting three different factors that reflected an information security culture in organisations. Various factors and their positive correlations added additional support to the validity of a framework, which was consistent with the previously assumptions and what can improve the organisation security culture. The SEM results presented the potential ways that researchers and security specialists are able to focus and direct information security when intending to improve an organisation's level of information security through the use of a study framework. The quantitative phase provided rich data sample of 266 employees. The data was used to develop the ISCFF by validating the identified factors.

The framework provided evidence in regard to the relevance of the establishment of organisational security culture by confirming the important factors that should be implemented and developed in organisations. The analysis confirmed the importance of identified factors in the framework for providing support for organisational security culture. The results suggested that influential factors, organisational behavioural factors and reflection factors all contribute to a beneficial level of security culture. These factors are important in improving security of information assets and information security culture levels. It was also clear from the findings that the identified factors have been confirmed as vital and effectual upon employees' security culture behaviour.

This research examined and proved the relationship between employees' job satisfaction levels and organisational security culture, and ultimately ascertained relevant and beneficial results. Innovative evidence has been provided in regard to the positive impacts that job satisfaction provides on security culture efficiency levels. The results shown that a job satisfaction plays an important role in employees' behaviour and attitudes towards information security. The results indicated that the higher job satisfaction motivates employee to comply with security policies and proper commitment to the information security culture.

The personality traits (FFM) within information security culture were examined and were proved to be effectual. This research shown that the personality traits have a significant impact in the improvement of security culture efficiency. The results indicated that an information security culture and efficiency levels are positively affected by agreeableness, conscientiousness, and openness. These three constructs could function to predict security behaviour and improve employee security awareness and security compliance in organisations by understanding employee personality characteristics. The personality traits help organisations to determine the security areas that need to be improved or implement, such as improve relevant training sessions. This research fills an important research gap and providing important new insights to present literature in relation to the ways that personality traits and information security culture connect.

In general, a comprehensive ISCFF is vital in order to enable human security factors to be taken into consideration. Influential, organisational behaviour, and constituting factors have been determined to be imperative in the development of information security culture through both the research results and previous literature. It is evident that security risk assessment and analysis, top management, ethical conduct, agreeableness, security policy, security education and training, job satisfaction, conscientiousness and openness all positively influence organisational security culture, which generally indicate security awareness, security ownership and security compliance. These particular factors have been shown to all be vital in developing effective security culture levels. It can also be seen that influential, organisation behavioural and reflecting factors interact and result in an organisational security culture to affect employees' security behaviour. Thus, security is evidently not a purely technical issue, but actively involves with employees. The findings demonstrated that the framework components help to develop safety in the environment through providing behavioural guidance and support. Also, the factor's tasks in this research could be used to advance effective security culture measures and assessment tools. The results also provided some evidence that identified factors of ISCFF are moderated by organisation type, gender, and an individual's country.

The results of this research benefit the survey research conceptual framework and how it correlates with the research hypotheses as a vital stage in the achievement of showing a clear exchange of concepts. A total of seven hypotheses formed the examination of how the identified factors and information security culture connected, as well as how the data analysis generated mixed findings with the hypotheses. All hypotheses were supported, except two sub-

hypotheses related to two factors of personality traits were unsupported. In general, the exploratory survey results of this research are consistent with previous studies, such as Alnatheer et al. (2012), Alhogail (2016) and Martins and Da Veiga (2015). The testing hypotheses findings are shown in the following sections.

## 9.3 Influential Constructs/Factors

The current research analysed how influential factors are effectual upon information security culture and its relevance, which ascertained clear positive results. This group is comprised of five hypotheses (H1 to H5), (see Table 9.1). The samples showed a strong statistical support for how information security culture is directly and moderately affected by these five factors.

**Table 9.1: Results of the Research Hypotheses**

| Research Hypothesis | | Supported |
|---|---|---|
| **H1** | Top management support has a positive influence on the effectiveness of the security culture. | Yes |
| **H2** | Security policy has a positive influence on the effectiveness of the security culture. | Yes |
| **H3** | Security education and training has a positive influence on the effectiveness of the security culture. | Yes |
| **H4** | Security risk analysis and assessment has a positive influence on the effectiveness of the security culture. | Yes |
| **H5** | Ethical conduct has a positive influence on the effectiveness of the security culture. | Yes |
| **H6** | Job satisfaction has a positive influence on the effectiveness of the security culture. | Yes |
| **H7a** | Agreeableness has a positive influence on the effectiveness of the security culture. | Yes |
| **H7b** | Conscientious has a positive influence on the effectiveness of the security culture. | Yes |
| **H7c** | Openness has a positive influence on the effectiveness of the security culture. | Yes |

| Research Hypothesis | | Supported |
|---|---|---|
| **H7d** | Extraversion has a positive influence on the effectiveness of the security culture. | No |
| **H7e** | Neuroticism has a negative influence on the effectiveness of the security culture. | No |

***- Top Management Support***

This research hypothesised that top management support has a positive influence on effectiveness of security culture. Both the literature and the semi-structure interview findings have pointed out the existence evidence of positive relationship between information security culture and top management support (D'Arcy & Greene 2009; Masrek et al. 2017; Martins & Da Veiga 2015). Top management support is capable of, developing quality security training programmes and simultaneously improve security awareness and security ownership in an organisational security culture.

The exploratory survey findings confirmed the direct relationship between top management and security culture, which support H1. The results stated how the involvement of top management positively influence the advancement of security culture. The majority of respondents clearly indicated upon the importance of top management involvement in an organisation. They indicated how senior management were dedicated to the improvement of information security culture, as well as implementing relevant security training programmes. The research findings coincided with previous studies (D'Arcy & Greene 2009; Knapp et al. 2007; Masrek et al. 2017; Martins & Da Veiga 2015). It could be concluded that the levels of commitment from top management in organisations, combined with strong leadership, function in supporting the advancement of information security culture, helps to improve long-term success levels (Nasir et al. 2018).

***- Security Policy***

It has been hypothesised that security policy is able to positively influence the effectiveness of security culture. Various research studies have shown that security policies need to be imposed as a top priority for organisations (Alnatheer et al. 2012; Alhogail 2016; Da Veiga 2016). Security policy enables security compliance to be encourages through security awareness and the implementation sufficient levels of security culture (Alhogail 2016; Da Veiga 2016).

The findings confirmed hypothesis H2 with regard to a significant correlation between security policy and information security culture. The survey data indicated that security policies function in the advancement of quality security culture, and in the implementation of security compliance policy. A security policy is necessary in the establishment of information security culture, alongside security management if it is to be effective. Security awareness requires a base of security policies in order for an organisational security culture to be succeed (Hovav & D'Arcy 2012).

It was evident from the findings that there was a lack of access to security policies. 38.73% of respondents did not know how to obtain a copy of their organisation's security policies or details of any updated material. This was consistent with the details provided in the interviews. Interviewees stated that security policies were important in the procedure of security measures, although they could be inadequate if employees are not informed correctly about existing security policies or remain unaware of the relevant content. It is possible to deduce that when an employee has a low level of policy awareness, this can often result in noncompliant behaviour. Therefore, it is important that an organisation maintains its security policy and that its development and implementation continue to function with the overall aims of organisations.

The multi-group analysis revealed that amongst country groupings (the United Kingdom and Saudi Arabia), there are significant differences, which highlighted the correlation between implemented security policy and developed information security culture. The analysis demonstrated that relationship is higher and significant for respondents living in the United Kingdom. The reason for this difference could stem from the ways that policies and strategies are implemented by different organisations between the two cultures. However, there is minimal evidence in regard to how national culture influences information security culture (Alnatheer et al. 2012; Connolly et al. 2017).

The research findings agreed with those studies Alnatheer et al. (2012), Alhogail (2016) and Da Veiga (2016), which concluded that an information security culture requires the integration of the development of culture with daily work routines, which will help to improve organisations' security environment and increase comprehension levels of employees and how they interact with information security. This will also improve organisations' adaptability levels, and thus, create consistent security policy enforcement techniques.

***- Security Education and Training***

This research hypothesised that security education and training have a positive influence on effectiveness of security culture. The literature review highlighted how security education and training programmes are the most important factors to influence information security culture. Effective security culture is the basis for the advancement of security management, which becomes impossible without implementing security education and training in organisations (Alhogail 2016; Nasir et al. 2018).

The testing results from H3 correlated with how security education and training programmes emphasise positivity upon the effectiveness levels of security culture. The findings indicated that it is necessary to conduct periodic security education and training sessions in order to support employees to achieve specific roles within the development of information security culture. As this will reduce the potential risks to information assets, and increase security awareness levels, and ultimately improve security compliance. The finding also stated that continuous security education training sessions would prove beneficial in the advancement of organisational security cultures (Da Veiga 2015; Van Niekerk & Von Solms 2005).

The findings indicated a gap on the efficiency provision of security education and training programmes in organisations. 49.63% of respondents do not know how to locate or find relevant security training programmes in their organisations. This related to a lack of comprehension and lack of knowledge. A total of 48.50% of respondents had not received any security training sessions during their time at their respective organisations. 61.65% of respondents did confirm that they believed in the benefits of security education and training sessions for improving security awareness. This correlates with the findings from the interviews, as the respondents remarked upon how periodic security training sessions are important to improve information security culture, as at present it is common for information security to only be mentioned at the start of employment.

The findings demonstrated the contrasts between Saudi Arabia and the United Kingdom in regard to the correlation between this factor and the development of information security culture. It could be seen that security education and training programmes help to create positive connections in United Kingdom organisations, which could stem from contrasting implementation strategies between the nations.

The current research findings are consistent with results found by other studies (Alhogail 2016; Da Veiga 2015; Hassan & Ismail 2012; Nasir et al. 2018). The research findings highlighted that security awareness, security education and organisational leadership must be integrated together in order to ensure the effectiveness of security culture (Martins & Da Veiga 2015; Zakaria 2004).

***- Security Risk Analysis and Assessment***

The research hypothesised the positive impact of security risk analysis and assessment on effectiveness of security culture. The literature review had shown the importance of considering security risk analysis and assessment validation in the development of information security culture. Security risk analysis and assessment support organisations to reduce losses and increase damage awareness levels among employees.

It can be seen from the results that the security risk analysis and assessment presented a positive effect on organisational security culture, which support H4. The quantitative results revealed that security risk analysis and assessment are the most relevant and effectual factor on information security culture in this research. The findings revealed that security risk assessment and analysis help in the provision of employees' comprehension levels and how they perceive security in their places of work. Subsequently, this can prove to be influential in how employees conduct themselves due to increased security understanding and awareness, which can positively affect an organisational security culture.

The multi-group moderation highlighted how a significant contrast exists between males and females in regard to the relationship between security risk analysis and information security culture. It can actually be observed that the males demonstrate higher sign of positivity when compared to females. This finding suggested that males are normally present more concern for security risk analysis and assessment when evaluating their organisational security cultures. There may be numerous reasons for these differences. But it could stem from the differences in knowledge bases and cybersecurity interests. In accordance, several studies, such as Anwar et al. (2017) and McGill and Thompson (2018) have presented contrasts between males and females in relation to their beliefs and behavioural intentions for information security. For instance, in the study by Anwar et al. (2017), employees' cybersecurity behaviours are examined with a particular focus on gender differences. It was determined that cybersecurity behaviours were different between genders and that males generally had better computer skills

and cues to action. Anwar et al. (2017) concluded that it is necessary to consider the individual differences. Anwar et al. (2017) suggested to develop gender-focused cybersecurity training and interventions, which would target relevant cybersecurity behaviour model constructs in order to develop employees' knowledge levels, their attitudes and behaviour.

The research finding is consistent with Alnatheer et al. (2012), Martins and Eloff (2002), and Nasir et al. (2018) studies. It could be seen from the research findings that the security risk analyses, and assessment are important in the establishment of organisational security culture. The security risk analysis and assessment help organisations to develop loss, damage awareness, and increase security knowledge, in order to reduce employees' misbehaviour levels, and subsequently improve the level of security culture.

- ***Ethical Conduct***

This research presented a hypothesis that ethical conduct is a positive factor upon information security culture and its utilisation. Ethical codes help to show which actions are required in an ethical manner that support employees to behave ethically in relation to information security whilst working (Da Veiga & Eloff 2010; OECD 2005).

A positive influence of ethical codes on security culture was evaluated in this research, where it was determined that there were clear positive results, as H5 had predicted. The findings indicated that an organisation's ethical conduct functions to guide employees, as they are able to clarify and define ethical actions and procedures. Ethical conduct enables employees in organisations to recognise and be aware of their security obligations, and ultimately reduce risk, and thus, develop information security culture positively.

It could be clearly noted from the survey results that there was a failing in how to access organisations' ethical codes. 45.49% of respondents did not know how they could find and access their organisations' ethical codes. Many organisations failed to correctly implement ethical conduct and codes in their practice; hence, this ultimately proved detrimental upon the development of information security culture.

The multi-group analysis helped to reveal that for the United Kingdom and Saudi Arabia, noticeable contrasts exist between them in relation to ethical codes and information security culture. The analysis demonstrated that the correlation is more positively significant for employees from the United Kingdom. The reason for this difference could be due to the fact

that there are different ethical and policy standards between the United Kingdom and Saudi Arabia; this commonly occurs between different countries (Alnatheer et al. 2012; Dojkovski et al. 2007).

The research findings supported previous studies to conclude that organisations require to develop ethical codes and notify members about it. Codes of ethical conduct were shown to be a main base for organisational security culture development because this helps to support and improve employee behaviour and organisations' acceptance criteria (Martins & Eloff 2002; OECD 2005).

## 9.4 Organisational Behaviour Construct/Factors

Several studies have determined that there are other security factors affect people behaviour and understanding these may assist in improving the security of information assets in organisations (Greene & D'Arcy 2010; McCormac et al. 2017). It has been established that these factors are beneficial and that their contributions occur across many areas of workplace behaviour, which include individuals adhering to organisations policies and rules (D'Arcy & Greene 2014). Numerous studies, such as D'Arcy and Greene (2009) and McCormac et al. (2017) have evaluated whether job satisfaction and personality traits are beneficial to the development of information security. Accordingly, this research followed on from recent literature by evaluating how job satisfaction impacts upon information security culture, as well as analysing the effect of five personality traits of: agreeableness, conscientiousness, openness, extraversion and neuroticism on the information security culture. Organisational behavioural constructs were hypothesised, which investigated (H6 and H7a-e) in order to evaluate whether there are a significant positive influence from the organisational behavioural factors on the levels of security culture effectiveness (see Table 9.1). The survey analysis demonstrated that there was significant positive result of direct effects from both factors upon the overall information security culture.

- ***Job Satisfaction***

This research hypothesised that job satisfaction has a positive influence on the effectiveness of information security culture. Previous studies have noted the significance of considering job satisfaction to motivate employees to comply with security protocol and establish an acceptable

level of security culture in an organisation. Job satisfaction it able to motivate the behaviour of employees in order to comply with the requirements of security.

The findings confirmed H6 with marked significant correlations between job satisfaction and information security culture. The survey results shown that individuals who report positivity and satisfaction in their jobs commonly comply with the security requirements of an organisation, as their improved engagement enables group interaction and collective responsibilities. A higher job satisfaction levels help to develop an increased tendency for security behaviour conformity. Thus, organisations comprise of more satisfied employees, who are willing to fulfil their job responsibilities and commit to information security culture.

The findings demonstrated the differences among organisational types in relation to the correlation between employees' job satisfaction levels and information security culture. The multi-group analysis proved that this correlation is significantly positive in respondents working in the public sector, when compared to the private sector. The relationship is noticeably stronger between job satisfaction levels and information security culture in the public sector, which implied better possibilities to predict the levels of information security culture. Job satisfaction is imperative towards the effective development of information security culture in the public sector, whilst contrastingly it is lower in the private sector. This could be due to the fact that employment conditions and colleague relationships differ between the two sectors within organisations.

Therefore, it can be determined that employees' attitudes toward their job and the organisations that they work for often contrast, which can affect how they adapt and work with security procedures and regulations (Markovits et al. 2010). Several studies have shown evidence of differences in both the public and private sectors related to the relationship between job satisfaction levels and commitment to the organisation (Aldhuwaihi 2013; Agarwal & Sajid 2017; Wang et al. 2012). These studies have confirmed that job satisfaction levels help in the predication of employees' effective commitment in public organisations, in comparison to private ones. Accordingly, when job satisfaction levels increase, which often occurs more in public organisations, employees start to present more beneficial toward their organisations and the overall security of the organisation (Markovits et al. 2010; Wang et al. 2012).

The research result supported previous studies and concluded that job satisfaction is an imperative factor upon the advancement of individuals' behaviour and their active compliance

with information security procedures and requirements in organisations (Farokhi et al. 2016; Greene & D'Arcy 2010). It can be determined from this research findings that that higher job satisfaction levels help to motivate employees in their compliance with their organisation security policies, whilst simultaneously advancing employees' security awareness and security ownership, in order to implement security relevance and continuation.

- ***Personality Traits***

This research examined and analysed how the main five personality traits effect the development of information security culture. The personality traits potentially support in improving security awareness and information asset in organisations (Gabriel & Furnell 2011). The quantitative results indicated that three personality traits have a significant influential on information security culture levels. The results from a survey indicated that information security culture and efficiency levels are positively affected by agreeableness, conscientiousness, and openness. The research findings concurred with previous studies, such as Pattinson et al. (2015) and Mcbride et al. (2012). It can be concluded that conscientiousness, agreeableness, openness, and ability to control impulsivity explained variance in information security behaviour. It can also be determined from the research findings that information security behaviour is improved, following an evaluation of employees' personality differences.

- ***Agreeableness***

It was hypothesised in this research that agreeableness has a positive influence on the effectiveness of security culture. An individual's agreeableness has been deemed to have a positive connection with increased levels of organisational safety (Cellar et al. 2001). This research findings have determined that agreeableness positively impacts on an organisational security culture, and thus, supports H7a. The results shown that employees who present with high levels of agreeableness commonly exercise more concerned with security issues, have more acute levels of security awareness and compliance with security policy, which generally results in more compliant behaviour, and consequently, develops an organisational security culture. The research findings coincidence with Mcbride et al. (2012), McCormac et al. (2017) and Shropshire et al. (2015) studies. It can be deduced that agreeable employees are influential upon positive information security cultures.

- ***Conscientiousness***

This research hypothesised that conscientious has a positive influence on the effectiveness of security culture. Employees who are conscientious present a greater impact on a security compliance with information policy (Shropshire et al. 2006; Mcbride et al. 2012). The research results indicated how conscientiousness positively affects information security culture and its maintenance, which supported H7b. The findings indicated that conscientiousness in employees develops a higher level of security awareness, with commonly resulting in exercising greater levels of care in an organisation and maintaining their organisational security cultures. This findings coincidences with McCormac et al. (2017) study. Therefore, conscientiousness in an individual positively influence the information security culture.

- ***Openness***

It was hypothesised that openness has a positive influence on the effectiveness of security culture. Individuals with openness are generally more adept at overcoming challenges through critical thinking. The survey results determined that when employees have higher openness levels, there is a significant positive influence on information security culture, as H7c stated. The research findings supported previous studies, such as McBride et al. (2012). It can be concluded that increased levels of openness increase security awareness and security compliance that establish an effective security culture in organisations.

- ***Extraversion and Neuroticism***

This research hypothesised that extraversion and neuroticism have a positive influence on the effectiveness of security culture. The quantitative findings shown that extraversion and neuroticism were not found to be significant influential on information security culture; thus, not providing support to H7d and H7e. The research findings consistent with Pattinson et al. (2015) and McCormac et al. (2017). It had shown that extraversion and neuroticism did not significantly correlate with self-reported behaviour and security awareness. It can be determined that extraversion and neuroticism are not significantly effectual on information security culture.

The main contribution from this research findings relate to personality traits impact on the effectiveness of information security culture. The research findings helped to fill an important gap and presented new evidence to existing literature in regard to the relationship between

personality traits and information security culture. From the perspective of application, personality traits are able to assist organisations in noting potential necessary developments, which can improve and maintain security training programmes for employees. These programmes could then be personalised in a way that matches the personality profile of individual and their own style of learning, in order to increase the level of learning outcomes. Therefore, this research provided an opportunity to better comprehend individual differences regarding information security culture, which is imperative to information security culture advancement in organisations.

## 9.5 The Constituting Constructs/Factors

Various studies, such as Alnatheer et al. (2012), have reflected on the necessity to differentiate between the factors that constitute information security culture in organisations, and those which affect it. This helps organisations in their development of implementing better human interaction form employees towards information security; and thus, advancing the level of information asset protection. Unfortunately, there is currently limitation in regard to the number of studies that help to determine factors that reflect information security culture (Alnatheer et al. 2012; Walton 2015). Due to a clear gap in the existing literature in determining what constitutes an information security culture in regard to the identification of vital factors required for its development, the current research focused on information security culture are correlated to security awareness, security ownership, and security compliance.

The survey instrument provided confirmation of three factors of information security culture that comprise security awareness, security ownership, and security compliance. The results of survey analysis demonstrated that these three factors have positive and significant correlations to information security culture. The survey analysis also shown that the three first-order constructs directly connect to a second-order. This helped to justify a definition of information security culture as a second-order construct. Overall, security ownership had the highest level of path coefficients, and subsequently, it can be determined that this has a stronger correlation to information security culture. Following security ownership, security compliance, and then security awareness. This research determined that these three key factors of information security culture strongly correlate with each other.

These findings correspond with the evidence provided by Alnatheer et al. (2012), who stated that, an information security culture is a reflection of security awareness, security ownership, and security compliance.

- ***Security Ownership***

The research findings shown that security ownership benefits the development of information security culture. Through the provision of responsibility, and the advancement of information security protection in an organisation, employees begin to comprehend the security risks that occur as consequential of their own actions. Employees should understand their own roles and clearly learn their responsibilities within an organisation. This helps to develop their security awareness and increase compliance levels with security policy, which consequently leads to improvements in information security culture (Alhogail & Mirza 2014; Alnatheer et al. 2012; Walton 2015).

- ***Security Compliance***

The results determined that security compliance helped in benefiting the progression of an organisational security culture. The findings from the survey provided evidence of how it is imperative to develop security compliance during the stage of information security culture implementation, and to improve the organisation's overall level of security. This will increase the levels of understanding of how information security culture is influential upon behaviour and compliance with security procedures and regulations. The research findings supported other studies findings, such as Da Veiga and Eloff (2010) and Masrek et al. (2017). When employees comply with security measures, it results in organisational security culture improvement, and the number of security breaches are able to be reduced.

- ***Security Awareness***

The research findings produced evidence of important connections between security awareness and information security culture. The security awareness is one of the main challenges that organisations face when attempting to achieve sufficient security levels. Both security education programmes and security policy commonly encourage compliance through the augmentation of employees' security awareness levels. When there is an increase in security policy awareness, security compliance occurs more frequently; hence, better information security culture progression. The research findings consisted with previous studies, such as Da

Veiga (2015), Parsons et al. (2017) and Wiley et al. (2020). It can be concluded that in order to create more conducive security culture environments, there is a requirement for improving security awareness

Based on the research findings, strong correlations were presented between information security culture and the reflection factors (security awareness, security ownership and security compliance). These three factors strongly connect to information security culture as factors to comprise its development. When employees working in organisations presenting high levels of information security awareness, and better levels of responsibility and ownership in the protection of information security, subsequently this helps to follow an organisation's security policy, and then develop an improved information security culture. Specifically, this research helped to confirm that the information security culture is a reflection of security awareness, security ownership and security compliance. Overall, the current research added a contribution to other studies in the provision of better understanding and to present clarity distinction between factors that constituting information security culture and which factors influencing an organisational security culture.

The ISCFF has helped to confirm the most significant factors that are required to improve the security levels of information assets and how to measure information security culture in organisations. The correlation between the components of factors that prove influential upon information security culture, organisational behavioural factors and factors that constitute information security culture had been tested statistically in order to provide the validity levels of ISCFF and how it influences organisational security culture. The findings provided evidence to support the framework and hypotheses. The findings indicated that all correlations between factors influencing information security culture and factors constituting information security culture were shown to have positive effects, apart from extraversion and neuroticism. Similarly, a developed information security culture also influences upon certain constructs, as highlighted by Alhogail (2016), Martins and Da Veiga (2015) and Nasir et al. (2018). Therefore, the relationship among numerous factors helped in the development of an organisational security culture, with employees exhibiting certain behaviours that form their organisational security culture, which is a direct result of the different factors that influence employees' interaction levels.

An example is provided in the following sections in order to demonstrate how these factors correlate with each other, starting with security policy. Security policy attempts to direct the

behaviour of employees in their protection of information assets, and to control which people are able to gain access through a process of monitoring. Each organisation should have a written security policy and guidelines that focus on the goals of the organisation. Security policies are often modified or updated periodically in an organisation. For example, the company ABC updated its security policies. One of the updated security policies states that a password must be kept and used in secret at all times. Security policy will impact and correlate with a variety of factors. First, top managers need to make sure that employees know about updated security policies through the company's communication systems, which can include training session in order to advance security policy understanding.

Employees should be educated and alerted about the updated security policy, security risk analysis and perceive dangers that could prove detrimental if the security policy is not adhered to. This also will help employees to develop their comprehension of security policy and understand their responsibilities toward updated security policy. Hence, employees will respect new security policies and behave in an ethical manner. Likewise, it is vital that all managers and employees in leadership positions should show the adherence to all the set security policies in order to send a clear message of support towards security's relevance and set examples to the other employees. Accordingly, this will help to improve a company security level through increased employee compliance, as the general quality of life within the company begins to improve. Therefore, ABC company increases its levels of employee satisfaction, and how willing an employee is to fulfil their job responsibilities.

In addition, ABC company needs to use a personality trait (i.e., Big Five Factor Model (FFM)) as a way to understand and measure employees' personalities. This will assist in the predictions of various factors that prove effectual upon information security compliance levels. This will help in the advancement of employees' security education and training programmes that are designed to connect with the employees' personality profile and learning styles, in order to increase the specific learning outcomes. Employees will also become aware of the updated security policies, and their responsibilities towards it. Additionally, employees will gain a better level of ownership and responsibility due to the increase in their security knowledge and skills levels, which will subsequently increase security compliance behaviour in the company, and thus, advance the information security culture.

The information security culture is significantly impactful upon the presented factors. For example, a security policy becomes ineffective when employees are unaware of the relevance

of its importance, which might result in detriment to the organisation's information assets. Through the implementation of a beneficial security culture, an employee's level of security awareness, security ownership and security compliance will be changed. As educating employees in relation to security policies and their relevance helps to increase security awareness levels and the belief that information security-related policies are the employees' responsibilities on a daily basis. Hence, employees start to comply more frequently with their organisation's security policy, which ultimately demonstrates that these factors and their interaction help to develop information security culture. This results in higher levels of responsibility regarding information security, which provides a base to implement effective innovative security systems in organisations. As employees start to adapt their behaviour more frequently, which helps to preserve organisations' information security levels.

## 9.6 Conclusion

One of a main goal of the current research has been to assess and validate the research framework. This objective was achieved through using Structural Equation Modelling (SEM). SEM has helped in the process of acquiring practical situation data. The ISCFF was tested in Chapter 8, which provided an evaluation of how valid and reliable it was deemed to be. This ultimately assisted in addressing the research main objectives, which enabled the current chapter to present a discussion of findings from the survey and a discussion of previously analysed structural model. Accordingly, the survey produced relevant information which helped to support the identified factors as shown from both the current research's literature review and conducted interviews. This research helped to provide evidence of the way to validate the research framework and hypotheses.

The main findings shown that the identified factors are important to the advancement of framework in order to develop organisational security culture. It has become clear that the research factors continue to be significant to the ISCFF and help to improve employees' behaviour in relation to information security culture. Also, it can be determined that the research findings provide evidence to prior research in regard to the benefits impact of increased job satisfaction levels upon the effectiveness of security culture. This research analysed the effect of the personality traits on developing an organisational security culture. This research filled an important research gap and added new evidence to existing literature of the significant relationship between personality traits and information security culture.

Generally, the context of information security culture has a positive influence through security risk analysis and assessment, top management, ethical conduct, agreeableness, security policy, security education and training, job satisfaction, conscientiousness and openness. The information security culture is a reflection of three specific factors: security awareness, security ownership and security compliance. In this research, these factors have been confirmed its importance in the improvement of organisational security culture. Also, there is positive relationship between various factors, which help to support the validity levels of information security culture and key factors framework, which correspond with the theoretical assumptions that these factors are positive in nature and can potentially predict the specific information security culture of different organisations.

The demographic characteristics' moderation has been shown to affect job satisfaction levels. It a clearer evidential that job satisfaction levels are a more comprehensive way of predicting an information security culture levels of public organisations and to measure how effective it is for employees, although it remains less relevant in private organisations. The research findings demonstrated that male employees, when compared to females, specifically expressed increased levels of concern regarding their organisations' risk analysis and assessment in evaluating information security culture. This research also provided analysis of the moderating effects regarding different nations of United Kingdom and Saudi Arabia. In particular in relation to employees working in the United Kingdom, there was evidential positivity in the correlation between security policies, ethical conduct, security education and training development and the provision of information security culture. Subsequently, it is evident that these particular concepts help in the prediction of information security culture and relevance in the United Kingdom.

After the research framework's analysis and assessment and seven hypotheses tested, it can be determined that it is necessary to advance a research framework based on relevant hypotheses and by removing the non-supported hypotheses. Therefore, it can be deduced that the three factors of security awareness, security ownership and security compliance correlate with information security culture, as well as the influential factors: top management, security policy, security education and training, security risk analysis and assessment, ethical conduct, job satisfaction and personality traits. Nevertheless, two constructs of personality traits of extraversion and neuroticism were removed, as they failed to support the hypotheses.

In general, the empirical study was beneficial to validate the research framework. It showed that the framework was valid and reliable. This also helped in validating the significance level of each component defined in the framework and seven supported hypotheses. The ISCFF has presented a comprehensive base for organisations to increase and improve better security cultures, which will help in the protection of information assets. It has also been determined that framework components are able to develop a safe work setting that can provide guidance and support in the advancement of security culture in organisations.

Organisations will be able to improve their employees' behaviour through the implementation of the ISCFF and be able to analyse and improve how they interact with information assets and data. Subsequently, it will be possible to augment security benefits and work against potential threats that employees can pose. This can reduce employees' threats to information security, as guidance will improve their behaviour and change their own values, perceptions, and opinions, as based on the ISCFF. Furthermore, this will assist in the development of necessary security education and train programmes to raise security awareness levels and improve the security knowledge of employees.

# Chapter Ten :

# Conclusions and Future Work

## 10.1 Introduction

The purpose of this chapter is to present a conclusion, and a summary of the research that has been performed during the study. Initially, a general overview of the research study is presented. Then, the conclusions are detailed, including the main contributions addressed and the research goals that have been accomplished. Next, the main limitations of the research are also outlined. Finally, future research recommendations, and various suggestions for possible future information security culture development are presented.

## 10.2 General Overview of Research

The management and development of information security relates to the people, processes and technology involved. In general, the technology involved is objective in design, whilst the people and processes are contrastingly affected by the environment setting where they operate. Human behaviour also affects people and processes, which can subsequently influence information security management. Various studies, such as Alhogail (2016), Connolly et al. (2017) and Da Veiga and Eloff (2010) stated that the human dimension within the advancement of information security produces the weakest link in its development. Therefore, the progression of information security culture is vital for organisations to increase the levels of effectiveness in information security management (Martins & Martins 2016; Walton 2015).

The information security culture normally has the goal of implementing the necessary beliefs, values, and knowledge levels that can result in desirable behaviour traits, which protect information assets against internal threats. There are few security culture models available, which comprehensively improve organisational security culture. There are limited studies that have identified the factors that influence or affect the information security culture. Nevertheless, the available studies show that no mutual agreement is present in regard to these factors. There is also a lack of models to guide and integrate the necessary main factors in developing an efficient information security culture. There are relevant efficient factors have not been determined or analysed in information security culture, such as personality traits and job satisfaction. These two factors have been shown to motivate better employee behaviour toward the implementation and advancement of information security.

Due to this lack of comprehensive models, the current researcher proposed a comprehensive, reliable and valid framework. The conceptual framework components were inspired by

different relevant frameworks, such as Alnatheer et al. (2012) model. The ISCFF of this research aimed to identify and combine the important human factors that help to improve security culture efficiency levels. It was also vital to comprehend the influential factors upon organisational security culture, which include the base understanding of correlation between these factors and those reflect information security culture. The ISCFF helped to better understand the information security culture and the different elements that are able to reinforce the information security culture.

The ISCFF was confirmed through using a mixed methods approach of data collection. The first phase was a qualitative design in order to signify and confirm the importance of the identified factors in ISCFF. Semi-structure interviews with thirteen experienced and knowledgeable IT professionals and experts were conducted in an exploratory manner, as they presented their opinions and relevant feedback regarding the identified factors and understanding of framework. The second phase was quantitative data for an exploratory survey was conducted to validate the framework applicability and test research hypotheses through a description and explanation of organisational security culture. Quantitative different techniques were also conducted, particularly Exploratory Factor Analysis (EFA), Confirmatory Factor Analysis (CFA), and Structural Equation Modelling (SEM), which were based on the questionnaire's obtained data. These techniques helped to demonstrate the levels of validity and applicability of ISCFF.

Many respondents had written notes that indicated their own curiosity in the current research findings, as they understood the necessity to advance the information security culture in their organisations and to improve security practices. Correspondingly, it is important that effective security culture cultivation includes a model pre-assessment, as this will help to determine the strengths and weaknesses, and thus, minimise additional required efforts, reduce expenditure and ensure focusing on the desired issues.

The current research contributed to existing literature on the topic of information security culture development, and provided a comprehension, validity, and reliability as a framework. This research provided a base comprehension of factor correlation in regard to the influences upon information security culture and the factors that reflect it. The ISCFF is able to direct both organisations and individual professionals in developing effective information security culture that reduce the potential threats to information security by those working inside companies. Also, the research fulfilled the requirement for additional empirical studies that

have focused on information security culture cultivation. Accordingly, the presented framework would help to improve the performance of any organisation's employees, as it provides a guide and relevant support for their behaviour, advancing their values and assumptions following key initial assessments. The present framework is able to be used as the base to develop an instrument to measure organisational security culture assessments, as it functions as a comprehensive framework to define relevant items in information security culture. Further, the framework practicality is supported in this research to be the best guideline, which is based on the framework that can be used by security specialists as a reference point in the development of a better security culture.

## 10.3 The Achievements and Contributions from the Research

The main aim of the current research had been to design and develop a comprehensive Information Security Culture and key Factors Framework (ISCFF), which is reliable and valid in order to develop an effective security culture. ISCFF will help organisations to understand the main human factors that require consideration in order to develop and help employees to intuitively protect information assets and data in their organisations. Therefore, the primary objective was originally divided into sub-goals, as presented in Chapter 1. Accordingly, the research had contributed to the field of information security culture development and the research objectives, which have been able to realise the following achievements:

1. **To explore and evaluate the conceptualisation of information security culture and the importance of implementation in an organisation.**

2. **To present a summary of previous studies aimed at establishing and managing information security culture and various factors that could influence the effectiveness of information security culture and the behaviour of employees.**

In order to address aims 1 and 2, an extensive literature review was undertaken based on the cultivation of information security culture. This provided a clear overview of research field, potential models, used methodologies, and to demonstrate the areas that require additional research and the gap in knowledge that this research is aims to fill. A summary was presented in Chapter 3 and Appendix A of previous research studies that had the goal of developing and maintaining the information security culture in organisations. The literature review also concluded that the majority of information security culture issues relate to the identification of

security culture concepts and factors that are affect by or result in information security culture; or to the development of information security culture; or as an assessment of information security culture that helps to measure whether it is sufficient.

The comprehensive review of literature also demonstrated that there are different important factors, have an influence on the information security culture, which should be considered in order to have an effective security culture in organisations. This research reviewed a total of fourteen research perspectives that showed essential knowledge in regard to the identification of factors that assist in information security culture establishment and development. It was revealed that the most available models and frameworks were concerned with the conceptualisation of security culture. These available models lacked a comprehensive view that integrated the human aspects in order to provide organisations with an all-inclusive framework that would help practitioners and organisation to create and assess their information security culture. These currently used models also lacked guidance in relation to their effectiveness by practitioners as a way of cultivating and improving the information security culture. Therefore, a more comprehensive practical framework is clearly required in order to cultivate and maintain information security culture. Chapter 3 presented a review and conclusion of the models, as were published in (Tolah et al. 2017).

3. **To identify the critical success factors that have a direct influence or constitute information security culture components.**

4. **To understand the relevance of these identified factors and their relationship with each other in order to inform the design of an information security culture framework.**

In order to address aims 3 and 4, it was necessary to conduct a comprehensive review of recent studies on information security culture, and exploratory qualitative interviews with thirteen experienced and knowledgeable security specialists from seven organisations. The semi-structure interview helped to determine which information security culture factors were relevant, and what influences information security culture initiation and improvement. This research had helped to highlight and conceptualise the main factors that are beneficial in the creation of information security culture. The semi-structure interview findings confirmed the importance of the identified factors and demonstrated the comparisons between factors in this research. Based on the outcome of literature review and interview findings, the main impactful

factors on information security culture effectiveness were: top management support; security policy; security education and training programmes; security awareness; security ownership; security risk assessment and analysis; ethical conduct and security compliance. Additionally, this research had the goal to reduce the confusion of factors that constitute information security culture. This research conducted a literature analysis and an exploratory interview aimed to identify and confirm the elements that can reflect information security culture, which was shown to constitute a three-factor reflection: security awareness, security ownership, and security compliance.

This research also demonstrated the provision of comprehending the correlation among factors that influence information security culture and those that reflect the information security culture. Correspondingly, this research developed ISCFF that was designed to better understand the relationship among these factors and determine how they influence the information security culture. ISCFF developed a clearer overview of how to implement and improve organisational security culture, which helped to improve information security culture understanding amongst employees and practitioners of information security. The discussion and conclusion were presented in Chapters 3 and 6 and published in Tolah et al. (2017; 2019).

5. **To identify any other security factors that could have a direct influence on the information security culture.**

The research comprehensive review shown that the understanding of influential factors remains limited. There are factors that are widely investigated and examined in organisational behaviour studies, which are able to motivate employees toward improving information security and awareness levels. Unfortunately, these particular factors have not been deeply considered in previous studies that have focused on information security culture, which include the personality traits and job satisfaction. No previous studies have tested the correlation between the information security culture and employees' personality traits. Nonetheless, the qualitative interviews highlighted the benefit of understanding job satisfaction and its contribution to the information security culture and improving the security of information assets in organisations. Therefore, this research confirmed the importance and benefits of these factors on security culture effectiveness. This research added new evidence to existing literature on the positive influence of job satisfaction on the effectiveness level of information security culture. Also, it filled an important research gap and added new evidence to existing literature reviews on the significant relationship between personality traits and information

security culture. This review and conclusion were discussed in Chapters 3, 6, 8 and published in Tolah et al. (2017; 2019).

6. **To develop a comprehensive framework that integrates all important factors that can be used for the implementation of an effective information security culture.**

It can clearly be determined by previous studies from the literature review that more inclusive investigation into the security culture was necessary in order to provide comprehensive framework and present best practices when establishing information security culture. The current research had proposed a comprehensive Information Security Culture and key Factors Framework (ISCFF) that combines the most important human factors that could potentially help in the development of security measures to avoid insider threats in organisations. In accordance, the ISCFF helps to develop an understanding of information security culture, and of elements that can reinforce organisational security culture. ISCFF helped to determine whether the level of security culture enhances the security of information assets and helped in the process of assessing the correlations between factors that influence information security culture and factors that constitute information security culture. When the influential factors or reflection factors are understood, it becomes possible to help in improving employee interaction with information security. The ISCFF can be used by researchers and organisations as a starting point to understand how to create and assess an information security culture. The framework provides management with the means to implement an appropriate information security management approach. Management approaches include, providing guides and the implementation of controls in understanding the importance of factors involved, for the cultivation and measurement of information security culture. The developed ISCFF was presented in Chapter 5 and published in Tolah et al. (2017; 2019).

7. **To assess the validity of the proposed information security culture framework through a structural equation modelling (SEM) technique by gathering data from a real-world situation.**

In order to achieve this aim, and to prove the framework validity and applicability in its ability to create and assess information security culture, the ISCFF was tested by conducting an exploratory survey with a sample size of 266 respondents. An assessment was implemented based on the ISCFF, which was influenced by previous security culture assessment models, such as Alhogail (2016) and Da Veiga (2018). The ISCFF was used in the data collection from

respondents in regard to their values, beliefs, perceptions, knowledge and practices of information security. To accomplish this objective, SEM techniques were implemented to provide results validity to the assessment and test the original research hypotheses. Overall, the measurement and structure model instruments produced quality reliability estimates. It was also shown that a framework supported the content validity, discriminant validity, convergent validity, explanatory power of model (R2), path significance (β value), effect size (*f2*), prediction relevance (*q2)* and Goodness of Fit Indices (GFI). The factors that influenced information security culture were determined to be able to positively predict the factors that reflecting the information security culture in organisations. Also, positive correlations between factors that provided additional support to ISCFF validity were ascertained in regard to how they influence the information security culture.

Following the analysis of research framework and research tested hypotheses, it has been determined that ISCFF redesign is required based on the supporting hypotheses and the removal of non-supported hypotheses. Therefore, it can be deduced that the identified factors that constitute information security culture (security awareness, security ownership and security compliance) and influential factors (top management, security policy, security education and training, security risk analysis and assessment, ethical conduct, job satisfaction and personality traits (which include agreeableness, conscientiousness, openness)) are the most important factors and considered as part of information security culture conceptualisation. However, two personality trait constructs were removed as they had non-supported hypotheses: extraversion and neuroticism (see Chapter 8 for the results). In general, this research was beneficial in providing the framework validation and for the hypothesis. The findings demonstrated that the framework components develop a safe environment that is able to guide behaviour and provide vital support in order to accomplish it. Hence, it could be beneficial for organisations to use ISCFF when improving and maintaining their information security culture. This research had helped to provide a beneficial structure and guidance that can reduce the threats to information assets, as posed by employees' behaviour.

## 10.4 Implications

There are two implications: research implication and practice implication for this research.

### 10.4.1 Research Implication

It is imperative that important factors are assessed in order to comprehend their influence on information security culture. Therefore, the current research developed an Information Security Culture and key Factors Framework (ISCFF) that would increase the understanding of organisational security culture development and enhancement. The main benefit of this research was in the provision of ISCFF that was valid and reliable, which also helped in the assessment of correlation between factors that constitute and influence information security culture. The research implications are presented in the subsequent points:

1. This research had identified present gaps in research into information security culture field, which included the identification of additionally required empirical research regarding the topic; and the examination of information security culture in organisations from different settings and backgrounds, such as Asian societies. Therefore, this research helped to fill a major gap in the area of information security culture, which includes the incorporation of an Information Security Culture and key Factors Framework (ISCFF) with validity and reliability, which could be used and replicated in a variety of environments.

2. The research framework provides a reference point for a wide range of empirical studies, which are able to be conducted to further test the model and can be undertaken in several contexts or environments. This ISCFF can be used as a point of guidance for additional empirical research on the information security culture area. Similarly, the constructs within the information security culture can be used as dependent variables for different research studies. This helps to gain better insight into the factors that are beneficial to organisational security culture; thus, increasing managerial understanding of how information security culture can be enhanced and maintained.

3. In regard to a methodological perspective, this research presented two significant contributions to information system security development. It highlighted that a mixed-method design for research (qualitative and quantitative) can be conducted in studies attempting to better understand information security. Specifically, this research provided exploratory interviews which confirmed the identified factors to improve the ISCFF. This research shown that interviews were valuable when exploring potential insights, and in the development of correlation between constructs. The second major

contribution of the research was achieved through the quantitative assessment, which helped to validate the ISCFF. Also, the exploratory survey assisted in the exploration of the correlation between the framework constructs, which include the factors that are influential upon information security culture and those that constitute the information security culture. The two used methodologies in this research assisted in the potential to conduct further empirical studies on information security culture. In general, the contributions from this research promote the utilisation of a mixed-method approach in the investigation into the information security culture and to enhance the potential to replicate the research in similar contexts.

### 10.4.2 Practical Implications

A quantitative assessment was presented in the current research, which security managers and practitioners can use as a measuring technique for their organisational security culture and to develop an information security culture. The research instruments were created academic rigour and tested through various stages with empirical data. The ISCFF was statistically tested in order to note whether it was valid and reliable. This was undertaken with 266 respondents from different organisations comprising different industries, types, sizes and roles. Overall, the research framework offered numerous observations that can helps to develop guidance structures for managers, and to improve information security culture. Consequently, the practical implications are as follows:

1. The current research helps security managers and organisations in the development of important information security concepts that are able to develop information security culture enhancement. The ISCFF provides the management with the means to implement improved management techniques for information security, which provides a single point of reference to understand how sufficient security culture levels can be achieved and maintained. This includes the provision of guidance to managers to better comprehend how they can personally contribute to the advancement of security culture, as they can enforce and communicate security policies.

2. The current research has helped to reduce the potential threats from the behaviour of employees pose to the protection of information assets. As a result, the ISCFF helps to increase information security culture understanding and to better determine the elements that are able to improve the information security culture. When the

information security culture reflection factors are understood, (which include security awareness, security compliance and ownership of security), management is able to assist in improving how employees interact with information security, which will increase the levels of information asset protection.

## 10.5 Research Limitations

Due to the scope and breadth of the current topic on information security culture, there are a number of research limitations that had to be considered, as the following points show:

1. Even though the sample for the analysis presented a balanced gender distribution and the respondents worked in different types of organisation with different size companies, the majority lived in the United Kingdom or Saudi Arabia, whilst other nations were not represented accurately. Hence, there was potential limited bias, as most participants originated from only two countries. As a result, this could restrict the generalisability of findings to other organisations, as all organisations present with their own distinct forms of human-related security challenges. Information security management issues for organisations are complex and require a great level of comprehension of combined organisational dynamics, different risks, and industry sectors and classification. Thus, the current research was tested to avoid any values and beliefs bias that are specific to the culture being studied.

2. The original aim was to include approximately 350 responses obtained through online questionnaires; however, this was challenging to achieve. The general access to employees and organisations from which the data could be gathered was an issue, as certain people and organisations were not willing to participate in the research. Organisations were sometimes reluctant to share security-related information for the study, which resulted in a low response rate. The final respondent figure was 266, even though in excess of 600 were sent out via direct emails, and posting survey on an online website (https://www.callforparticipants.com). Nevertheless, a representative sample of organisations was achieved. Also, the obtained responses still confirmed the data analysis technique's (SEM) requirements, although a higher rate would have been able to provide a clearer understanding and a higher level of validity to the findings.

3. The method of non-probability convenience sampling method limited the level of representativeness and generalisability for the research findings (Nadler et al. 2015). The selection of this particular technique generally stems from resource and time limitations when contacting potential respondents. Nevertheless, the obtained responses still ascertained the data analysis technique's (SEM) requirements, although a higher rate would have been able to provide a clearer understanding and a higher level of validity to the findings.

4. The current research was based on a single cross-sectional design. The data were collected in a single period, which means that potential change analysis was not possible. The organisations' absorptive capacities or business models were based on a longitudinal perspective. Even though this single cross-sectional process enabled the researcher to collect a significant data sample in a short span of time without the need for extended use of time (Bordens & Abbott 2007). It was not possible to understand the main predictors fully in respect to the time when the intentions and common behaviour traits regarding information security culture were accepted.

5. Most of the survey items were derived from the literature review, qualitative interviews and expert reports, as there was a lack of prior survey instruments that could be used for the current research. Consequently, the process for item selection was not fully objective, although the literature review, interviews and expert reports did reduce the subjectivity levels. There was also initially a pilot of survey instrument in order to improve the validity of construct, as the original lack of prior instruments resulted in challenges to the construct operations.

## 10.6 Future Research and Recommendation

The current research achieved the main objectives of this research and was able to implement a comprehensive information security culture and key factors framework. This framework would assist organisations in the development and maintenance of quality security culture that would protect organisations' information from internal threats. Nevertheless, this has specific limitations for various areas of future research that will attempt to improve upon the current findings, which relate to the following:

1. Problems related to the sample size, which resulted in only minimal responses. Additional future research with larger sample sizes is important, in order to increase the statistical relevance and evidence, and to improve the scope of findings from the current research. Also, additional research needs to be conducted with probability sampling in order to increase statistical inference.

2. Additional studies in the future should be able to enhance the current findings and increase levels of security culture comprehension from different perspective, which include determining the factors that may constitute or influence information security culture in another environment. For instance, it could be beneficial to conduct replica study in a different environment in order to conduct framework testing; this could include different demographics or nationalities. Findings from studies such as these should be able to improve the level of security culture research in regard to the environmental factors that might affect information security culture and result in an increase to the way that international standards are applied. Moreover, in order to produce more domain-specific practices, dedicated studies could be conducted to investigate the ISCFF in chosen sectors (i.e., health or finance organisations). Additional research is imperative in the process of improving data collection among various countries, as this will help to establish the research framework generalisability and increase the comprehension levels for the findings.

3. It would be beneficial for conducting a longitudinal study to collect data from different points of time, as this would provide a better understanding of topic of information security culture. Therefore, future studies need to implement a panel data collection that enables change analysis for cultural behaviour, and for the absorptive capacity of organisations and how this affects long-term business model innovation.

4. Structured Equation Modelling (SEM) can be used to develop additional analysis of the nature of correlations between the framework's variables and collecting additional data from various case studies or focus groups. This will assist in gathering rich contextual data in relation to possibilities of developing information security culture.

## 10.7 The Future for Information Security Culture

Information security can be problematic and challenging for organisations, as it is digitally structured and has constant connectivity. The format of information security is based on humans and the different information security strategies need to focus on human factors. Accordingly, it has become generally accepted that increasing security culture levels means instilling security behaviour in those that interact with ICTs, which is vital in the maintenance of the security information position (Karyda 2017). Improving levels of information security culture in organisations has been the aim of several studies in the recent years, as both organisations and countries aim to improve the mind-set of individuals in regard to information security and improving its culture. In general, an organisational security culture is deemed to be the way that individuals act with information security, which should result in the protection of information assets, improvement in security understanding, attitudes and values that help to determine their individual behaviour. However, empirical evidence of information security culture is currently not comprehensive, and comprises of merely descriptive, theoretical, and philosophical approaches (Karlsson et al. 2014; Nasir et al. 2018). Thus, organisational security culture and its impact upon organisations have not been analysed in detail.

Therefore, this research was conducted in order to respond to the need for more empirical research studies that have focus on the development of security culture measures. The ISCFF was implemented in order to achieve the research objectives, which comprised of factors that influence information security culture and those that constitute information security culture. The ISCFF derived from a literature review and the qualitative findings. Subsequently, the ISCFF was assessed and improved through the use of quantitative technique. The quantitative technique helped to provide a valid and reliable framework, and improved understanding of the correlation between factors that influence information security culture and factors that reflect information security culture. Also, this research provided practical security culture implications for organisations by offering a framework that is able to explain and provide valuable information regarding this topic. The model's potential is to function as a framework for organisations in order to improve the cultivation of information security culture.

The questionnaire in this research could be improved in order to develop an automated security culture assessment tool, which would improve the statistical analysis model and data mining models. The survey could potentially include multiple versions in future studies, such as

develop a specific survey for management, information security officers, IT staff or non-IT staff members, in order to achieve innovative recommendations. The ISCFF could be developed if it were initially implemented in an organisation, in order to ascertain a clear analysis of its function, and subsequently provide potential recommendations for the organisational security culture. Additionally, the framework could be used in the evaluation of acceptable security culture levels based on the activity of the organisation. Hence, it is vital to develop an acceptable security culture levels with no matter what the business activity is. Nonetheless, the applied efforts should not be equal between different organisations, as the levels of sensitive information contrast between organisations.

As human behaviour and knowledge correlate together, it is imperative that research regarding this topic focuses on the security knowledge that organisations require, in order to develop their information security culture. The management of knowledge that is able to capture, acquire and encode knowledge to help decision making can assist to improve a framework, which helps organisations to efficiently develop their information security culture and provide predictions of how it will advance. The process of sharing knowledge among organisations assists in the efficiency of working with security incidents caused by employees. The most beneficial security research and practice guidelines require additional investigations in order to recommend practical standards that performance indicators and indexes could improve through the development of effective security culture in relation to different groups and organisations. These indicators need to measure the actual security culture level, which includes: an assessment, evaluation, planning, implementation, and the provision of the criteria.

# References

1. Agarwal, P. and Sajid, S.M., 2017. A study of job satisfaction, organizational commitment and turnover intention among public and private sector employees. *Journal of Management Research*, *17*(3), pp.123-136.

2. Aguinis, H., Edwards, J.R. and Bradley, K.J., 2017. Improving our understanding of moderation and mediation in strategic management research. *Organizational Research Methods*, *20*(4), pp.665-685.

3. Anwar, M., He, W., Ash, I., Yuan, X., Li, L. and Xu, L., 2017. Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, *69*, pp.437-443.

4. Albrechtsen, E. and Hovden, J., 2010. Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers & Security*, *29*(4), pp.432-445.

5. Aldhuwaihi, A., 2013. The influence of organisational culture on job satisfaction, organisational commitment and turnover intention: a study on the banking sector in the Kingdom of Saudi Arabia. PhD Thesis, Victoria University.

6. Alfawaz, S. and Nelson, K, Mohannak, K., 2010. Information security culture: A Behaviour Compliance Conceptual Framework. *Proceedings of the 8th Australasian Information Security Conference (AISC 2010)*, pp.47–55.

7. Alhogail, A., 2015. Design and validation of information security culture framework. *Computers in Human Behavior*, 49, pp.567–575.

8. Alhoagail, A., 2016. A Framework for the Analysis and Implementation of an Effective Information Security Culture Based on Key Human Factor Elements and Change Management Principles. PhD Thesis, King Saud University.

9. Alhogail, A. and Mirza, A., 2014. Information security culture: a definition and a literature review. In *2014 World Congress on Computer Applications and Information Systems (WCCAIS)* (pp. 1-7). IEEE.

10. Alnatheer, M., Chan, T. and Nelson, K., 2012. Understanding and Measuring Information Security Culture. In *PACIS* (p.144).

11. Alreck, P.L. and Settle, R.B., 1995. *The survey research handbook: Guidelines and strategies for conducting a survey*. Chicago: Irwin.

12. Ary, D., Jacobs, L. C., and Razavieh, A., 2002. *Introduction to Research in Education*. Belmont: Thomson Learning.

13. Alvesson, M. and Berg, P.O., 1992. Corporate culture and symbolism: An overview.

14. Ang, S., Van Dyne, L. and Begley, T.M., 2003. The employment relationships of foreign workers versus local employees: A field study of organizational justice, job satisfaction, performance, and OCB. *Journal of Organizational Behavior*, *24*(5), pp.561-583.

15. Arthur Jr, W. and Graziano, W.G., 1996. The five-factor model, conscientiousness, and driving accident involvement. *Journal of personality*, *64*(3), pp.593-618.

16. Ashenden, D., 2009. Information Security management: A human challenge? *Information security technical report*, *13*(4), pp.195-201.

17. Ashenden, D., 2018. In their own words: employee attitudes towards information security. *Information & Computer Security*.

18. Atkinson, P.E., 1997. *Creating Culture Change: Strategies for Success*. Rushmere Wynne Limited.

19. Babbie, E.R., 2012. *The practice of social research*. Thomas Wadsworth.

20. Backhaus, K., Erichson, B., Plinke, W. and Weiber, R., 2016. *Multivariate analysemethoden*. Springer.

21. Baggett, W.O., 2003. Creating a culture of security: The OECD standards for systems security provide internal auditors with a tool for operationalizing tone at the top. *Internal Auditor*, *60*(3), pp.37-41.

22. Bagozzi, R.P. and Fornell, C., 1982. Theoretical concepts, measurements, and meaning. *A second generation of multivariate analysis*, *2*(2), pp.5-23.

23. Bagozzi, R.P. and Yi, Y., 1988. On the evaluation of structural equation models. *Journal of the academy of marketing science*, *16*(1), pp.74-94.

24. Bagozzi, R.P., Yi, Y. and Phillips, L.W., 1991. Assessing construct validity in organizational research. *Administrative science quarterly*, pp.421-458.

25. Baker, W.H. and Wallace, L., 2007. Is information security under control? Investigating quality in information security management. *IEEE Security & Privacy*, *5*(1).

26. Bakry, S.H., 2004. Development of e-government: a STOPE view. *International Journal of Network Management*, *14*(5), pp.339-350.

27. Bandura, A., 1999. Social cognitive theory: An agentic perspective. *Asian journal of social psychology*, *2*(1), pp.21-41.

28. Baron, R.M. and Kenny, D.A., 1986. The moderator–mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. *Journal of personality and social psychology*, *51*(6), p.1173.

29. Bansal, G., 2011. Security concerns in the nomological network of trust and big 5: first order vs. second order.

*30.* Bartlett, M.S., 1954. A note on the multiplying factors for various $\chi$ 2 approximations. *Journal of the Royal Statistical Society*, pp.296-298.

31. Barlow, J.B., Warkentin, M., Ormond, D. and Dennis, A.R., 2013. Don't make excuses! Discouraging neutralization to reduce IT policy violation. *Computers & security*, *39*, pp.145-159.

32. Barrick, M.R., Mount, M.K. and Judge, T.A., 2001. Personality and performance at the beginning of the new millennium: What do we know and where do we go next? *International Journal of Selection and assessment*, *9*(1-2), pp.9-30.

33. Beach, L.R., 1993. *Making the right decision: Organizational culture, vision, and planning.* Prentice Hall.

34. Beautement, A., Sasse, M.A. and Wonham, M., 2008. The compliance budget: managing security behaviour in organisations. In *Proceedings of the 2008 New Security Paradigms Workshop* (pp. 47-58).

35. Bell, A.J., Rogers, M.B. and Pearce, J.M., 2019. The insider threat: Behavioral indicators and factors influencing likelihood of intervention. *International Journal of Critical Infrastructure Protection*, *24*, pp.166-176.

36. Bélanger, F. and Crossler, R.E., 2011. Privacy in the digital age: a review of information privacy research in information systems. *MIS quarterly*, pp.1017-1041.

37. Benbasat, I. and Zmud, R.W., 1999. Empirical research in information systems: the practice of relevance. *MIS quarterly*, pp.3-16.

38. Berg, B.L., 2004. Methods for the social sciences. *Qualitative Research Methods for the Social Sciences.* Pearson Education.

39. Berry, L.M. and Houston, J.P., 1993. *Psychology at work: An introduction to industrial and organizational psychology*. Brown & Benchmark/Wm. C. Brown Publ.

40. Bess, D.A., 2012. Understanding Information Security Culture in An Organization: An Interpretive case study. PhD Thesis, Nova Southeastern University.

41. Blaikie, N. and Priest, J., 2019. *Designing social research: The logic of anticipation.* John Wiley & Sons.

42. Blacharski, D., 1998. *Network Security in a Mixed Environment with Cdrom*. IDG Books Worldwide, Inc.

43. Black, T.R., 1999. *Doing quantitative research in the social sciences: An integrated approach to research design, measurement and statistics*. Sage.

44. Blakley, B., McDermott, E. and Geer, D., 2001, September. Information security is information risk management. In *Proceedings of the 2001 workshop on New security paradigms* (pp. 97-104).

45. Boone, H.N. and Boone, D.A., 2012. Analysing Likert data. *Journal of extension*, *50*(2), pp.1-5.

46. Bordens, K.S. and Abbott, B.B., 2007. *Research design and methods: A process approach*. Mountain View, Mayfield.

47. Bornman, W.G. and Labuschagne, L., 2004, June. A comparative framework for evaluating information security risk management methods. In *Information Security South Africa Conference* (Vol. 4, pp. 13-23).

48. Box, D. and Pottas, D., 2013. Improving information security behaviour in the healthcare context. *Procedia Technology*, *9*, pp.1093-1103.

49. Brady, J.W., 2010. An investigation of factors that affect HIPAA security compliance in academic medical centers. PhD Thesis, Nova Southeastern University.

50. Bresz, F.P., 2004. People—often the weakest link in security, but one of the best places to start. *Journal of health care compliance*, *6*(4), pp.57-60.

*51.* Brewerton, P. and Millward, L., 2002. *Organizational Research Methods: A Guide for Students and Researchers.* Sage

52. Briggs, A.R., 2012. Academic writing. *Research Methods in Educational Leadership and Management.* Sage, pp.397-412.

53. British Standards Institute., 1999. *Information Security Management- BS 7799-1:1999*. London: BSI.

54. Bryman, A., 2015. *Social research methods*. Oxford university press.

55. Bryman, A. and Bell, E., 2015. *Business research methods*. Oxford university press.

56. Bulgurcu, B., Cavusoglu, H. and Benbasat, I., 2010. Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly*, pp.523-548.

57. Byrne, B.M., 2010. *Structural equation modeling with AMOS Basic concepts, applications, and programming*. Multivariate Applications Series.

58. Caelli, W. and Longley, D., 1989. *Information security for managers*. Springer.

59. Caldwell, T., 2014. The quantified self: a threat to enterprise security? *Computer Fraud & Security*, *2014*(11), pp.16-20.

60. Campbell, D.T. and Fiske, D.W., 1959. Convergent and discriminant validation by the multitrait-multimethod matrix. *Psychological bulletin*, *56*(2), p.81.

61. Cavana, R.Y., Delahaye, B.L. and Sekaran, U., 2001. *Applied business research: Qualitative and quantitative methods*. John Wiley & Sons.

62. Cazemier, J.A., Overbeek, P. and Peters, L., 2010. *Information Security Management with ITIL*. Van Haren.

63. Cellar, D.F., Nelson, Z.C., Yorke, C.M. and Bauer, C., 2001. The five-factor model and safety in the workplace: Investigating the relationships between personality and accident involvement. *Journal of Prevention & Intervention in the community*, *22*(1), pp.43-52.

64. CERT, 2013. 2013 US State of Cybercrime Survey: How Bad is the Insider Threat? Available at: http://resources.sei.cmu.edu/asset_files/Presentation/2013_017_101_58739.pdf

65. CERT, 2014. 2014 U.S. State of Cybercrime Survey. Available at: http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=298318.

66. Chan, H. and Mubarak, S., 2012. Significance of information security awareness in the higher education sector. *International Journal of Computer Applications*, *60*(10).

67. Chang, S. and Lin, C.S., 2007. Exploring organizational culture for information security management. *Industrial Management & Data Systems*, *107*(3), pp.438-458.

68. Chang, S. and Ho, C.B., 2006. Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems*, *106*(3), pp.345-361.

69. Chaula, J.A., A Socio-Technical Analysis of Information Systems Security Assurance: A case study for effective assurance. PhD Thesis, Stockholm University

70. Chen, Y., Ramamurthy, K. and Wen, K., 2015. Impacts of Comprehensive Information Security Programs on Information Security Culture. *The Journal of Computer*

*Information Systems*, 55(3), p.11.

71. Chia, P.A., Maynard, S.B. and Ruighaver, A.B., 2002. Understanding organizational security culture. *Proceedings of PACIS2002. Japan*.

72. Chin, W.W., 1998. The partial least squares approach to structural equation modeling. *Modern methods for business research*, *295*(2), pp.295-336.

73. Chin, W.W., 2010. *How to write up and report PLS analyses*. Springer.

74. Chin, W.W. and Dibbern, J., 2010. An introduction to a permutation-based procedure for multi-group PLS analysis: Results of tests of differences on simulated data and a cross cultural analysis of the sourcing of information system services between Germany and the USA. In *Handbook of partial least squares* (pp. 171-193). Springer.

75. Chin, W.W. and Todd, P.A., 1995. On the use, usefulness, and ease of use of structural equation modeling in MIS research: a note of caution. *MIS quarterly*, pp.237-246.

76. Chin, W.W., Marcolin, B.L. and Newsted, P.R., 2003. A Partial Least Squares Latent Variable Modeling Approach for Measuring Interaction Effects: Results from a Monte Carlo Simulation Study and an Electronic-Mail Emotion/Adoption Study. *Information Systems Research*, *14*(2), pp.189-217.

77. COBIT, 2004. Security Baseline – An Information Security Survival kit IT Governance Institute, USA.

78. Colwill, C., 2009. Human factors in information security: The insider threat–Who can you trust these days? *Information security technical report*, *14*(4), pp.186-196.

79. Comrey, A.L. and Lee, H.B., 1992. Interpretation and application of factor analytic results. *Comrey AL, Lee HB. A first course in factor analysis*, *2*, p.1992.

80. Connolly, L. and Lang, M., 2012, December. Investigation of cultural aspects within information systems security research. In *2012 International Conference for Internet Technology and Secured Transactions* (pp. 105-111). IEEE.

81. Connolly, L. and Lang, M., 2013. Information Systems Security: The Role of Cultural Aspects in Organizational Settings. *Proceedings of the Eighth Pre-ICIS Workshop on Information Security and Privacy*, pp.1–15.

82. Connolly, L., Lang, M. and Tygar, J.D., 2015, May. Investigation of employee security behaviour: A grounded theory approach. In *IFIP International Information Security and Privacy Conference* (pp. 283-296). Springer, Cham.

83. Connolly, L.Y., Lang, M., Gathegi, J. and Tygar, D.J., 2017. Organisational culture, procedural countermeasures, and employee security behaviour. *Information & Computer Security*.

84. Connolly, L.Y., Lang, M. and Wall, D.S., 2019. Information Security Behavior: A Cross-Cultural Comparison of Irish and US Employees. *Information Systems Management*, *36*(4), pp.306-322.

85. Cohen, J., 2013. *Statistical power analysis for the behavioral sciences*. Academic press.

86. Cohen, J., Cohen, P., West, S.G. and Aiken, L.S., 2013. *Applied multiple regression/correlation analysis for the behavioral sciences*. Routledge.

87. Cohen, L., Manion, L. and Morrison, K., 2013. *Research methods in education*. Routledge.

88. Cordeiro, C., Machás, A. and Neves, M.M., 2010. A case study of a customer satisfaction problem: Bootstrap and imputation techniques. In *Handbook of partial least squares* (pp. 279-287). Springer.

89. Cronbach, L. J., 1971. Test Validation. *Educational Measurement*.

90. Costa Jr, P.T. and McCrae, R.R., 1992. Reply to eysenck. *Personality and individual differences*, *13*(8), pp.861-865.

91. Creswell, J.W., 2002. *Educational research: Planning, conducting, and evaluating quantitative* (pp. 146-166). Prentice Hall.

92. Creswell, J.W., 2008. The selection of a research design. *Research Design-Qualitative, Quantitative, and Mixed Method Approaches*-, pp.3-22.

93. CSI, 2008. CSI computer crime and security survey. Available at: http://www.sis.pitt.edu/jjoshi/courses/IS2150/Fall11/CSIsurvey2008.pdf

94. CPNI, "SeCuRE: Security Culture Review and Evaluation Tool," Crown, 2014. Available: http://www.cpni.gov.uk/Documents/Publications/2014/2014-02-20-secure_tool_guide_for_organisations.pdf.

95. Cybersecurity Insiders, 2019. Insider Threat Report. Available at: https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/insider-threat-report.pdf

96. D'Arcy, J. and Greene, G., 2009. The multifaceted nature of security culture and its influence on end user behavior. In *Proceedings of IFIP TC 8 International Workshop on Information Systems Security Research*.

97. D'Arcy, J. and Greene, G., 2014. Security culture and the employment relationship as drivers of employees' security compliance. *Information Management & Computer Security*, *22*(5), pp.474-489.

98. D'Arcy, J. and Hovav, A., 2007. Towards a best fit between organizational security countermeasures and information systems misuse behaviors. *Journal of Information System Security*, *3*(2), pp.3-30.

99. Da Veiga, A., 2008. Cultivating and assessing information security culture. PhD thesis, University of Pretoria.

100. Da Veiga, A., 2015. An Information Security Training and Awareness Approach (ISTAAP) to Instil an Information Security-Positive Culture. *Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance*. In *HAISA* (pp. 95-107).

101. Da Veiga, A., 2016. Comparing the information security culture of employees who had read the information security policy and those who had not. *Information & Computer Security*.

102. Da Veiga, A., 2018. An approach to information security culture change combining ADKAR and the ISCA questionnaire to aid transition to the desired culture. *Information & Computer Security*.

103. Da Veiga, A. and Eloff, J.H., 2010. A framework and assessment instrument for information security culture. *Computers & Security*, *29*(2), pp.196-207.

104. Da Veiga, A. & Martins, N., 2015. Information security culture and information protection culture: A validated assessment instrument. *Computer Law & Security Review*, 31(2), pp.243–256.

105. Da Veiga, A., Martins, N. and Eloff, J.H.P., 2007. Information security culture-validation of an assessment instrument. *Southern African Business Review*, *11*(1), pp.147-166.

106. Deal, T.E. and Kennedy, A.A., 1982. *Organization Cultures: The Rites and Rituals of Organization Life.* Addison Wesley.

107. Denning, D.E., 1999. *Information warfare and security*. Addison Wesley.

108. Denscombe, M., 2014. *The good research guide: for small-scale social research projects*. McGraw-Hill Education.

109. Detert, J.R., Schroeder, R.G. and Mauriel, J.J., 2000. A Framework for Linking Culture and Improvement Initiatives in Organizations. *Academy of Management Review*, pp.850-863.

110. Devaraj, S., Easley, R.F. and Crant, J.M., 2008. Research note—how does personality matter? Relating the five-factor model to technology acceptance and use. *Information systems research*, *19*(1), pp.93-105.

111. Dhillon, G., 1995. Interpreting the management of information systems security. PhD Thesis, The London School of Economics and Political Science (LSE).

112. Dhillon, G., 2007. *Principles of information systems security: Texts and cases*. John Wiley & Sons Incorporated.

113. Dhillon, G. and Backhouse, J., 2000. Technical opinion: Information system security management in the new millennium. *Communications of the ACM*, *43*(7), pp.125-128.

114. Dhillon, G. and Backhouse, J., 2001. Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal*, *11*(2), pp.127-153.

115. Dhillon, G. and Torkzadeh, G., 2006. Value-Focused Assessment of Information System Security in Organizations. *Information Systems Journal*, 16, pp.293–314.

116. Dibbern, J. and Chin, W.W., 2005. Multi-group comparison: Testing a PLS model on the sourcing of application software services across Germany and the USA using a permutation-based algorithm. *Handbook PLS-P fadmodellierung. Method,Praxisbeispiele*, pp.135-160.

117. Dikko, M., 2016. Establishing Construct Validity and Reliability: Pilot Testing of a Qualitative Interview for Research in Takaful (Islamic Insurance). *Qualitative Report*, *21*(3).

118. Dillon, W.R., Madden, T.J. and Firtle, N.H., 1993. *Essentials of Marketing Research*. Boston: Irwin.

119. Dojkovski, S., Lichtenstein, S. and Warren, M., 2006. Challenges in fostering an information security culture in Australian small and medium sized enterprises. In *ECIW2006: proceedings of the 5th European conference on Information Warfare*

*and Security* (pp. 31-40).

120. Dojkovski, S., Lichtenstein, S. and Warren, M.J., 2007. Fostering Information Security Culture in Small and Medium Size Enterprises: An Interpretive Study in Australia. In *ECIS* (pp. 1560-1571).

121. Dojkovski, S., Lichtenstein, S. and Warren, M., 2010. Enabling information security culture: influences and challenges for Australian SMEs. In *ACIS 2010: Proceedings of the 21st Australasian Conference on Information Systems*.

122. Eberl, M., 2010. An application of PLS in multi-group analysis: The need for differentiated corporate-level marketing in the mobile communications industry. In *Handbook of partial least squares* (pp. 487-514). Springer.

123. Egress, 2020. Insider Data Breach Survey 2020. Available at: https://www.egress.com/media/vs2jl031/egress-insider-data-breach-survey-2020_uk.pdf

124. Eisenhardt, K.M., 1989. Building theories from case study research. *Academy of management review*, *14*(4), pp.532-550.

125. Eloff, J.H.P. and Eloff, M.M., 2005. Information security architecture. *Computer Fraud & Security*, *2005*(11), pp.10-16.

126. Eloff, M.M. and Von Solms, S.H., 2000. Information security management: an approach to combine process certification and product evaluation. *Computers & Security*, *19*(8), pp.698-709.

127. Elsheikh, Y., 2012. A model for the Adoption and Implementation of Web-based Government services and applications. A Study Based in Grounded Theory Validated by Structural Equation Modelling Analysis in a Jordanian Context. PhD Thesis, University of Bradford.

128. Emma, W., 2017. Growing positive security cultures. Available at: https://www.ncsc.gov.uk/blog-post/growing-positive-security-cultures

129. ENISA (2010). The new Users' Guide: How to Raise Information Security Awareness. Available at: https://www.enisa.europa.eu/publications/archive/copy_of_new-users-guide

130. Ernst and Young (2013). Under cyber attack. EY's Global Information

131. Security Survey 2013. London, Ernst & Young. Available at: https://www.ey.com/Publication/vwLUAssets/EY_-_2013_Global_Information_Security_Survey/$FILE/EY-GISS-Under-cyber-attack.pdf

132. Ernest and Young, 2015. Creating trust in the digital world. EY's Global Information

133. Security Survey 2013. London, Ernst & Young. Available at: https://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2015/$FILE/ey-global-information-security-survey-2015.pdf

134. Farokhi, A., Bahrami, S., Esfandnia, F., Parvaresh, M., Moradi, S. and Esfandnia, A., 2016. Review the Relationship between Organizational Culture and Job Satisfaction among Staff of Kermanshah Medical Sciences University in 2014. *Innovation*, *11*, pp.0-544.

135. Feast, L. and Melles, G., 2010, June. Epistemological positions in design research: A brief review of the literature. In *2nd International Conference on Design Education, University of New South Wales, Sydney, Australia*.

136. Feilzer, M., 2010. Doing mixed methods research pragmatically: Implications for the rediscovery of pragmatism as a research paradigm. *Journal of mixed methods research*, *4*(1), pp.6-16.

137. Fidock, J. and Carroll, J., 2009, December. Combining variance and process research approaches to understand system use. In *Proceedings of the 20th Australasian Conference on Information Systems* (pp. 2-4).

138. Field, A., 2009. *Discovering statistics using SPSS*. Sage.

139. Flick, U., 2011. Mixing methods, triangulation, and integrated research. *Qualitative inquiry and global crises*, *132*(1), pp.1-79.

140. Flowerday, S. and Von Solms, R., 2006, May. Trust: An element of information security. In *IFIP International Information Security Conference* (pp. 87-98). Springer.

141. Fornell, C. and Larcker, D.F., 1981. Structural Equation Models with Unobservable Variables and Measurement Error: Algebra and Statistics. *Journal of Marketing Research (JMR)*, *18*(3).

142. Fourie, L.C.H., 2003. The management of information security-A South African case study. *South African journal of business management*, *34*(2), pp.19-29.

143. Fulford, H. and Doherty, N.F., 2003. The application of information security policies in large UK-based organizations: an exploratory investigation. *Information Management & Computer Security*, *11*(3), pp.106-114.

144. Furnell, S., 2007. IFIP workshop–Information security culture. *Computers & Security*, *26*(1), p.35.

145. Furnell, S. and Clarke, N., 2012. Power to the people? The evolving recognition of human aspects of security. *Computers & Security*, *31*(8), pp.983-988.

146. Furnell, S. and Thomson, K.L., 2009. From culture to disobedience: Recognising the varying user acceptance of IT security. *Computer Fraud & Security*, *2009*(2), pp.5-10.

147. Furnell, S.M., Gennatou, M. and Dowland, P.S., 2000, November. Promoting security awareness and training within small organisations. In *Proceedings of the 1st Australian Information Security Management Workshop, Deakin University, Geelong, Australia* (Vol. 7).

148. Furnell, S.M., Chiliarchaki, P. and Dowland, P.S., 2001. Security analysers: administrator assistants or hacker helpers? *Information management & computer security*.

149. Furnell, S.M., Gennatou, M. and Dowland, P.S., 2002. A prototype tool for information security awareness and training. *Logistics Information Management*, *15*(5/6), pp.352-357.

150. Gabriel, T. and Furnell, S., 2011. Selecting security champions. *Computer Fraud & Security*, *2011*(8), pp.8-12.

151. Gable, G.G., 1994. Integrating case study and survey research methods: an example in information systems. *European journal of information systems*, *3*(2), pp.112-126.

152. Garver, M.S. and Mentzer, J.T., 1999. Logistics research methods: employing structural equation modeling to test for construct validity. *Journal of business logistics*, *20*(1), p.33.

153. Gaunt, N., 2000. Practical approaches to creating a security culture. *International Journal of Medical Informatics*, *60*(2), pp.151-157.

154. Gay, L.R., Mills, G.E. and Airasian, P., 2009. *Educational research: Competencies for analysis and applications.* New Jersey: Person Education.

155. Gefen, D., Straub, D. and Boudreau, M.C., 2000. Structural equation modeling and regression: Guidelines for research practice. *Communications of the association for information systems*, *4*(1), p.7.

156. Geisser, S., 1974. A predictive approach to the random effect model. *Biometrika*, *61*(1), p.101.

157. Gerber, M., Von Solms, R. and Overbeek, P., 2001. Formalizing information security requirements. *Information Management & Computer Security*, *9*(1), pp.32-37.

158. Gerbing, D.W. and Anderson, J.C., 1988. An updated paradigm for scale development incorporating unidimensionality and its assessment. *Journal of marketing research*, *25*(2), pp.186-192.

159. Glaser, B.G. and Strauss, A.L., 2017. *Discovery of grounded theory: Strategies for qualitative research*. Routledge.

160. Gill, P., Stewart, K., Treasure, E. and Chadwick, B., 2008. Methods of data collection in qualitative research: interviews and focus groups. *British dental journal*, *204*(6), pp.291-295.

161. Gliem, J.A. and Gliem, R.R., 2003. Calculating, interpreting, and reporting Cronbach's alpha reliability coefficient for Likert-type scales. Midwest Research-to-Practice Conference in Adult, Continuing, and Community Education.

162. Goddard, W. and Melville, S., 2004. *Research methodology: An introduction*. Juta and Company Ltd.

163. Goh, R., 2003. Information Security: The Importance of the Human Element. PhD Thesis, Preston University.

164. Goldberg, L.R., 1993. The structure of phenotypic personality traits. *American psychologist*, *48*(1), p.26.

165. Goswami, S., Teo, H.H. and Chan, H.C., 2009. Decision-maker mindfulness in it adoption: The role of informed culture and individual personality. *ICIS 2009 Proceedings*, p.203.

166. Götz, O., Liehr-Gobbers, K. and Krafft, M., 2010. Evaluation of structural equation models using the partial least squares (PLS) approach. In *Handbook of partial least squares* (pp. 691-711). Springer.

167. Greene, G. and D'Arcy, J., 2010, June. Assessing the impact of security culture and the employee-organization relationship on IS security compliance. In *5th annual*

*symposium on information assurance (ASIA'10)* (p.1).

168. Hair, J.F., Black, W.C., Babin, B.J., Anderson, R.E. and Tatham, R.L., 2006. *Multivariate data analysis.* 6th Edition. Pearson Prentice Hall.

169. Hair Jr, J.F., Hult, G.T.M., Ringle, C. and Sarstedt, M., 2016. *A primer on partial least squares structural equation modeling (PLS-SEM)*. Sage publications.

170. Hair, J., Hollingsworth, C.L., Randolph, A.B. and Chong, A.Y.L., 2017. An updated and expanded assessment of PLS-SEM in information systems research. *Industrial Management & Data Systems*.

171. Hair, J.F., Risher, J.J., Sarstedt, M. and Ringle, C.M., 2019. When to use and how to report the results of PLS-SEM. *European Business Review*.

172. Hagberg, R. and Heifetz, J., 2000. Corporate culture/organizational culture: Understanding and assessment.

173. Haralambos, M. and Holborn, M., 2000. *Introduction to sociology: Themes and perspectives.* London, Collins.

174. Hassan, N.H. and Ismail, Z., 2012. A Conceptual Model for Investigating Factors Influencing Information Security Culture in Healthcare Environment. *Procedia - Social and Behavioral Sciences*, 65, pp.1007–1012.

175. Hassan, N.H., Ismail, Z. and Maarop, N., 2015. Inofrmation Secuirty Culture: A Systematic Literature Review. *205*, pp.456-463.

176. Hedström, K., Kolkowska, E., Karlsson, F. and Allen, J.P., 2011. Value conflicts for information security management. *The Journal of Strategic Information Systems*, *20*(4), pp.373-384.

177. Hedström, K., Karlsson, F. and Kolkowska, E., 2013. Social action theory for understanding information security non-compliance in hospitals: The importance of user rationale. *Information Management & Computer Security*, *21*(4), pp.266-287.

178. Helokunnas, T. and Kuusisto, R., 2003, November. Information security culture in a value net. In Engineering Management Conference, 2003. IEMC'03. Managing Technologically Driven Organizations: The Human Side of Innovation and Change (pp. 190-194). IEEE.

179. Henseler, J., 2007. A new and simple approach to multi-group analysis in partial least squares path modeling. In *5th International Symposium on PLS and Related Methods,* (pp. 104-107).

180. Henseler, J., Ringle, C.M. and Sinkovics, R.R., 2009. The use of partial least squares path modeling in international marketing. In *New challenges to international marketing*. Emerald Group Publishing Limited.

181. Henseler, J. and Fassott, G., 2010. Testing moderating effects in PLS path models: An illustration of available procedures. In *Handbook of partial least squares* (pp. 713-735). Springer.

182. Hofstede, G., 2001. *Culture's consequences: Comparing values, behaviors, institutions and organizations across nations*. Sage publications.

183. Hofstede, G., 2011. Dimensionalizing cultures: The Hofstede model in context. *Online*

*readings in psychology and culture*, *2*(1), p.8.

184. Holbrook, M.B. and Addis, M., 2007. Taste versus the Market: An Extension of Research on the Consumption of Popular Culture. *Journal of Consumer Research*, *34*(3), pp.415-424.

185. Hong, K.S., Chi, Y.P., Chao, L.R. and Tang, J.H., 2003. An integrated system theory of information security management. *Information Management & Computer Security*, *11*(5), pp.243-248.

186. Hong, K.S., Chi, Y.P., Chao, L.R. and Tang, J.H., 2006. An empirical study of information security policy on information security elevation in Taiwan. *Information Management & Computer Security*, *14*(2), pp.104-115.

187. Hovav, A. and D'Arcy, J., 2012. Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the US and South Korea. *Information & Management*, *49*(2), pp.99-110.

188. Hoyle, R.H., 1995. *Structural equation modeling: Concepts, issues, and applications*. Sage.

189. Höne, K. and Eloff, J.H.P., 2002. Information security policy—what do international information security standards say? *Computers & Security*, *21*(5), pp.402-409.

190. Hu, Q., Dinev, T., Hart, P. and Cooke, D., 2012. Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, *43*(4), pp.615-660.

191. International Atomic Energy Agency, 2017. IAEA Annual Report 2017. Available at: https://www.iaea.org/sites/default/files/publications/reports/2017/gc62-3.pdf

192. IBM, 2014. IBM Security Services 2014 Cyber Security Intelligence Index Analysis of cyber attack and incident data from IBM's worldwide security operations. Available at: https://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom/IBMSecurityServices2014.PDF

193. IBM, 2015. IBM 2015 Cyber Security Intelligence Index Analysis of cyber attack and incident data from IBM's worldwide security Services operations. Available at: https://essextec.com/wp-content/uploads/2015/09/IBM-2015-Cyber-Security-Intelligence-Index_FULL-REPORT.pdf

194. IBM, 2016. Reviewing a year of serious data breaches, major attacks and new vulnerabilities Analysis of cyber attack and incident data from IBM's worldwide security operations. Available at: https://www.ibm.com/downloads/cas/GN0D7O4N

195. International Organisation for Standardisation (ISO), 2005. ISO/IEC 27002, Information technology - Security Techniques - Code of practice for IS security management, second edition.

196. International Organisation for Standardisation (ISO), 2013. ISO/IEC 27002, Information technology - Security Techniques - Code of practice for information security controls.

197. Information Security Breaches Survey, 2013. 2013 Information Security Breaches Survey. Available at:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/191671/bis-13-p184es-2013-information-security-breaches-survey-executive-summary.pdf

198. Information Security Breaches Survey, 2014. 2014 Information Security Breaches Survey. Available at: http://www.pwc.co.uk/assets/pdf/cyber-security-2014-technical-report.pdf

199. Information Security Forum, 2000. Information Security Culture – A Preliminary Investigation. UK, Information Security Forum.

200. Institute of Chartered Accountants in England & Wales, 1999. *Internal control: Guidance for directors on the combined code*. London: Institute of Chartered Accountants in England & Wales.

201. Information Systems Security Association (ISSA), 2013. Incidental Security Leaks: Are You an Insider Threat? Available at: http://c.ymcdn.com/sites/www.issa.org/resource/resmgr/2013_november_web_conference_slides/2013_november_web_conference.pdf

202. Ismail, Z., Masrom, M., Sidek, Z. and Hamzah, D., 2010. Framework to Manage Information Security for Malaysian Academic Environment. *Information Assurance & Cybersecurity*, *2010*, p.16.

203. John, O.P. and Srivastava, S., 1999. The Big Five trait taxonomy: History, measurement, and theoretical perspectives. *Handbook of personality: Theory and research*, *2*(1999), pp.102-138.

204. Johnson, E.C., 2006. Security awareness: switch to a better programme. *Network Security*, *2006*(2), pp.15-18.

205. Jöreskog, K.G. and Sörbom, D., 1996. *LISREL 8: User's reference guide*. Scientific Software International.

206. Joshi, C., Rios Insua, D. and Rios, J., 2019. Insider threat modeling: An adversarial risk analysis approach. In *Sixth Symposium on Games and Decisions in Reliability and Risk.*

207. Judge, T.A., Bono, J.E., Ilies, R. and Gerhardt, M.W., 2002. Personality and leadership: a qualitative and quantitative review. *Journal of applied psychology*, *87*(4), p.765.

208. Junglas, I.A., Johnson, N.A. and Spitzmüller, C., 2008. Personality traits and concern for privacy: an empirical study in the context of location-based services. *European Journal of Information Systems*, *17*(4), pp.387-402.

209. Kaiser, H.F., 1974. An index of factorial simplicity. *Psychometrika*, *39*(1), pp.31-36.

210. Karlsson, F. and Hedström, K., 2014, June. End user development and information security culture. In *International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 246-257). Springer International Publishing.

211. Karlsson, F., Åström, J. and Karlsson, M., 2015. Information security culture–state-of-the-art review between 2000 and 2013. *Information and Computer Security*, *23*(3), pp.246-285.

212. Karyda, M., 2017. Fostering Information Security Culture in Organizations: A Research Agenda. In *MCIS* (p. 28).

213. Kaspersky, 2018. The State of Industrial Cybersecurity 2018. Available at: https://ics.kaspersky.com/the-state-of-industrial-cybersecurity-2018/

214. Kaur, J. and Mustafa, N., 2013, November. Examining the effects of knowledge, attitude and behaviour on information security awareness: A case on SME. In *2013 International Conference on Research and Innovation in Information Systems (ICRIIS)* (pp. 286-290). IEEE.

215. Keil, M., Tan, B.C., Wei, K.K., Saarinen, T., Tuunainen, V. and Wassenaar, A., 2000. A cross-cultural study on escalation of commitment behavior in software projects. *MIS quarterly*, pp.299-325.

216. Kelly, C.J., 2006. Awareness trumps new security toys. *Computer World-Newton Then Framingham Massachusetts*, *40*(41), p.44.

217. Kettaneh, N., Berglund, A. and Wold, S., 2005. PCA and PLS with very large data sets. *Computational Statistics & Data Analysis*, *48*(1), pp.69-85.

218. Khan, B., Alghathbar, K.S., Nabi, S.I. and Khan, M.K., 2011. Effectiveness of information security awareness methods based on psychological theories. *African Journal of Business Management*, *5*(26), pp.10862-10868.

219. Killmeyer, J., 2006. Information security architecture: an integrated approach to security in the organization. CRC Press.

220. King Committee on Corporate Governance and Institute of Directors, 2002. *King Report on Corporate Governance for South Africa, 2002*. Institute of Directors in Southern Africa.

221. Kline, R.B., 2005. *Principles and practice of structural equation modelling*. 2nd edition, Guild Wood.

222. Klein, H.K. and Myers, M.D., 1999. A set of principles for conducting and evaluating interpretive field studies in information systems. *MIS quarterly*, pp.67-93.

223. Kluge, E.H.W., 1998. Fostering a security culture: a model code of ethics for health information professionals. *International journal of medical informatics*, *49*(1), pp.105-110.

224. Knapp, K.J., 2005. A Model of Managerial Effectiveness in Information Security: From grounded theory to empirical test. PhD Thesis, Auburn University.

225. Knapp, K.J., Marshall, T.E., Rainer, R.K. and Ford, F.N., 2006. Information security: management's effect on culture and policy. *Information Management & Computer Security*.

226. Knapp, K.J., Marshall, T.E., Rainer Jr, R.K. and Ford, F.N., 2007. Information security effectiveness: Conceptualization and validation of a theory. *International Journal of Information Security and Privacy (IJISP)*, *1*(2), pp.37-60.

227. Kock, N., 2015. Common method bias in PLS-SEM: A full collinearity assessment approach. *International Journal of e-Collaboration*, *11*(4), pp.1-10.

228. Koh, J. and Kim, Y.G., 2004. Knowledge sharing in virtual communities: an e-business perspective. *Expert systems with applications*, *26*(2), pp.155-166.

229. Koh, K., Ruighaver, A.B., Maynard, S.B. and Ahmad, A., 2005, September. Security

Governance: Its Impact on Security Culture. In *AISM* (pp. 47-58).

230. Korovessis, P., 2015. Establishing an Information Security Awareness and Culture. PhD Thesis, University of Plymouth

231. Korzaan, M.L. and Boswell, K.T., 2008. The influence of personality traits and information privacy concerns on behavioral intentions. *Journal of Computer Information Systems*, *48*(4), pp.15-24.

232. Koskosas, I. et al., 2011. Information Security: Corporate Culture and Organizational Commitment. *Journal of Humanities*, 1(3), pp.192–198.

233. Korzaan, M.L. and Boswell, K.T., 2008. The influence of personality traits and information privacy concerns on behavioral intentions. *Journal of Computer Information Systems*, *48*(4), pp.15-24.

234. Koufteros, X.A., 1999. Testing a model of pull production: a paradigm for manufacturing research using structural equation modeling. *Journal of operations Management*, *17*(4), pp.467-488.

235. Kraemer, S. and Carayon, P., 2005. Computer and information security culture: findings from two studies. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 49, No. 16, pp. 1483-1488). Sage publications.

236. Kraemer, S. and Carayon, P., 2007. Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. *Applied ergonomics*, *38*(2), pp.143-154.

237. Kraemer, S., Carayon, P. and Clem, J., 2009. Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computers & security*, *28*(7), pp.509-520.

238. Kreitner, R., 1995. Kinicki A. *Organizational Behavior*. Irwin Inc.

239. Kritzinger, E. and Smith, E., 2008. Information security management: An information security retrieval and awareness model for industry. *Computers & Security*, *27*(5), pp.224-231.

240. Kruger, H.A. and Kearney, W.D., 2006. A prototype for assessing information security awareness. *Computers & Security*, 25(4), pp.289–296.

241. Kuusisto, T. and Ilvonen, I., 2003. Information security culture in small and medium size enterprises. *Frontiers of E-business Research*.

242. Kwok, L.F. and Longley, D., 1999. Information security management and modelling. *Information Management & Computer Security*, *7*(1), pp.30-40.

243. Lacey, D., 2011. *Managing the Human Factor in Information Security: How to win over staff and influence business managers*. John Wiley & Sons.

244. Lane, T. and May, L., 2006. A Model for Improving E-Security in Australian Universities. *Journal of Theoretical and Applied Electronic Commerce Research (JTAER)*, *1*(2), pp.90-97.

245. Lancaster, G., 2007. *Research methods in management*. Routledge.

246. Lauriola, M. and Levin, I.P., 2001. Personality traits and risky decision-making in a controlled experimental task: An exploratory study. *Personality and individual differences*, *31*(2), pp.215-226.

247. Lee, A.S., 1989. A scientific methodology for MIS case studies. *MIS quarterly*, pp.33-50.

248. Leach, J., 2003. Improving user security behaviour. *Computers & Security*, 22(8), pp.685-692.

249. LePine, J.A. and Van Dyne, L., 2001. Voice and cooperative behavior as contrasting forms of contextual performance: evidence of differential relationships with big five personality characteristics and cognitive ability. *Journal of applied psychology*, *86*(2), p.326.

250. Lewis, B.R., Templeton, G.F. and Byrd, T.A., 2005. A methodology for construct development in MIS research. *European Journal of Information Systems*, *14*(4), pp.388-400.

251. Li, Y., Tan, C.H., Teo, H.H. and Tan, B.C., 2006. Innovative usage of information technology in Singapore organizations: Do CIO characteristics make a difference? *IEEE Transactions on Engineering Management*, *53*(2), pp.177-190.

252. Lichtenstein, S. and Swatman, P.M., 2003. The potentialities of focus groups in e-business research: theory validation. In *Seeking Success in E-Business* (pp. 207-226). Springer.

253. Lim, J.S., Chang, S., Maynard, S. and Ahmad, A., 2009, December. Exploring the relationship between organizational culture and information security culture. In *Australian information security management conference* (p. 12).

254. Lim, J.S., Ahmad, A., Chang, S. and Maynard, S.B., 2010, July. Embedding Information Security Culture Emerging Concerns and Challenges. In *PACIS* (p. 43).

255. Lindell, M.K. and Whitney, D.J., 2001. Accounting for common method variance in cross-sectional research designs. *Journal of applied psychology*, *86*(1), p.114.

256. Loch, K.D., Carr, H.H. and Warkentin, M.E., 1992. Threats to information systems: today's reality, yesterday's understanding. *Mis Quarterly*, pp.173-186.

257. Locke, E.A., 1976. The nature and causes of job satisfaction. Handbook of industrial and organizational psychology. *RandMc Narlly*, *2*(5), pp.360-580.

258. Lopes, I. and Oliveira, P., 2014. Understanding information security culture: a survey in small and medium sized enterprises. In *New Perspectives in Information Systems and Technologies, Volume 1* (pp. 277-286). Springer International Publishing.

259. Lowry, P.B. and Gaskin, J., 2014. Partial least squares (PLS) structural equation modeling (SEM) for building and testing behavioral causal theory: When to choose it and how to use it. *IEEE transactions on professional communication*, *57*(2), pp.123-146.

260. Lu, C.S., Lai, K.H. and Cheng, T.E., 2007. Application of structural equation modeling to evaluate the intention of shippers to use Internet services in liner shipping. *European Journal of Operational Research*, *180*(2), pp.845-867.

261. Luck, D.J. and Rubin, S. 1987. *Marketing research.* Englewood Cliffs, Prentice Hall.

262. Luthy, D. and Forcht, K., 2006. Laws and regulations affecting information management and frameworks for assessing compliance. *Information Management & Computer Security*, *14*(2), pp.155-166.

263. MacKenzie, S.B. and Podsakoff, P.M., 2012. Common method bias in marketing: Causes, mechanisms, and procedural remedies. *Journal of retailing*, *88*(4), pp.542-555.

264. Mackinnon, D., 2011. Integrating mediators and moderators in research design. *Research on Social Work Practice*, *21*(6), pp.675-681.

265. Magklaras, G.B. and Furnell, S.M., 2005. A preliminary model of end user sophistication for insider threat prediction in IT systems. *Computers & Security*, *24*(5), pp.371-380.

266. Mahfuth, A., Yussof, S., Baker, A.A. and Ali, N.A., 2017, July. A systematic literature review: Information security culture. In *2017 International Conference on Research and Innovation in Information Systems (ICRIIS)* (pp. 1-6). IEEE.

267. Mahfuth, A., 2019. Human Factor as Insider threat in Organizations. *International Journal of Computer Science and Information Security (IJCSIS)*, *17*(12).

268. Malcolmson, J., 2009, October. What is security culture? Does it differ in content from general organisational culture? In *43rd Annual 2009 international Carnahan conference on security technology* (pp. 361-366). IEEE.

269. Malhotra, N.K. and Birks, D.F., 2007. *Marketing research: An applied approach*. Pearson.

270. Markovits, Y., Davis, A.J., Fay, D. and Dick, R.V., 2010. The link between job satisfaction and organizational commitment: Differences between public and private sector employees. *International Public Management Journal*, *13*(2), pp.177-196.

271. Markus, M.L., 1981. Implementation politics: Top management support and user involvement.

272. Martins, A. and Eloff, J., 2002. Assessing Information Security Culture. *Proceedings of the ISSA 2002 Information for Security for South-Africa 2nd Annual Conference, 10-12 July 2002*, pp.1–14.

273. Martins, N. and Da Veiga, A., 2015. An Information Security Culture Model Validated with Structural Equation Modelling. *Proceedings of the Ninth International Symposium on Human Aspects of Information Security and Assurance.* In HAISA (pp.11–21).

274. Masrek, M.N., Harun, Q.N. and Zaini, M.K., 2017. Information security culture for Malaysian Public Organisation: a conceptual framework. In *Proceedings of INTCESS 2017 4th international conference on education and social sciences* (pp. 156-166).

275. Maynard, S. and Ruighaver, A.B., 2002. Evaluating IS Security Policy Development. In *3rd Australian Information Warfare and Security Conference*.

276. McAfee, 2012. Combating the Insider Risk to Data. Available at: http://www.mcafee.com/us/resources/solution-briefs/sb-combating-insider-risk-to-data.pdf

277. McBride, M., Carter, L. and Warkentin, M., 2012. Exploring the role of individual employee characteristics and personality on employee compliance with cybersecurity policies. *RTI International-Institute for Homeland Security Solutions*, *5*(1), p.1.

278. McClendon, M. J., 1994. *Multiple Regression and Causal Analysis*. Peacock Publishers Inc.

279. McCormac, A., Calic, D., Parsons, K., Zwaans, T., Butavicius, M. and Pattinson, M., 2016. Test-retest reliability and internal consistency of the Human Aspects of Information Security Questionnaire (HAIS-Q).

280. McCormac, A., Zwaans, T., Parsons, K., Calic, D., and Butavicius, M., 2017. Individual Differences and Information Security Awareness. *Computers & security*, *69*, pp.151-156.

281. McCormac, A., Calic, D., Parsons, K., Butavicius, M., Pattinson, M. and Lillie, M., 2018. The effect of resilience and job stress on information security awareness. *Information and Computer Security*.

282. McCrae, R.R. and John, O.P., 1992. An introduction to the five-factor model and its applications. *Journal of personality*, *60*(2), pp.175-215.

283. McDaniel, C., 2004. *Marketing research: The impact of the internet*. John Wiley & Sons.

284. McGill, T. and Thompson, N., 2018. Gender Differences in Information Security Perceptions and Behaviour. In *29th Australasian Conference on Information Systems*.

285. McHaney, R., Hightower, R. and Pearson, J., 2002. A validation of the end-user computing satisfaction instrument in Taiwan. *Information & Management*, *39*(6), pp.503-511.

286. McIlwraith, A., 2006. *Information security and employee behaviour: how to reduce risk through employee education, training and awareness*. Gower Publishing, Ltd.

287. Mears, L. and Von Solms, R., 2004. Corporate information security governance: a holistic approach. In *ISSA 2004 enabling tomorrow Conference*, (Vol. 6, pp. 30-2004).

288. Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C. and Giannakopoulos, G., 2014. The human factor of information security: Unintentional damage perspective. *Procedia-Social and Behavioral Sciences*, *147*, pp.424-428.

289. Mehan, J., 2016. *Insider threat: A guide to understanding, detecting, and defending against the enemy from within*. IT Governance Ltd.

290. Miles, M.B. and Huberman, A.M., 1994. *Qualitative data analysis: An expanded sourcebook*. Sage.

291. Miles, M.B., Huberman, A.M. and Saldana, J., 2014. *Qualitative Data Analysis: A Methods Sourcebook.* SAGE Publications Ltd.

292. Mitchell, R.C., Marcella, R. and Baxter, G., 1999. Corporate information security management. *New Library World*, *100*(5), pp.213-227.

293. Mouton, J. and Marais, H.C., 1996. *Basic concepts in the methodology of the social sciences.* Pretoria.

294. Mount, M.K., Barrick, M.R. and Stewart, G.L., 1998. Five-factor model of personality and performance in jobs involving interpersonal interactions. *Human performance*, *11*(2-3), pp.145-165.

295. Mount, M.K., Barrick, M.R., Scullen, S.M. and Rounds, J., 2005. Higher-order dimensions of the big five personality traits and the big six vocational interest types. *Personnel psychology*, *58*(2), pp.447-478.

296. Myers, M.D., 1997. Qualitative research in information systems. *Management Information Systems Quarterly*, *21*(2), pp.241-242.

297. Myers, M.D. and Avison, D. eds., 2002. *Qualitative research in information systems: a reader*. Sage.

298. Myers, M.D. and Newman, M., 2007. The qualitative interview in IS research: Examining the craft. *Information and organization*, *17*(1), pp.2-26.

299. Nadler, J.T., Weston, R. and Voyles, E.C., 2015. Stuck in the middle: the use and interpretation of mid-points in items on questionnaires. *The Journal of general psychology*, *142*(2), pp.71-89.

300. Nasir, A., Rashid, M. and Hamid, A., 2018. Conceptualizing and validating information security culture as a multidimensional second-order formative construct. In *the Thirteenth International MultiConference on Computing in the Global Information Technology* (pp. 1-8).

301. Nasir, A., Arshah, R.A., Ab Hamid, M.R. and Fahmy, S., 2019. An analysis on the dimensions of information security culture concept: A review. *Journal of information security and applications*, *44*, pp.12-22.

302. Neuman, G.A. and Kickul, J.R., 1998. Organizational citizenship behaviors: Achievement orientation and personality. *Journal of Business and Psychology*, *13*(2), pp.263-279.

303. Neuman, W.L. and Neuman, L.W., 2006. *Workbook for Neumann Social research methods: qualitative and quantitative approaches*. Allyn & Bacon.

304. Ngo, L., Zhou, W. and Warren, M., 2005. Understanding Transition towards Information Security Culture Change. *Proceeding of the 3rd Australian Computer, Network and Information Forensics Conference*, pp. (67–73).

305. Norman, A.A. and Yasin, N.M., 2009, November. An analysis of Information Systems Security Management (ISSM): The hierarchical organizations vs. emergent organization. In *Internet Technology and Secured Transactions, 2009. ICITST 2009. International Conference for* (pp. 1-8). IEEE.

306. Norusis, M.J., 1992. *SPSS for Windows: Base System User's guide, release 5.0*. SPSS Incorporated.

307. Nunnally, J.C. and Bernstein, I.H., 1994. The Assessment of Reliability. *Psychometric Theory*, 3, pp.248-292.

308. Oates, B.J., 2005. *Researching information systems and computing*. Sage.

309. Organisation for Economic Co-operation and Development, 2005. *The promotion of a culture of security for information systems and networks in OECD countries*. OECD

Publishing. Available at: at: www.oecd.org/document/42/0,2340,en_2649_34255_15582250_1_1_1_1,00.html

310. Okere, I., Van Niekerk, J. and Carroll, M., 2012, August. Assessing information security culture: A critical analysis of current approaches. In *2012 Information Security for South Africa* (pp. 1-8). IEEE.

311. Okun, M.A., August, K.J., Rook, K.S. and Newsom, J.T., 2010. Does volunteering moderate the relation between functional limitations and mortality? *Social science & medicine*, *71*(9), pp.1662-1668.

312. Olson, K., 2010. An examination of questionnaire evaluation by expert reviewers. *Field methods*, *22*(4), pp.295-318.

313. Pallant, J., 2011. Survival manual. *A step by step guide to data analysis using SPSS*.

314. Parsons, K., McCormac, A., Butavicius, M. and Ferguson, L., 2010. *Human factors and information security: individual, culture and security environment*. Defence Science and Technology Organisation Edinburgh (Australia) Command Control Communications and Intelligence DIV.

315. Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. and Jerram, C., 2014. Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & security*, *42*, pp.165-176.

316. Parsons, K.M., Young, E., Butavicius, M.A., McCormac, A., Pattinson, M.R. and Jerram, C., 2015. The influence of organizational information security culture on information security decision making. *Journal of Cognitive Engineering and Decision Making*, *9*(2), pp.117-129.

317. Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A. and Zwaans, T., 2017. The human aspects of information security questionnaire (HAIS-Q): two further validation studies. *Computers & Security*, *66*, pp.40-51.

318. Pattinson, G.M.R. and Anderson, G., 2007. End-user risk-taking behaviour: an application of the imb model. In *Proceedings of 6th Annual Security Conference* (Vol. 5902).

319. Pattinson, M., Butavicius, M., Parsons, K., McCormac, A. and Calic, D., 2015. Factors that influence information security behavior: An Australian web-based study. In *International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 231-241). Springer.

320. Patton, M.Q., 1990. *Qualitative evaluation and research methods*. Sage Publications.

321. Pevchikh, E., 2015. Information Security Culture: Definition, Frameworks and Assessment: A Systematic Literature Review. Master Thesis, Luleå University of Technology.

322. Pierce, E.A. and Hansen, S.W., 2008. Leadership, trust, and effectiveness in virtual teams. *ICIS 2008 Proceedings*, p.43.

323. Pinsonneault, A. and Kraemer, K., 1993. Survey research methodology in management information systems: an assessment. *Journal of management information systems*, *10*(2), pp.75-105.

324. Plog, F. and Bates, D.G., 1976. *Cultural anthropology*. New York, McGraw-Hill.

325. Podsakoff, P.M., MacKenzie, S.B., Lee, J.Y. and Podsakoff, N.P., 2003. Common method biases in behavioral research: a critical review of the literature and recommended remedies. *Journal of applied psychology*, *88*(5), p.879.

326. Ponemon Institute, 2015. Cost of Data Breach Study: Global Analysis. Available at: https://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.PDF

327. Ponemon Institute, 2019. Cost of a Data Breach Report. Available at: https://www.all-about-security.de/fileadmin/micropages/Fachartikel_28/2019_Cost_of_a_Data_Breach_Report_final.pdf

328. Presser, S. and Blair, J., 1994. Survey pretesting: Do different methods produce different results? *Sociological methodology*, pp.73-104.

329. Price Waterhouse Coopers PwC, 2015. Turnaround and transformation in cybersecurity: Power and Utilities Key findings from The Global State of Information Security Survey 2016. Avalaible at: https://www.ourenergypolicy.org/wp-content/uploads/2016/02/pwc-gsiss-2016-power-utilities.pdf

330. Price Waterhouse Coopers PwC, 2015. 2015 Information Security Breaches Survey. Available at: https://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-03.pdf

331. Price Waterhouse Coopers PwC, 2018. The Global State of Information Security Survey 2018. Available at: https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey.html

332. Ramachandran, S., Rao, S.V. and Goles, T., 2008, January. Information security cultures of four professions: A comparative study. In *Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008)* (pp. 454-454). IEEE.

333. Ragu-Nathan, B.S., Apigian, C.H., Ragu-Nathan, T.S. and Tu, Q., 2004. A path analytic study of the effect of top management support for information systems performance. *Omega*, *32*(6), pp.459-471.

334. Renaud, K. and Goucher, W., 2014, June. The curious incidence of security breaches by knowledgeable employees and the pivotal role a of security culture. In *International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 361-372). Springer, Cham.

335. Reid, R. and Van Niekerk, J., 2014, August. From information security to cyber security cultures. In *2014 Information Security for South Africa* (pp. 1-7). IEEE.

336. Richardson, R., 2007. CSI/FBI Computer Crime Survey. *Twelfth Annual Computer Crime and Security*, pp.1-30.

337. Ritchie, J., Lewis, J., Nicholls, C.M. and Ormston, R. eds., 2013. *Qualitative research practice: A guide for social science students and researchers.* Sage.

338. Ringle, C.M., Wende, S. and Will, A., 2005. SmartPLS 2.0. Beta, Hamburg.

339. Ringle, C.M., Sarstedt, M. and Straub, D.W., 2012. Editor's Comments: A Critical Look at the Use of PLS-SEM in" MIS Quarterly". *MIS quarterly*, pp.iii-xiv.

340. Robbins, S.P., 2001. *Organizational behavior*. Pearson Education India.

341. Robson, C., 2011. *Real World Research: A Resource for Users of Social Research Methods in Applied Settings*. Wiley.

342. Roer, K. and Pertic, G., 2017. Indepth insight into the Human factor: The Security Culture Report 2017. CLTRe North America, Inc.

343. Ruighaver, A.B. and Maynard, S.B., 2006, May. Organizational security culture: More than just an end-user phenomenon. In *IFIP International Information Security Conference* (pp. 425-430). Springer US.

344. Ruighaver, A.B., Maynard, S.B. and Chang, S., 2007. Organisational security culture: Extending the end-user perspective. *Computers and Security*, 26(1), pp.56–62.

345. Runeson, P. and Höst, M., 2009. Guidelines for conducting and reporting case study research in software engineering. *Empirical software engineering*, *14*(2), p.131.

346. Sarbanes, P., 2002, July. Sarbanes-oxley act of 2002. In *the Public Company Accounting Reform and Investor Protection Act. Washington DC: US Congress* (p. 55).

347. Sarstedt, M., Ringle, C.M. and Hair, J.F., 2017. Partial least squares structural equation modeling. *Handbook of market research*, *26*, pp.1-40.

348. Sas, M., Hardyns, W., van Nunen, K., Reniers, G. and Ponnet, K., 2020. Measuring the security culture in organizations: a systematic overview of existing tools. *Security Journal*, pp.1-18.

349. Saunders, M., Lewis, P. and Thornhill, A., 2009. *Research methods for business students*. Pearson education.

350. Saunders, M.N., 2011. *Research methods for business students*. Pearson Education.

351. Schein, E.H., 1999. The corporate culture survival guide: sense and nonsense about culture change. San rancisco. *Jossey-Bass*, *1*(2), p.1.

352. Schein, E.H., 2009. *The corporate culture survival guide* (Vol. 158). John Wiley & Sons.

353. Schlienger, T. and Teufel, S., 2002. Information security culture. In *Security in the Information Society* (pp. 191-201). Springer, Boston, MA.

354. Schlienger, T. and Teufel, S., 2003, September. Analysing information security culture: increased trust by an appropriate information security culture. In *14th International Workshop on Database and Expert Systems Applications, 2003. Proceedings.* (pp. 405-409). IEEE.

355. Schlienger, T. and Teufel, S., 2005, May. Tool supported management of information security culture. In *IFIP International Information Security Conference* (pp. 65-77). Springer, Boston, MA.

356. Schneier, B., 2000. *Secrets & Lies: Digital Security in a Networked World*. John Wiley & Sons.

357. Schulze, H., 2018. Insider Threat 2018 Report. *CA Technologies, Cybersecurity Insiders, Tech. Rep*.

358. Schultz, E., 2004. Security training and awareness—fitting a square peg in a round hole. *Computers & Security*, *23*(1), pp.1-2.

359. Schultz, E., 2005. The human factor in security. *Computers & Security*, *24*(6), pp.425-426.

360. Sedera, D., Gable, G. and Chan, T., 2003. Knowledge management for ERP success. *PACIS 2003 proceedings*, p.97.

361. Seidman, I., 2012. *Interview as Qualitative Research: A Guide for Researchers in Education and Social Science*. Teacher College Press.

362. Sekaran, U. and Bougie, R., 2003. *Research Methods for Business, A Skill Building Approach*. John Willey & Sons.

363. Sekaran, U. and Bougie, R., 2016. *Research methods for business: A skill building approach*. John Wiley & Sons.

364. Shah, R. and Goldstein, S.M., 2006. Use of structural equation modelling in operations management research: Looking back and forward. *Journal of Operations management*, *24*(2), pp.148-169.

365. Shane, S., Nicolaou, N., Cherkas, L. and Spector, T.D., 2010. Genetics, the Big Five, and the Tendency to Be Self-Employed. *Journal of Applied Psychology*, *95*(6), pp.1154-1162.

366. Sharma, R. and Yetton, P., 2003. The contingent effects of management support and task interdependence on successful information systems implementation. *MIS quarterly*, pp.533-556.

367. Sherif, E., Furnell, S. and Clarke, N., 2015. An identification of variables influencing the establishment of information security culture. In *International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 436-448). Springer, Cham.

368. Shropshire, J., Warkentin, M., Johnston, A. and Schmidt, M., 2006. Personality and IT security: An application of the five-factor model. *AMCIS 2006 Proceedings*, p.415.

369. Shropshire, J., Warkentin, M. and Sharma, S., 2015. Personality, attitudes, and intentions: predicting initial adoption of information security behavior. *Computers and Security*, *49*, pp.177-191.

370. Singleton Jr, R.A., Straits, B.C. and Straits, M.M., 2009. *Approaches to social research*. 2nd and 5th ed. Oxford University Press.

371. Siponen, M.T., 2000. A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8*(1), pp.31-41.

372. Siponen, M., 2006. Information security standards focus on the existence of process, not its content. *Communications of the ACM*, *49*(8), pp.97-100.

373. Sosik, J.J., Kahai, S.S. and Piovoso, M.J., 2009. Silver bullet or voodoo statistics? A primer for using the partial least squares data analytic technique in group and organization research. *Group & Organization Management*, *34*(1), pp.5-36.

374. Spector, P.E., 1997. *Job satisfaction: Application, assessment, causes, and consequences* (Vol. 3). Sage publications.

375. Spector, P.E., 2000. *Industrial and organisational Psychology-Research and practice*. John Wiley & Sons, Inc.

376. Spector, P.E., Cooper, C.L. and Poelmans, S., 2004. A cross-national comparative study of work-family stressors, working hours and well-being. *Personnel Psychology*, *57*, pp.119-142.

377. Stanton, J.M., Stam, K.R., Mastrangelo, P. and Jolton, J., 2005. Analysis of end user security behaviors. *Computers & security*, *24*(2), pp.124-133.

378. Stankov, L., Boyle, G.J. and Cattell, R.B., 1995. Models and paradigms in personality and intelligence research. In *International handbook of personality and intelligence* (pp. 15-43). Springer, Boston, MA.

379. Straub Jr, D.W., 1990. Effective IS Security. *Information Systems Research*, *1*(3), pp.255-276.

380. Straub, D.W. and Welke, R.J., 1998. Coping with systems risk: security planning models for management decision making. *MIS quarterly*, pp.441-469.

381. Symantec Corporation, 2014. Internet Security Threat Report 2014. Available at: http://www.symantec.com/content/en/us/enterprise/other_resources/bistr_main_report_v19_21291018.en-us.pdf

382. Tabachnick, B. and Fidell, L., 1983. Conditioning matrices: Cleaning up your act before analyzing your data. *Using multivariate statistics*, pp.66-85.

383. Tabachnick, B.G. and Fidell, L.S., 2007. *Experimental designs using ANOVA*. Thomson/Brooks/Cole.

384. Tarimo, C.N., 2006. ICT security readiness checklist for developing countries: A social-technical approach. PhD Thesis, Stockholm University

385. Tashakkori, A. and Teddlie, C., 1998. *Mixed methodology: Combining qualitative and quantitative approaches* (Vol. 46). Sage.

386. TechTarget, 2014. Definition of a Framework. Available at: http://whatis.techtarget.com/definition/framework.

387. Tenenhaus, M., Vinzi, V.E., Chatelin, Y.M. and Lauro, C., 2005. PLS path modeling. *Computational statistics & data analysis*, *48*(1), pp.159-205.

388. Tessem, H.M. and Skaaraas, K.R., 2005. Creating a security culture. *Information Society and Security*, p.15.

389. Thomson, M.E. and Von Solms, R., 1998. Information security awareness: educating your users effectively. *Information management & computer security*, *6*(4), pp.167-173.

390. Thomson, K.L. and Von Solms, R., 2005. Information security obedience: a definition. *Computers & Security*, *24*(1), pp.69-75.

391. Thomson, K.L., Von Solms, R. and Louw, L., 2006. Cultivating an organizational information security culture. *Computer Fraud & Security*, *2006*(10), pp.7-11.

392. Thorne, S., 2000. Data analysis in qualitative research. *Evidence-based nursing*, *3*(3), pp.68-70.

393. Ticehurst, G.W. and Veal, A.J., 2000. Business research methods. *Frenchs Forest, Australia: Longman*.

394. Tolah, A., Furnell, S. and Papadaki, M., 2017. A comprehensive framework for cultivating and assessing Information Security Culture. In *HAISA* (pp. 52-64).

395. Tolah, A., Furnell, S.M. and Papadaki, M., 2019. A Comprehensive Framework for Understanding Security Culture in Organizations. In *IFIP World Conference on Information Security Education* (pp. 143-156). Springer.

396. Trompeter, C.M. and Eloff, J.H.P., 2001. A framework for the implementation of socio-ethical controls in information security. *Computers & Security*, *20*(5), pp.384-391.

397. Trust wave, 2014. 2014 Trustwave Global Security Report. Available at: https://trustwave.azureedge.net/media/13250/2014_trustwave_global_security_report.pdf?rnd=131657087920000000

398. Turban, E., Wetherbe, J. and McLean, E.R., 1996. *Information technology for management: improving quality and productivity*. John Wiley & Sons, Inc.

399. Urbach, N. and Ahlemann, F., 2010. Structural equation modeling in information systems research using partial least squares. *Journal of Information technology theory and application*, *11*(2), pp.5-40.

400. Van Niekerk, J.F., 2010. Fostering information security culture through integrating theory and technology. PhD Thesis, Nelson Mandela Metropolitan University.

401. Van Niekerk, J. and Von Solms, R., 2005. A holistic framework for the fostering of an information security sub-culture in organizations. In *ISSA* (pp. 1-13).

402. Van Niekerk, J. and Von Solms, R., 2006. Understanding Information Security Culture: A Conceptual Framework. *Proceedings of ISSA 2006*, pp.1–10.

403. Van Niekerk, J. and Von Solms, R., 2009, July. Using Bloom's taxonomy for information security education. In *IFIP World Conference on Information Security Education* (pp. 280-287). Springer, Berlin, Heidelberg.

404. Van Niekerk, J.F. and Von Solms, R., 2010. Information security culture: A management perspective. *Computers & Security*, *29*(4), pp.476-486.

405. Van Nunen, K., Sas, M., Reniers, G., Vierendeels, G., Ponnet, K. and Hardyns, W., 2018. An integrative conceptual framework for physical security culture in organisations. *Journal of Integrated Security Science*, *2*(1), pp.25-32.

406. Van Selm, M. and Jankowski, N.W., 2006. Conducting online surveys. *Quality and quantity*, *40*(3), pp.435-456.

407. Verizon, 2017. 2017 Data Breach Investigations Report. Available at: https://www.ictsecuritymagazine.com/wp-content/uploads/2017-Data-Breach-Investigations-Report.pdf

408. Vinzi, V.E., Trinchera, L. and Amato, S., 2010. PLS path modeling: from foundations to recent developments and open issues for model assessment and improvement.

In *Handbook of partial least squares* (pp. 47-82). Springer.

409. Von Solms, R., 1996. Information security management: The second generation. *Computers & Security*, *15*(4), pp.281-288.

410. Von Solms, R., 1998. Information security management (1): why information security is so important. *Information Management & Computer Security*, *6*(4), pp.174-177.

411. Von Solms, R., 1999. Information security management: why standards are important. *Information Management & Computer Security*, *7*(1), pp.50-58.

412. Von Solms, B., 2000. Information security -the third wave? *Computers & Security*, *19*(7), pp.615-620.

413. Von Solms, B., 2001. Information security-a multidimensionale discipline. *Computers & Security*, *20*(6), pp.504-508.

414. Von Solms, B., 2005. Information Security governance: COBIT or ISO 17799 or both? *Computers & Security*, *24*(2), pp.99-104.

415. Von Solms, B., 2006. Information security–the fourth wave. *Computers & security*, *25*(3), pp.165-168.

416. Von Solms, R. and Von Solms, B., 2004. From policies to culture. *Computers & security*, *23*(4), pp.275-279.

417. Vroom, C. and Von Solms, R., 2004. Towards information security behavioural compliance. *Computers & Security*, *23*(3), pp.191-198.

418. Wang, Y.D., Yang, C. and Wang, K.Y., 2012. Comparing public and private employees' job satisfaction and turnover. *Public Personnel Management*, *41*(3), pp.557-573.

419. Ward, P. and Smith, C.L., 2002. The development of access control policies for information technology systems. *Computers & Security*, *21*(4), pp.356-371.

420. Warkentin, M. and Willison, R., 2009. Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems*, 18(2), pp.101–105.

421. Warkentin, M., Malimage, N. and Malimage, K., 2012, December. Impact of Protection motivation and deterrence on IS security policy compliance: a multi-cultural view. In *Pre-ICIS Workshop on Information Security and Privacy (SIGSEC)*.

422. Walsham, G., 1995. Interpretive case studies in IS research: nature and method. *European Journal of Information Systems*, *4*(2), pp.74-81.

423. Walton, M.H., 2015. *Security Culture: A How-to Guide for Improving Security Culture and Dealing with People Risk in Your Organisation*. Ashgate Publishing, Ltd.

424. Weber, R.P., 1990. *Basic content analysis*. Sage.

425. Weirich, D. and Sasse, M.A., 2001, September. Pretty good persuasion: a first step towards effective password security in the real world. In *Proceedings of the 2001 workshop on New security paradigms* (pp. 137-143).

*426.* Westervelt, R., 2013. Top 10 Security Breaches Of 2013. Available at: *https://www.crn.com/slide-shows/security/240165003/top-10-security-breaches-of-*

*2013.htm*

427. Whitten, D., 2008. The chief information security officer: An analysis of the skills required for success. *Journal of Computer Information Systems*, *48*(3), pp.15-19.

428. Wiles, R., Crow, G. and Pain, H., 2011. Innovation in qualitative research methods: a narrative review. *Qualitative Research*, *11*(5), pp.587-604.

429. Wiley, A., McCormac, A. and Calic, D., 2020. More than the individual: Examining the relationship between culture and Information Security Awareness. *Computers & Security*, *88*, p.101640.

430. Williams, S.E., Cumming, J., Ntoumanis, N., Nordin-Bates, S.M. and Ramsey, R., 2012. Further Validation and Development of the Movement Imagery Questionnaire. *Journal of Sport & Exercise Psychology*, *34*, pp.621-646.

431. Wolverton, M.L., 2009. Research Design, Hypothesis Testing, and Sampling. *Appraisal journal*, *77*(4).

432. Wong, K.K.K., 2013. Partial least squares structural equation modeling (PLS-SEM) techniques using SmartPLS. *Marketing Bulletin*, *24*(1), pp.1-32.

433. World Institute for Nuclear Security (WINS)., 2011. *Nuclear Security Culture Revision 2.0: A WINS International Best Practice Guide for Your Organisation.* Vienna: WINS.

434. Yin, R.K., 2003. Designing case studies. *Qualitative Research Methods*, pp.359-386.

435. Zakaria, O., 2004, November. Understanding Challenges of Information Security Culture: A Methodological Issue. In *AISM* (pp. 83-93).

436. Zakaria, O. and Gani, A., 2003, June. A conceptual checklist of information security culture. In *2nd European Conference on Information Warfare and Security, Reading, UK*.

437. Zikmund, W.G., Babin, B.J., Carr, J.C. and Griffin, M., 2003. Research methods. *Health economics research method*, *2*.

438. Zikmund, W.G., Carr, J.C. and Griffin, M., 2013. *Business Research Methods*. Cengage Learning.

439. Zurko, M.E., Kaufman, C., Spanbauer, K. and Bassett, C., 2002. Did you ever have to make up your mind? What Notes users do when faced with a security decision. In *Computer Security Applications Conference, 2002. Proceedings. 18th Annual* (pp. 371-381). IEEE.

# Appendices

# Appendix A. Summary Discussion of Fourteen Studies of The Current Perspective Offered by Each Study Reviewed in Chapter 3

1. **Martin and Eloff (2002) Study:** provide a formalised comprehensive definition for an information security culture and integrate information security with the knowledge fields of information security and organisational behaviour. This study developed a theoretical security culture framework based on the concepts of organisational behaviour (Robbins et al. 2003) by identifying various information security controls, which can also be referred as principles, on an individual level, group level and organisational level of organisational behaviour that have an impact on the security culture. The identified nine theoretical components of security controls are security policy, change management, risk analysis, awareness, budget, benchmarking, ethical conduct and trust. Also, this study provides a foundation for the security culture assessment instrument and developed items to assess a security culture. Their assessment approach consists of four phases, which are developing a questionnaire, survey process, analyses data and interpret data.

   This study used a mixed of quantitative and qualitative approach in order to test and valid their proposed model. The researchers developed the questionnaire and conduct a case study to test the proposed approach and assess the security culture in an IT consultancy organisation with a sample consisting of less than fifty employees.

   The designed framework could be used as a guideline to address the issues concerning security culture and served as the theoretical base to ensure content validity of the security culture assessment instrument. However, the designed security culture questionnaire of this study has not been statistically tested and validated in the real world.

2. **Chia et al. (2002) research**: studied the effect of organisational culture on the security culture by adopting the organisational culture framework of Detert et al. (2000). They identified eight cultural aspects, which are important as regards measuring the efficiency of the security culture. The identified dimensions are security budget, security expenditure, security awareness, the security risk, a security policy, making security suggestions, security ownership and audits.

The study established on the basis of the qualitative approach. Empirical case studies were conducted in SMEs Australia environment, in order to identify and establish the correlation between organisational culture and the security culture. They highlighted the importance of some constructs, such as top management support and awareness that could be used for developing a security culture.

However, they did not provide of how to improve the quality of security culture. Their study had constructed for SMEs in Australia national setting, which might imply that it is not scalable to larger organisations that operate on a global basis. A further limitation of their research is that they did not design a process or an assessment instrument in order to measure the security culture in the organisation.

3. **Kuusisto and Ilvonen (2003) and Helokunnas and Kuusisto (2003) studies:** proposed a system in which the security culture is cultivated on the basis of the interaction between the reference framework and its components by focusing on hub organisations that form part of a value net. They concluded that the security culture could be created by formalising a framework that consists of standardisation, certification and measurement of information security and influencing content component which includes individual attitude, motivation, knowledge, communication and compliance.

   They performed an assessment instrument by focusing on the information security framework. They implemented as semi-structured interviews in eleven SMEs in Finland, in order to determine the state of information system security. They used ISO/IEC / IEC 17799:2000 (ISO/IEC 2000) as the base for developing their questionnaire.

   This study stated that a security culture is dependent not only on employee behaviour, but also on organisational processes. However, this study did not design a framework to explain the interaction between the framework components and content components, which they had defined. They did not perform an extensive research on the assessment of security culture, but rather on the controls to be considered in implementing information security in an organisation. They did not develop a security culture questionnaire. Also, their work had constructed for SMEs environment and it might not be applicable for larger organisations.

4. **Schlienger and Teufel (2002) study:** was one of the early studies that use existing social theories to explore the security culture. They proposed a paradigm shift from a technical to a socio-cultural approach towards information security, in order to address the human element and minimise risks to information assets in the organisation. Their work is based on Schein's culture model (1999) and had been discussed in terms of a case study implementation. They defined the security culture with three layers, which are corporate policies that include (policy, organisation structure and resources), management includes (implementation of security policy, responsibility, qualification and training, awards and prosecutions, audits and benchmarks) and individual (attitude, communication and compliance).

   Schlienger and Teufel (2003, 2005) developed assessment instrument for analysing the security culture of an organisation based on internal marketing, in order to create, change and maintain the security culture. Also, they proposed a model consists of five phases, which are pre-evaluation, strategic planning, operative planning, implementation and post-evaluation for managing and assessing the information security culture.

   This study used quantitative and qualitative approaches, in order to understand the official rules that are supposed to influence the security behaviour of employees and recognise the areas that need improvements in the organisation. They designed the assessment tool based on the three levels of organisational behaviour of Robbins (2001), and on Schein (1999) study. They perform a survey method with interview employees in a private bank and the working group (Information Security Society) in Switzerland to ensure the practicability of the process and used the data to validate the assessment instrument.

   This study contributed towards the effective development of an assessment instrument that could be used by the organisation and that has been tested for reliability and validity. This study concluded that a security culture is a subset of the overall organisational culture. They explained that the security culture should support an environment where information security becomes a natural part of the employee's daily activities. Finally, they argued that in order to create, maintain and modify the security culture continuously, there has to be an ongoing measurement and analysis of the culture. This could be achieved by use of an ongoing survey during the lifetime of the

organisation. However, the researchers did not focus on the design a framework for an security culture that could be served as the foundation for developing a security culture assessment instrument.

5. **Organisation for Economic Co-operation and Development (OECD) (2005) study:** proposed nine principles which organisations should be considered, in order to promote the security culture through their participants and increase awareness regarding the risk to information assets in organisations. The proposed principles or guidelines emphasised the importance of creating a culture of information security, which would encourage everyone to protect their information systems and networks, irrespective of their work roles. The nine principles are awareness, responsibility, response, ethics, democracy, risk assessment, security design and implementation, security management and re-assessment. Unfortunately, the OECD's guidelines did not extend to a framework that explains the interaction between the principles or how to assess them in an organisation.

6. **Tessem and Skaraas (2005) study:** considered the information security to be a part of the organisational culture that needs to be combined with change management, marketing and communications in order to understand how to cultivate a security culture and improve the awareness message for users. This study focused on management roles and its play in creating the security culture based on the study of Schein (1999). They presented different components that should be considered when cultivating a security culture in an organisation, which are long term plan, change management, top management, participation, branding and organisation culture. They highlighted the importance of considering a measure that assesses the level of security culture in the organisation.

   Unfortunately, they did not propose a mechanism or assessment instrument that could be used for assessing the security culture. Another limitation of this study is that they did not extend their work to a framework that could show how the principles influence each other to cultivate the security culture.

7. **Ruighaver, Maynard and Ahmad (2005, 2006) study:** proposed two frameworks. The first one for security governance based on literature review analysis. The second one for security culture by adapting Chia et al. (2002) security culture framework,

which based on Deter et al. (2000) organisation culture framework that has eight dimensions of culture (the basis of truth and rationality, the nature of time and time horizon, motivation, stability versus change/innovation/personal growth, orientation to work, task, co-workers, isolation versus collaboration/ corporation, control, coordination and responsibility, and orientation and focus internal or external), in order to investigate the elements of security governance that influence on any of the eight dimensions of security culture model. This study explored the specific elements of security governance, which are a structural mechanism, functional mechanisms and social participation that have an impact on the dimension of control, coordination and responsibility of security culture.

The study established on the basis of qualitative approach by performing a number of case studies in SMEs organisations in Australia. The authors reported that there is a need to formalise social participation activities into the organisational structure in order to increase responsibility and a stronger sense of ownership that people have over security. Also, they noted that the concept of security culture could not be covered with one single framework or a model because it is a complex issue.

However, this study conducted on SMEs environment in a national setting. It might not be applicable to other organisations in another area in the world. Also, they did not propose a mechanism or an assessment instrument to assess the security culture in the organisation.

8. **Dojkovski, Lichtenstein and Warren (2006) study:** developed a framework for fostering a security culture in SMEs in Australia environment. They identified various external and internal elements as well as illustrate the interaction between them which security culture should include in SMEs. Several approaches were used in this study to develop a valid model. First, they designed a framework based on a literature review. Second, they conducted a focus group study by following the Lichtenstein (2003) principles to validate their framework. Then, they designed questions and conducted a case study in an engineering SME and in two IT service provider SMEs in order to determine their security consciousness, the challenges confronted by SMEs as regards fomenting a security culture and to confirm the proposed framework.

Their framework is formed of the following components: organisational and individual learning, e-learning, ethical, national, organisational culture, managerial includes (policies and procedures, benchmarking, risk analysis, budget, management, response, training, education, awareness and change management), behavioural includes (responsibility, integrity, trust, ethnicity, values, motivation and orientation personal growth).

The authors highlighted various principles that must be considered in order to cultivate a security culture. The authors suggested that management should be educated about the potential strategic role of information technology and information security. However, their framework had constructed for SMEs environment in a national setting. It might not be applicable to other organisations in another area in the world. Since they considered input from focus group to design their framework, thus this makes it practical and relevant to the specific industry. Also, they did not propose a mechanism or an assessment instrument to assess the security culture in the organisation.

9. **Kraemer and Carayon (2005, 2007) study:** were the first researchers who related security culture to six organisational culture dimensions of Guldenmund (2000), in order to define the culture principles for the organisation. The six dimensions are employee participation, training, hiring practices, reward system, management commitment, communication and feedback. The study established on the basis of qualitative approach by interviewing computer and security managers from various organisations in order to define the organisational culture principles. They defined and provided a list of comments for each of the six principles. Unfortunately, this study did not test their approach in the organisation to check if it is effective in cultivating the information security culture or not. Also, they did not design a mechanism or a process to assess the security culture in the organisation.

10. **Da Veiga and Eloff (2007, 2010) study:** developed a comprehensive framework (ISCF) to cultivate a security culture in an organisation based on their information security governance framework (CISF), a study of Robbins et al. (2003) and Schein's model (1999). They listed various component of information security that deal with the human, process and technical risks, which could direct employee behaviour in all required facets of information security and affect the cultivation of an acceptable level of security culture inside the organisation. Then, they grouped the identified

components into categories based on a study of Robbins et al. (2003) and implemented by the organisation on the individual, group or organisational tier of information security behaviour. So, the security culture cultivated on each of the three tiers of information security behaviour, and also reflected in the form of artefacts, values and assumptions based on Schein's model (1999) that develops for each component on each of the three information security behaviour tiers.

The six components are the leadership and governance includes (sponsorship, strategy, IT governance, risk assessment and ROI/metrics/measurement), security management and organisation includes (legal and regulatory and program organisation), policy includes (policies, standard, procedure, guidelines, best practice and certification), security program management includes (monitor, audit and compliance), user security management includes (awareness, training, trust, privacy and ethical conduct), technology protection and operations includes (system development, technical operation, physical and environment, asset management, incident management and business continuity) and change management. Their proposed (ISCF) considered all the required components for security culture, which are information security, organisational culture and organisational behaviour.

The researchers proposed an assessment tool in order to consider their proposed a comprehensive security culture framework (ISCF). They used their proposed (ISCF) as the basis of the instrument for assessing a security culture and help organisations to identify the developmental areas and determine plans whereby to make a security culture conducive to the protection of information assets. The designed assessment tool included five major components: leadership and governance, security management and organisations, security policies, security program management and user security management.

Their framework of security culture established on the basis of the quantitative research method to collect data. They collected data in a South African firm that performs audit and advisory assignments with 3000 employees through questionnaires from their developing the security culture assessment tool.

This study developed a comprehensive security culture model and contributed a good understanding of how organisations could create and maintain an acceptable level of

security culture. Also, their work serves as a foundation for designing a valid assessment instrument to assess the security culture. They suggested that in order to have successful security culture in the organisation, it requires a commitment from senior management and the other commitment is implementing a security awareness program. However, there is a lack in an illustration of the possible relationships between identified components.

11. **Alnatheer et al. (2012) study:** developed a conceptual measurement model that presented different components, which comprised and influence the security culture. The proposed model showed the relationship between factors influencing the security culture and factors reflecting the security culture. Several approaches have been used in this study to develop a reliable and valid model. First, a synthesised literature review analysis in thirteen studies and models focused on security culture and a qualitative interview with security management experts in different organisations in Saudi Arabia environment in order to develop a model. Then, they used a series of quantitative assessment techniques, which are Exploratory Factor Analysis (EFA), Confirmatory Factor Analysis (CFA), Structural Equation Modelling (SEM), and nomological validity in order to test and valid their proposed model.

    They identified three components that constitute the security culture which are security awareness, security ownership and security compliance. They outlined five factors that influence security culture, which are top management, policy enforcement, education and training, ethical conduct policy and risk assessment (policy maintenance).

    This study was one of the earliest in the security culture area that developed a reliable and valid security culture model. However, the study was unable to develop a valid scale for some identified factors, such as ethical conduct policies, policy maintenance, and security compliance. Also, this study had conducted in a national setting and it might not be applicable to another area in the world.

12. **Alhogail and Mirza (2014, 2015) and Alhogail (2016) study**: developed a comprehensive framework, which presents the key human factors and the change management principles that should be considered to be used as guidance for cultivation the security culture in organisations. The framework includes three components, and each component consists of a number of related tasks. The first component is the human

factor component, which based on the social cognitive theory of Bandura (2001) and literature review analysis. It provides the basic human factors influencing and forming the human behaviour. It covers four main human issues that are preparedness, responsibility, management, and society and regulations.

The second component is the scope component, which has on Bakry's (2004) framework. The framework includes five dimensions, which are a Strategy, Technology, Organisation, People, and Environment (STOPE). This component presents a structured view of the information security cultural issues and how these dimensions collaborate with each other, in order to create a secure environment for information assets. The third component is the development management component that is based on change management principles and tools in order to provide a tool for guiding the establishing the security culture. The interaction between each STOPE dimension and the human factor dimension are guided by principles.

The study established on the basis of qualitative and quantitative approaches, in order to provide accurate findings and valid the framework. The author validated the designed framework by experts review to provide their feedback on the comprehensiveness of the framework structure and its associated tasks. Then, the author designed questionnaire and conducted three case studies in three different organisations in Saudi Arabia national settings to measure the employees' artefacts, attitudes, perceptions and knowledge and to measure the level of security culture in each organisation.

This study presented the integration between three fields, which are the security culture, change management and human factor in information security. However, their framework had constructed in a national setting. It might not be applicable to another area in the world.

13. **Sherif, Furnell and Clarke (2015) study:** proposed a conceptual model, which identified variables that affect the cultivation of information security in the organisation and also investigate the relationship between identified variables by conducting a synthesised literature review analysis in the period of 1999 to 2014. The designed framework is formed with three models, which are national culture, organisational culture and security compliance. Each model contains a parent and its sub-variables. The variables of first model national culture based on Hofstede (1984) dimensions. The

variables of second model organisational culture based on Schein (1999) levels. The third model security compliance consists of information security behaviour includes (personality test and job satisfaction), security acceptance includes (current level of security acceptance), awareness and education include (targeted security promotion), information security policy includes (goal and vision) and management support includes (decision maker involvement).

Unfortunately, this study did not test their approach to check if it is effective in establishing a security culture or not. Also, they did not design a mechanism or a process to assess the security culture in the organisation.

14. **Masrek, Harun and Zaini (2017) study:** developed a conceptual framework for assessing the security culture in public organisations in Malaysian environment. They identified several dimensions, which security culture should include in public organisations. Several approaches were used in this study to develop a reliable and valid framework. First, they designed a framework based on previous studies, such as (Zakaria 2006; Alkabani et al. 2014; Martin & Da Veiga 2015; Alhogail & Mirza 2015) and verified it using interview method with IT managers working in agencies of Malaysian federal government. Then, they designed questionnaire for measuring information security culture in the public organisations of the federal ministries, in order to determine their security challenges confronted as regards fomenting the security culture and to confirm the proposed framework. The study applied various of quantitative assessment techniques, which are Exploratory Factor Analysis (EFA) and Confirmatory Factor Analysis (CFA) in order to test and valid their framework.

    Their framework is formed of the following six dimensions and each dimension contains two sub dimensions: management support includes (information security commitment, information security importance), policy and procedures includes (information security policy effectiveness, information security directives), compliance includes (information security monitoring compliance, information security consequences), awareness includes (information security responsibility, information security training), budget includes (information security budget practice, information security investment) and technology includes (information technology capability, information technology compatibility).

The study showed that all of the identified dimensions are significant and should be considered to develop the security culture. However, their framework had constructed for public environment in a national setting. It might not be applicable to other organisations in another area in the world. Since they considered input from specific group (IT directors) to confirm their framework, thus this makes it practical and relevant to the specific industry.

## Appendix B. Ethical Approval Letter -Interview

RESEARCH WITH PLYMOUTH UNIVERSITY

25 July 2017

**CONFIDENTIAL**
Alaa Tolah
School of Computing, Electronics and Mathematics

Dear Alaa

***Ethical Approval Application***

Thank you for submitting the ethical approval form and details concerning your project:

***A Comprehensive Measurement Framework for An Effective Information Security Culture***

I am pleased to inform you this has been approved, subject to the following conditions:

- Section 2.4: A list of the companies and statement of their agreement for the study is required before the start of the project.
- Section 2.6: Amend the start date to 'date of approval'
- Section 4.3 and 2.1 specify that individuals will be recruited because they have a professional position. The employer has agreed for the study to take place, and this needs to be made clear explicitly. There is a requirement for volunteers recruited because of their job, to be informed that their employer had agreed for their participation (see point 2.5.2 of guidelines)
  Amend the information sheet to add statement about their employer's agreement

Kind regards

Paula Simson
Secretary to Faculty Research Ethics Committee

Cc. Prof Steve Furnell
Dr Maria Papadaki

Faculty of Science and Engineering
Plymouth University
Drake Circus
PL4 8AA

**T** +44 (0) 1752 584 584
**F** +44 (0) 1752 584 540
**W** www.plymouth.ac.uk

Mrs Jayne Brenen
Head of Faculty Operations

# Appendix C. Ethical Approval Letter -Survey

UNIVERSITY OF PLYMOUTH

2 November 2018

**CONFIDENTIAL**
Alaa Tolah
School of Computing, Electronics and Mathematics

Dear Alaa

***Ethical Approval Application***

Thank you for submitting the ethical approval form and details concerning your project:

***A Comprehensive Measurement Framework for An Effective Information Security Culture***

I am pleased to inform you that this has been approved subject to clarification of the following:

- It is not clear who the participants will be in this research.
  In section 3.1, it states "The survey will be conducted via online questionnaire hosted within Centre for Security, Communications and Network Research (CSCAN) Plymouth University" Later on, it mentions "the organisation", and in the consent form "institutions" are referred to. The questionnaire also implies outside organisations.

  Which organisation or institutions? Is this the University of Plymouth only or an outside body or bodies?

  Section 2.5 that no external institutions are involved.

  However, in section 4,3 it states "An invitation email will be sent to a key contact person in company" and "Respondents will be nominated by the key contact person in their organisation".

This all suggests that the research is being conducted on participants in organisations other than the University.

Please clarify who the participants are. If they are from organisations other than the University, then section 2.5 requires amending.

Mrs Jayne Brenen, Head of Faculty Operations, Faculty of Science and Engineering, University of Plymouth, Drake Circus, Plymouth, Devon PL4 8AA T +44 (0)1752 584584 F +44 (0)1752 584540 W www.plymouth.ac.uk

## Appendix D. Interview Invitation Flyer

INFOSECURITY WITH PLYMOUTH UNIVERSITY

### Participants Invited for A Research Study

A Comprehensive Framework for an Effective Information Security Culture

We are looking for volunteers from security specialists to participate in an interview for the study conducted by Mrs. Alaa Tolah, a PhD candidate in the Centre for Security, Communications and Network Research at Plymouth University. The research aims to gain a better understanding of how security culture can be established and implemented in organisations.

The interview will take approximately 20 to 30 minutes and this can be completed face-to-face, via Skype, or telephone; whichever is your preference.

The questions will focus upon the security awareness practices to explore aspects of how the security culture is managed in the organisation and the organisation's efforts in building appropriate security values and knowledge among employees in order to provide guidance that improve information assets' security, while also avoiding information security risks to insiders.

If you are interested and would like more information about this study, or to volunteer for this study, please contact:

Mrs. Alaa Tolah at alaa.tolah@plymouth.ac.uk or +447493032212

Or fill out the table that located in the back of this paper to allow me to contact you.

Thank you!

**This study has been reviewed and approved by Plymouth University 's Ethical Principles for Research Involving Human Participants.**

# Appendix E. Interview Guide

### Interview invitation letter

Dear Sir/Madam,

I would initially like to express my sincere appreciation for your participation in the current study. I would like to emphasise that your participation in the present research will contribute to the acquisition of accurate results and will enhance the quality information security culture research within organisation.

The interview will take last approximately 20 to 35 minutes, and this can be completed face-to-face, via Skype or telephone; whichever is your preference. During the interview, the questions will relate to the security culture practices in your organisation and relate to your organisation's attempts to develop progressive values of security and knowledge among employees.

Moreover, I can assure you that your identity and all personal details will remain confidential, as well as the organisation's name, which will not be displayed in the results of this research or any published papers; all will remain anonymous. The results will be summarised together, and thus, the privacy and confidentiality will not be threatened in relation to any of the participants or the data collected, as this will not be shared outside of the research team. Furthermore, you can be assured that the confidentiality code of conduct will be complied with at all times.

Finally, we will hope that this participation will contribute to research data collection and that the findings will help to measures and improve the level of a security culture among employees in an organisation and illustrate the major threats that they may pose to the security of information assets in organisation and vulnerability in their practices. Also, your participation will help to understand the influence of information security practices factors on information security behaviour in your particular organisation. Please do not hesitate to contact me if you have any further queries at all.

Yours sincerely,

Alaa Tolah

PhD Candidate

Centre for Security, Communications and Network Research

School of Computing, Electronics and Mathematics

Plymouth University

alaa.tolah@plymouth.ac.uk

**Information Security Culture-Interview Guide**

*A) Introductory questions:*

Employment:

1. How long have you been working in your organisation?

□Less than a year □1 -4 □5-10 □more than 10 years

2. What are the main/core services of your department?

- Would you briefly talk about it, please?

*B) Information security culture practices questions:*

1. What do you know about the main information security practices and rules that are used in your organisation?

a) Do you have any information security education and training courses in your organisation?

b) What are the different methods of security awareness and training sessions you get in your organisation?

c) Do you get regular information about risks and dangers inherent in your work?

2. How would you rate the information security in your organisation? (Where 1 is 'not at all acceptable' and 5 is 'completely acceptable').

(1) Not at all acceptable. (3) Moderately acceptable.

(2) Slightly acceptable. (4) Very acceptable. (5) Completely acceptable.

*C) The employee security behaviour pattern questions:*

1. How good do you think employees' security behaviours reflect what they have told about security responsibilities? (Please rate below).

(1) Very poor. (2) Poor.

(3) OK. (4) Good. (5) Very good.

2. What do you consider to be the most effective of the following security practices on the security-related behaviours of employees in an organisation? (Please rank it in order of effectiveness.)

 Top Management commitment (e.g. management gives a strong guidance to support to security program).

 IT department initiatives in your organisation (e.g. Have clear policies, procedures, guidelines, risk analysis, education and training program).

 Information security technical countermeasure (e.g. Anti-viruses software, firewall and intrusion detection).

 Personal values and beliefs (culture) about the information security.

3. The concept of information security culture is related to artefacts, attitudes, values, assumptions and knowledge held by an employee for doing daily activities regarding their behaviour and attitude toward the information security in the organisation.

a) In your opinion, what would an effective security culture look like in your organisation?
b) What do you consider the main contributory factors in term of creating and implementing an effective security culture in your organisation?
c) What do you consider the main barriers or obstacles to achieving improved security compliance in the organisation?

*D) Closing Questions:*

1. What changes or improvements would you think that might have the most positive impact upon the security culture in the organisation?
2. Are there any comments you would like to add based on the discussion, so far?

# Appendix F. Interview - Code Book

| No. | Questions | Response | Code |
|---|---|---|---|
| **A-1** | Work experience | Less than a year | <1 |
| | | Between 1 and 4 years | 1<=4 |
| | | Between 5 and 10 | 5<=10 |
| | | More than 10 years | >10 |
| **A-2** | Department main/core services | Open | |
| **B-1** | Company information security practices and rules | Open | |
| **B-1-a** | Information security education and training course | Yes | 1 |
| | | No | 2 |
| **B-1-b** | Security awareness and training methods | Open | |
| **B-1-c** | Information security risks alert | Yes | 1 |
| | | No | 2 |
| **B-2** | Company's information security | Not at all acceptable | 1 |
| | | Slightly acceptable | 2 |
| | | Moderately acceptable | 3 |
| | | Very acceptable | 4 |

| No. | Questions | Response | Code |
|---|---|---|---|
| | | Completely acceptable | 5 |
| **C-1** | Employees security behaviours | Very poor | 1 |
| | | Poor | 2 |
| | | OK | 3 |
| | | Good | 4 |
| | | Very good | 5 |
| **C-2** | Rank effective security practices | Most important | 1 |
| | | 2nd important | 2 |
| | | 3rd important | 3 |
| | | Least important | 4 |
| **C-3-a** | Effective security culture | Open | |
| **C-3-b** | Main contributory factors | Open | |
| **C-3-c** | Main obstacles factors | Open | |
| **D-1** | Suggestion for improving security culture | Open | |
| **D-2** | Comments | Open | |

# Appendix G. Interview- List of Category Codes

| Themes | Codes |
|---|---|
| Top Management | TM |
| Policy | P |
| Education and Training | ET |
| Risk Assessment | RA |
| Ethical Conduct | EC |
| Awareness | A |
| Ownership | O |
| Compliance | C |
| Job Satisfaction | JS |
| Personality Trait | PT |

| Themes | Codes |
|---|---|
| Text Messages | TX |
| Email | E |
| Poster | PO |
| Information on Company website | CW |
| Training courses | TC |

# Appendix H. Interview - Example of Category Codes

**Table 1: An Effective Information Security Look Like in Company**

| Respond ID | Responses | Code |
|---|---|---|
| 1 | Increase training workshops for all staff | ET |
| | Employee must feel like a security person and enhance the sense of ownership | O |
| | Have clear policies and procedures that everyone must follow | P |
| 2 | Every employee should feel like a security responsible person | O |
| | Develop or use an application for the security awareness | A |
| | Develop or use an application that teach security lessons | ET |
| 3 | The importance of security should come from the highest levels of staff | TM |
| | Increase training sessions | ET |
| | Use different methods of awareness | A |
| 4 | Employee should know their security responsibility and have ownership | O |
| | Develop a security knowledge application that educate employees | ET |
| 5 | Develop clear security policies and procedures | P |
| | Establish training courses that educate all employees | ET |
| 6 | Have very clear policies and regulations that are clearly described | P |
| | Policies must be clearly described to all members of staff through training sessions | ET |

| Respond ID | Responses | Code |
|---|---|---|
| | It is absolutely vital for the top management to have very clear policies | TM |
| 7 | Publish and implement security policies | P |
| | Active & continuous engagement & endorsement of security by all levels of leadership | TM |
| | Active and current education and training program for all users | ET |
| 8 | Teach courses related to the organisations' information security | ET |
| 9 | Increase awareness among employees | A |
| | Do training sessions to all employees | ET |
| 10 | Do training sessions regrading security to increase employee’s knowledge | ET |
| 11 | Teaching the entire members the basic lessons about the importance of security | ET |
| | Make some creativity into awareness efforts | A |
| | Following the IT rules and procedures will keep the work safe | P |
| 12 | Increase the employee’s security knowledge by doing training courses | ET |
| | Establish clear security policies and rules | P |
| | Instil a concept that a security belongs to everyone responsibilities | O |
| 13 | Develop a knowledge application that teaches advanced lessons about security | ET |
| | Develop awareness program | A |

**Table 2: The Main Contributory Factors for Creating and Establishing the Security Culture**

| Respond ID | Responses | Code |
|---|---|---|
| 1 | Conduct periodic training workshops for all staff | ET |
| | Implement and update a security policy and rules | P |
| 2 | Policies, procedures and guidelines | P |
| | Risk analysis | RA |
| | Education and training program | ET |
| 3 | More involvement is needed from top management in company | TM |
| | Increase awareness | A |
| | Do training sessions | ET |
| | Produce a risk assessment report | RA |
| 4 | Induction session or training session at any time | ET |
| | Understanding ethical codes & obligations is an essential key to improve security culture | EC |
| 5 | Increase people awareness | A |
| | Increase people awareness about security by holding training courses | ET |
| 6 | Continuous updating to the security policy | P |
| | There must be severe consequences for anyone who doesn't comply with policy | C |

| Respond ID | Responses | Code |
|---|---|---|
| | Increase awareness | A |
| 7 | Leadership support and activism at all levels | TM |
| 8 | Have the controls, policies and the practices in place | P |
| | Education and training sessions | ET |
| 9 | Having a periodical risk assessment | RA |
| | Maintain a well security policy | P |
| 10 | Increasing the awareness | A |
| | Increasing the training program | ET |
| | Employee's satisfaction with his job | JS |
| 11 | Keep advising the employees by conduct a training workshop | ET |
| | A security culture can establish if employees comply with security policy | P |
| | A security culture can establish if employees comply with security policy | C |
| 12 | Improve the skills of information security employees by educate them | ET |
| | Update and develop security policy and procedures | P |
| 13 | Create that mind set within the employees by educate and aware them | A |
| | Create that mind set within the employees by educate and aware them | ET |

**Table 3: The Main Barriers Factors for Achieving the Security Compliance**

| Respond ID | Responses | Code |
|---|---|---|
| 1 | Lack of education program s | ET |
| | Unclear and not update security policy | P |
| 2 | Lack of flexibility and awareness | A |
| 3 | Lack of awareness | A |
| | Lack of training and limited to the managers and IT staffs | ET |
| 4 | Lack of ownership | O |
| | Some obstacles related to faulty human behaviour and ethical issues | EC |
| 5 | People awareness | A |
| | The administration support of IT security programs | TM |
| 6 | A lack of clarity on the policies | P |
| | Having no consequences to staff who fail to comply | C |
| 7 | Lack of leadership support and activism at all levels | TM |
| 8 | Lack of training materials | ET |
| | Lack of understanding their responsibility and thus lack of ownership | O |
| 9 | Lack of security awareness | A |
| | Lack of security education and training courses | ET |

| Respond ID | Responses | Code |
|---|---|---|
| | Not having clear security policies and roles | P |
| 10 | Lack of management | TM |
| | Lack of awareness | A |
| | Lack of training sessions | ET |
| 11 | Problem with not following security policies and regulations | P |
| | Not feeling the ownership of protecting company information security | O |
| 12 | Lack of awareness | A |
| | Lack of education program | ET |
| 13 | Improve education and training process | ET |
| | Lack of awareness | A |

**Table 4: The Improvements or Changes that Positively Affect the Security Culture**

| Respond ID | Responses | Code |
|---|---|---|
| 1 | Conduct training workshops | ET |
| | Develop and maintain policies and rules | P |
| 2 | Train and educate all employees at a different level in a company | ET |
| | Raise employee's awareness and knowledge | A |
| 3 | Increase staff's awareness | A |

| Respond ID | Responses | Code |
|---|---|---|
| | Conduct a risk assessment regularly | RA |
| 4 | Aware employees about security issues | A |
| | Strengthen the sense of ownership in employees | O |
| | Establish a code for ethic to know the accepted behaviour | EC |
| 5 | Organise security training sessions | ET |
| | Increase employee's awareness about the importance of a security | A |
| 6 | Top management support for security effectiveness | TM |
| | Improve a clear security policy | P |
| | Outlining the consequences on staff not complying with a security | C |
| 7 | The support of leadership for the importance of security | TM |
| | Train employees about information security issues | ET |
| 8 | The support of top management in security success | TM |
| 9 | All employees should have some training sessions | ET |
| | The CEO and leadership support for security | TM |
| 10 | Raise employee's awareness and knowledge | A |
| | Enhance education and training security programs | ET |
| | Motivate employee that do the right thing for security to enhance his satisfaction | JS |

| Respond ID | Responses | Code |
|---|---|---|
| 11 | Warn employee to increase awareness | A |
| | Develop education program | ET |
| | Improve a security policy and procedures | P |
| 12 | Run a successful security awareness program | A |
| | Establish a security education and training program | ET |
| | Have a clear updated security policy and rules | P |
| 13 | Giving employees high level of awareness | A |

**Table 5: Methods of Security Awareness and Training Used in Company**

| Respond ID | Responses | Code |
|---|---|---|
| 1 | Sending text messages | TX |
| | Sending email | E |
| | Online training workshops | TC |
| 2 | Text messages | TX |
| | Email notice | E |
| | Online training session | TC |
| 3 | Send text messages to employees | TX |
| | Send email | E |

| Respond ID | Responses | Code |
|---|---|---|
| | Training classes | TC |
| 4 | Send email | E |
| | Poster | PO |
| 5 | Warn by email | E |
| | Posters | PO |
| 6 | Email | E |
| | Poster | PO |
| | web based education program | TC |
| 7 | Sending email | E |
| | Produce poster | PO |
| | Online education session | TC |
| 8 | Warn by email | E |
| | Training course | TC |
| | Company website | CW |
| 9 | Send email to alert employees | E |
| 10 | Use email to warn employees | E |
| 11 | Employees alerted by emails. | E |

| Respond ID | Responses | Code |
|---|---|---|
| 12 | Sending emails twice a week | E |
| 13 | Sending text messages | TX |
| | Sending emails to employees | E |
| | Education sessions & induction day | TC |
| | Display security blacklisted on Company website | CW |

## Appendix I. Survey Invitation Flyer

INFOSECURITY WITH PLYMOUTH UNIVERSITY

**Participants Invited for A Research Study**

A Comprehensive Framework for an Effective Security Culture

We are looking for volunteers who work in the organisation to participate in a survey for the study conducted by Mrs Alaa Tolah, a PhD candidate in the Centre for Security, Communications and Network Research at Plymouth University. The research aims to gain a better understanding of how security culture can be established and implemented in organisations.

The survey will take approximately 10 to 15 minutes. The survey comprises some background questions, and statements about your perception of security awareness practices to explore aspects of how the security culture is managed in the organisation and the organisation's efforts in building appropriate security values and knowledge among employees in order to provide guidance that improve information assets' security.

If you are interested and would like more information about this study, or to volunteer for this study, Please contact:

Mrs.Alaa Tolah at alaa.tolah@plymouth.ac.uk or +447493032212

Or you can fill out the survey directly through the link below:

https://survey.eu.qualtrics.com/jfe/form/SV_cOzq2QjkXMAyvul

QR Code:

Thank you!

**This study has been reviewed and approved by Plymouth University's Ethical Principles for Research Involving Human Participants.**

# Appendix J. Survey

## Consent form

## Invitation to participate in the research entitled: A Comprehensive Framework for An Effective Information Security Culture

Dear Sir/Madam,

I would like to invite you to participate in a research survey that I am conducting as part of my Doctoral degree in the Centre for Security, Communications and Network Research at the University of Plymouth concerning about understanding and evaluating the conceptualisation of security culture and the need to implement it in organisations.

**Background**

Information security culture means that employees have the required values, beliefs and knowledge while behaving accordingly in a way that protects the information assets and to preserve confidentiality, integrity, and availability of information. For example, a clear-desk policy, strong passwords, updating antivirus software, and not disclosing private information.

**The overall aim of this study**

The research aims to gain a better understanding of how security culture can be established in organisations, to measure the current level, and identify new issues that may affect security culture within organisations. For this purpose, we brought together established research theories along with a few novel factors to propose a framework that can be used by practitioners to establish or measure security culture. We will provide management approaches and guidelines based on the proposed framework to assist in the establishment of effective security cultures in organisations.

**Aim of survey**

The survey aims to assess the current level of the security culture in the organisation and identify factors influencing it according to the proposed framework.

**Sample**

This study is directed at any persons who are above 18 years old and working in a relevant organisation. Your participation will contribute to our research findings from your organisation's perspective, help us to improve the accuracy of our results, and will enhance quality security culture research within organisations. The survey will take approximately 15 to 20 minutes, which comprises some background questions and statements regarding your perception of information security practices; therefore, there is no right or wrong answer. Each statement can be answered with only a single selection.

**Anonymity, informed consent and ethical consideration**

*1-Description of risks:*

I would like to assure you that the personal details are not required, and the name of the organisation will not be recorded or stored. **All participants will be anonymous.** The results will be summarised

and published as aggregate. The code of conduct will have complied with at all times. This study has received approval from our Faculty Ethics Committee.

*2-Benefits of proposed research:*

A report will be available that highlights the key developmental areas in the security culture. Your participation will help to further understand the influence of information security practice factors on information security behaviour in organisations. This hoped that this will contribute to research that will improve the level of the security culture in organisations.

*3-Right to withdraw:*

Participation in this study is voluntary. You have the right to quit or withdraw from the survey at any time up until the final submission.

***Informed consent is assumed once a person has read, understood all the above and continued to complete the survey*.**

**Contact for further information**

If you want any further information about this study, please do not hesitate to contact me via email: alaa.tolah@plymouth.ac.uk

In case you have any concerns about the way in which the study has been conducted, you can contact the Faculty of Science and Engineering Human Ethics Committee. Their current contact details are:

Mrs. Paula Simson
Faculty of Science and Engineering

University of Plymouth Drake Circus
Plymouth
PL4 8AA
Email: paula.simson@plymouth.ac.uk

Thank you for taking the time to read this information sheet.

---

**By submitting a response you agree that:**
**- I'm 18+ years old.**
**- I understand that I am free to withdraw up until the point of submission of my responses.**
**- I understand that my anonymity is guaranteed.**
**- I confirm that I have read and understood the information given and agree to take part in the study?**

**□Yes** **□ No**

***Section 1: Background Information***

1. Type of organisation:

☐ Private ☐ Public ☐ Semi-public (Charitable, Voluntary, etc.)

☐ Other (please specify): _____

2. Organisation industry:

☐Construction ☐ Consultant ☐ Education/ Training

☐ Energy ☐ Finance/ banking ☐ Industrial Tech

☐ Information and communication technology ☐ Insurance

☐ Manufacturing ☐ Medical/Healthcare ☐Merchandising

☐ Oil and gas ☐Retail/Wholesale ☐ Telecommunication

☐ Transportation ☐ Utilities ☐ Other (please specify): _____

3. Number of employees in the organisation:

☐ Less than 250 ☐ 250-1000 ☐ More than 1000

4. Gender:

☐ Male ☐ Female ☐ Prefer not to say

5. Age:

☐ Under 25 ☐ 25-35 ☐ 36-45 ☐ 46-55 ☐ 56 or above

6. The country do you currently reside:

7. Education qualification in an IT related field:

☐ Yes ☐ No

8. Length of service in the current organisation:

☐ Less than a year ☐ 1-4 ☐ 5-10 ☐ more than 10 years

9. What level of responsibility do you have in this organisation?

☐ Senior manager/Executive/Director ☐ Middle management

☐ Department manager/supervisor ☐ Operational staff (administrative, clerical, etc.)

☐ Technological staff ☐Security staff ☐ Other (please specify): _____

10. Did you have an induction when you started work with the organisation?

☐ Yes ☐ No **(If you choose No, please go to answer Section 2).**

11. Did the induction include security information awareness about using and protection of data and organisation's information?

☐ Yes ☐ No

***Section 2: Knowledge statements***

**Directions**

Below is a list of statements related to the level of information security knowledge. Please consider each statement and choose the answer (Yes, No or don't know) that is applicable.

| # | Statement | Yes | No | Don't know |
|---|---|---|---|---|
| 1 | The organisation has formal documents for information security policies. **(Choosing No or Don't know will jump you to Q5).** | | | |
| 2 | I have read the information security policy section that is applicable to my job. | | | |
| 3 | Are there disciplinary consequences if employees do not comply with the information security policies in the organisation? | | | |
| 4 | The organisation consistently reviews and updates the information security policies on a periodic basis. | | | |
| 5 | I am informed regularly about information security requirements and updates. | | | |
| 6 | Are your security responsibilities and roles clear? | | | |
| 7 | Does the organisation have a person/team that is assigned for assessing the risk of information assets? | | | |
| 8 | I am regularly informed and updated information about risks associated with security breaches such as scam email attachments, unknown senders, etc. | | | |
| 9 | Does the organisation consistently assesses and generates a report for the information security risk analysis on a periodic basis? | | | |
| 10 | To whom you should report information security incidents? (Please select all that apply).<br>☐Helpdesk ☐Human resources ☐IT department ☐My immediate manager<br>☐ Group information security officer ☐ I do not know<br>☐ The whistle-blowing process should be used | | | |
| 11 | The organisation has the ethical code of conduct. **(Choosing No or Don't know will jump you to Q16).** | | | |

| | | | | |
|---|---|---|---|---|
| 12 | Does the organisation have an ethics committee/advisory that is responsible for the code of conducts? | | | |
| 13 | Is the organisation's code of conducts clear and easy to understand? | | | |
| 14 | I am informed by my organisation about information relevant legislation and regulations, such as of intellectual property and copyright laws. | | | |
| 15 | Is there a procedure to ensure the safety of data at the end of each working day? For example, not leaving confidential documents on the desk when you leave the working area. | | | |
| 16 | Do you as an employee know where to find/access the following:<br>a) The organisational information security policies. | | | |
| | b) The organisation's ethical code of conduct. | | | |
| | c) The security-related training programs. | | | |
| | d) The update information/materials regarding the organisation's security. | | | |
| 17 | Have you attended any security training in the organisation such as Induction training or Web based training?<br>**(Please select all that apply :)**<br>☐Induction training ☐Hands-on training sessions<br>☐ Web based training ☐All the above | | | |
| 18 | I would like to receive information security awareness and training sessions. **(Choosing No or Don't know will jump you to Q20).** | | | |
| 19 | How do you prefer to receive information about security awareness and training messages? (Please select all that apply).<br>☐SMS messages ☐e-mail ☐Posters ☐Video's<br>☐Induction training ☐Hands-on training sessions ☐ Web based training<br>☐Discussion group ☐Business unite presentations ☐Articles in new frontiers | | | |

***Section 3: Information security culture practices and behaviour statements***

**Directions**

Below are nine factors relevant to security culture. Please consider each factor and choose the answer:

| |
|---|
| Strongly Disagree or the statement is definitely false. |
| Disagree or the statement is mostly false. |
| Neutral or the statement is equally true and false. |
| Agree or the statement is mostly true. |
| Strongly Agree or the statement is definitely true. |

that best reflects your opinion about **your organisational security**.

| # | Statement | Strongly Disagree | Disagree | Neutral | Agree | Strongly Agree |
|---|---|---|---|---|---|---|
| 1 | Top Management involvement and commitment for information security | | | | | |
| 1.1 | Top management perceives information security as an important organisational priority. | | | | | |
| 1.2 | In my organisation, all levels of leadership are always involved in key information security activities. | | | | | |
| 1.3 | Top managers give strong and consistent support to the security program. | | | | | |
| 1.4 | Top managers provide the required resources for training and learning to enable me to comply with information security requirements. | | | | | |
| 1.5 | The involvement and support from top management have a significant role in establishing the security culture. | | | | | |
| 2 | Information Security Policy | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 2.1 | The information security policy clearly states what is expected of me with regard to the safeguarding of information. | | | | | |
| 2.2 | The contents of the information security policy prescribed by the organisation are easy to understand. | | | | | |
| 2.3 | The information security policy is applicable to the information I use in my daily tasks. | | | | | |
| 2.4 | The written information security policy is important to create an effective security culture. | | | | | |
| 3 | Information Security Education and Training | | | | | |
| 3.1 | The security-related training program explains what is expected of me, as well as the related information security requirements, policies and how to behave securely from the start of employment. | | | | | |
| 3.2 | I received adequate information security training appropriate for my daily job duties. | | | | | |
| 3.3 | I believe that it is necessary to have security refresher training on security policies or any updates in the organisation. | | | | | |
| 3.4 | The appropriate information security education and training contribute to creating effective security culture. | | | | | |
| 4 | Risk Analysis and Assessment | | | | | |
| 4.1 | I believe the risk assessment processes of the organisation are adequate to identify risks that negatively impact on information security. | | | | | |
| 4.2 | It is important to understand the security | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | threats, vulnerabilities, and be alerted of any risks inherent to information assets in my workplace. | | | | | |
| 4.3 | The security risk analysis and assessment are important in creating an effective security culture. | | | | | |
| 5 | Ethical Code of Conduct | | | | | |
| 5.1 | It is important to have a clear ethical code of conduct and direction in protecting sensitive and confidential information by applying related regulations. | | | | | |
| 5.2 | It is important to take care when talking about work or confidential information in public places. | | | | | |
| 5.3 | The security-related ethical code of conduct is important for creating an effective security culture. | | | | | |
| 6 | Job Satisfaction | | | | | |
| 6.1 | I feel satisfied with the kind of work I do in this job. | | | | | |
| 6.2 | I feel I am being paid a fair amount of money for the work I do. | | | | | |
| 6.3 | I am satisfied with chances for promotion and rewards. | | | | | |
| 6.4 | I am satisfied with the benefits I receive. | | | | | |
| 6.5 | I feel satisfied with the organisation's level of supervision. | | | | | |
| 6.6 | I like my co-workers. | | | | | |
| 7 | Security Awareness | | | | | |
| 7.1 | I am aware of the information security policies and security aspects relating to my job, for example, a password policy. | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 7.2 | I am aware of ongoing initiatives about security awareness. | | | | | |
| 7.3 | It is important to raise awareness about information security with employees. | | | | | |
| 8 | Security Ownership | | | | | |
| 8.1 | Protecting information security is the responsibility of every employee in the organisation. | | | | | |
| 8.2 | It is important that individuals are involved in the development of security policies in the organisation. | | | | | |
| 8.3 | It is important to have a sense of ownership regarding the organisational security practices to enhance the security culture of the organisation. | | | | | |
| 9 | Security Compliance | | | | | |
| 9.1 | It is important to follow the information security policies and practices, such as not sharing passwords to enhance the security culture in the organisation. | | | | | |
| 9.2 | The organisation enforces adherence to the information security policy. | | | | | |
| 9.3 | I believe that the attention should be drawn on incidents of not adhering to the information security policies and requirements. | | | | | |

***Section 4: All about you***

**Directions**

Below are a number of 44 characteristics that may or may not apply to you. Please consider each item and score:

| | |
|---|---|
| 1 | Strongly Disagree or the statement is definitely false. |
| 2 | Disagree or the statement is mostly false. |
| 3 | Neutral or the statement is equally true and false. |
| 4 | Agree or the statement is mostly true. |
| 5 | Strongly Agree or the statement is definitely true. |

to indicate the extent you agree or disagree with the statement that describes you *at the present time.* Each statement begins with **"I see myself as someone who…"**

| Statement | # | Statement | # |
|---|---|---|---|
| 1. is talkative | | 23. tends to be lazy | |
| 2. tends to find fault with others | | 24. is emotionally stable, not easily upset | |
| 3. does a thorough job | | 25. is inventive | |
| 4. is depressed, 'blue' | | 26. has an assertive personality | |
| 5. is original, comes up with new ideas | | 27. can be cold and aloof | |
| 6. is reserved | | 28. perseveres until the task is finished | |
| 7. is helpful and unselfish with others | | 29. can be moody | |
| 8. can be somewhat careless | | 30. values artistic, aesthetic experiences | |
| 9. is relaxed, handles stress well | | 31. is sometimes shy, inhibited | |
| 10. is curious about many different things | | 32. is considerate and kind to almost everyone | |
| 11. is full of energy | | 33. does things efficiently | |
| 12. starts quarrels with others | | 34. remains calm in tense situations | |
| 13. is a reliable worker | | 35. prefers work that is routine | |
| 14. can be tense | | 36. is outgoing, sociable | |
| 15. is ingenious, a deep thinker | | 37. is sometimes rude to others | |
| 16. generates a lot of enthusiasm | | 38. makes plans and follow through with them | |
| 17. has a forgiving nature | | 39. gets nervous easily | |
| 18. tends to be disorganised | | 40. likes to reflect, play with ideas | |
| 19. worries a lot | | 41. has few artistic interests | |
| 20. has an active imagination | | 42. likes to cooperate with others | |
| 21. tends to be quiet | | 43. is easily distracted | |
| 22. is generally trusting | | 44. is sophisticated in art, music, or literature | |

**Thank you very much for taking the time to complete this survey. Your help in providing this information is appreciated. If there is anything else you would like to add regarding this research, please feel free to add them here.**

# Appendix K. Multivariate Normal P-P plot of Regression Standardised Residual

**Figure 1: Multivariate Normal P-P plot of Regression Standardised Residual for Top Management**

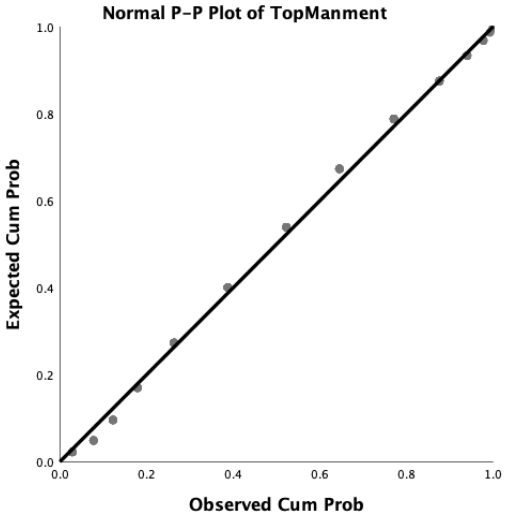



**Figure 2: Multivariate Normal P-P plot of Regression Standardised Residual for Security Policy**

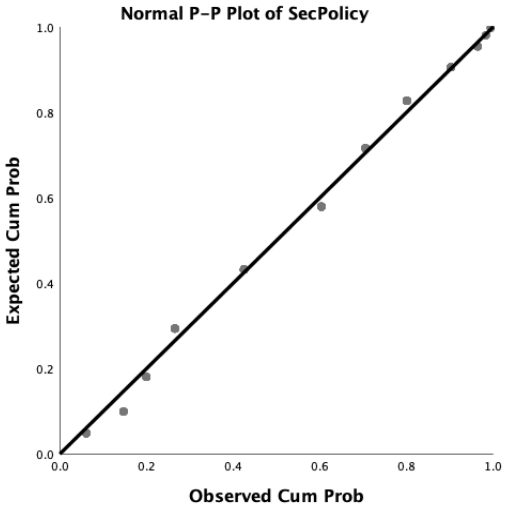


**Figure 3: Multivariate Normal P-P plot of Regression Standardised Residual for Security Education and Training**

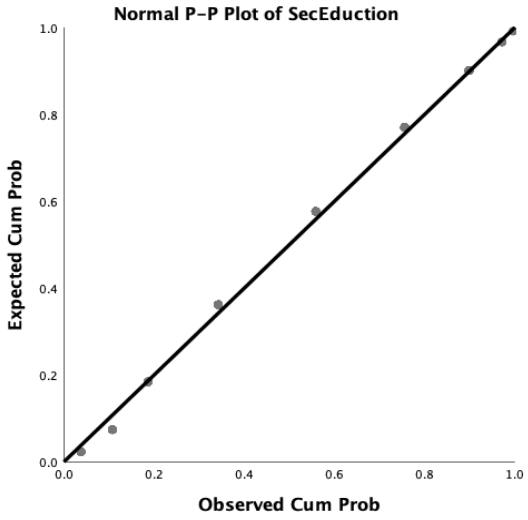



**Figure 4: Multivariate Normal P-P plot of Regression Standardised Residual for Security Risk Analysis and Assessment**

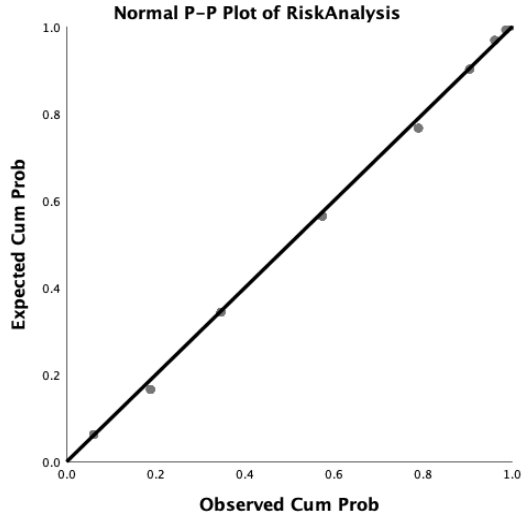


**Figure 5: Multivariate Normal P-P plot of Regression Standardised Residual for Ethical Conduct**

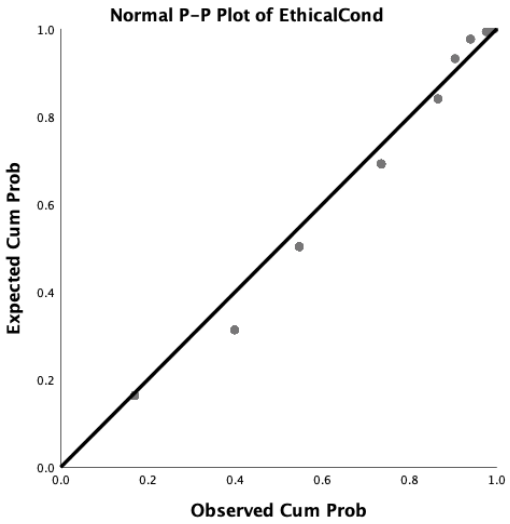



**Figure 6: Multivariate Normal P-P plot of Regression Standardised Residual for Job Satisfaction**

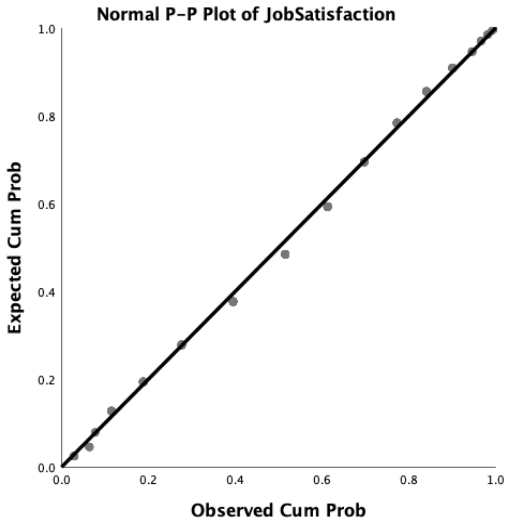


**Figure 7: Multivariate Normal P-P plot of Regression Standardised Residual for Extraversion**

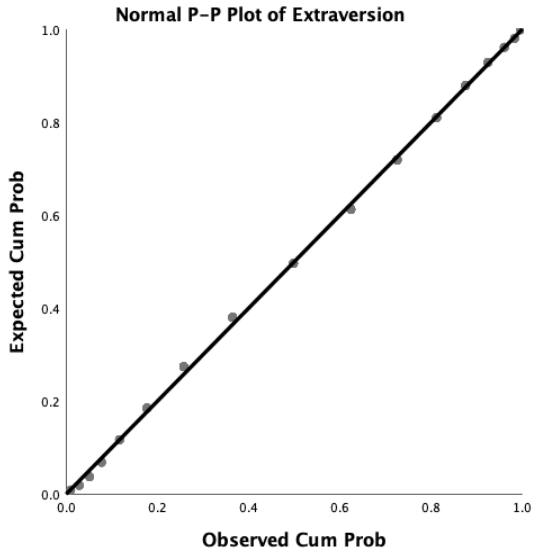



**Figure 8: Multivariate Normal P-P plot of Regression Standardised Residual for Agreeableness**

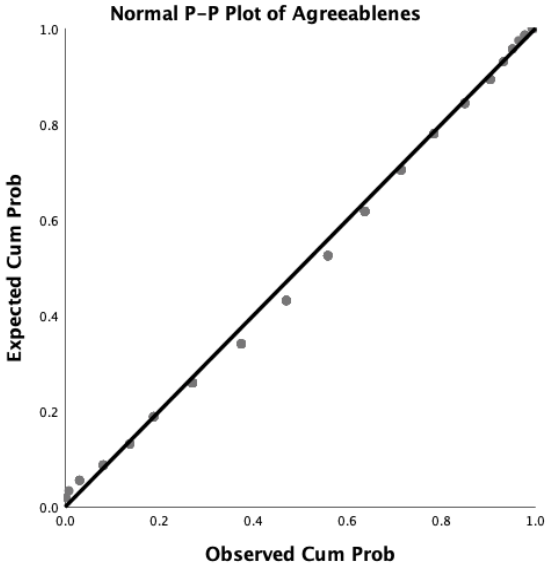


**Figure 9: Multivariate Normal P-P plot of Regression Standardised Residual for Conscientiousness**

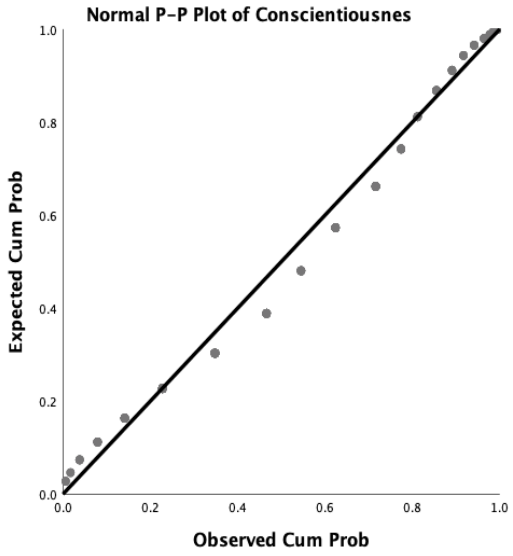



**Figure 10: Multivariate Normal P-P plot of Regression Standardised Residual for Neuroticism**

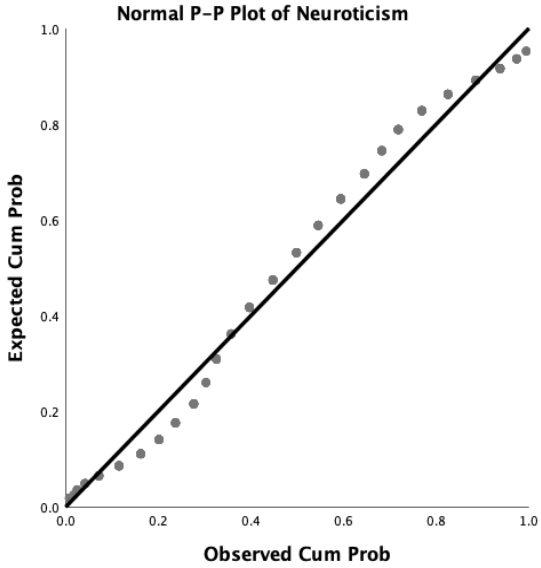


**Figure 11: Multivariate Normal P-P plot of Regression Standardised Residual for Openness**

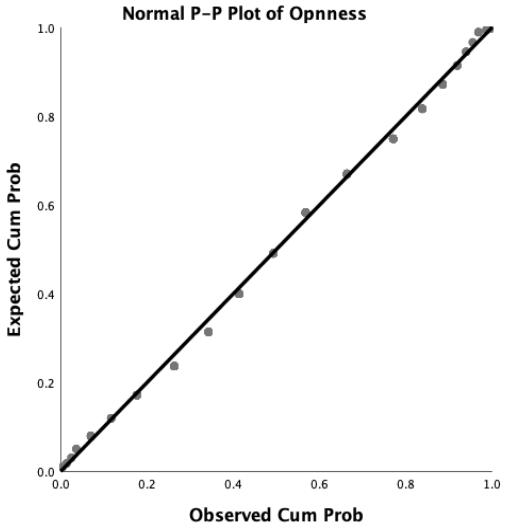



**Figure 12: Multivariate Normal P-P plot of Regression Standardised Residual for Security Awareness**

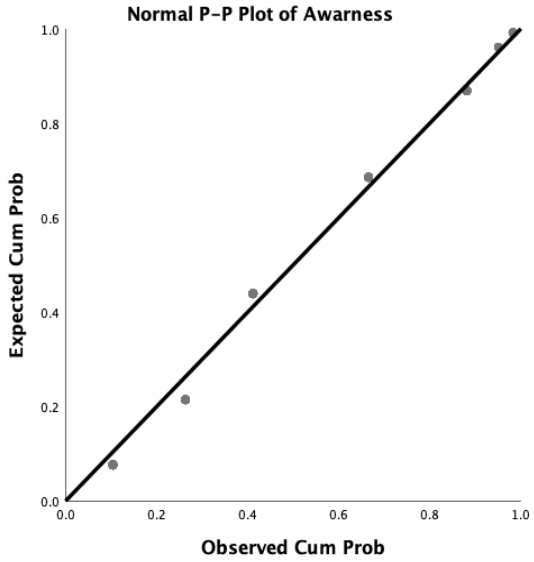


**Figure 13: Multivariate Normal P-P plot of Regression Standardised Residual for Security Ownership**

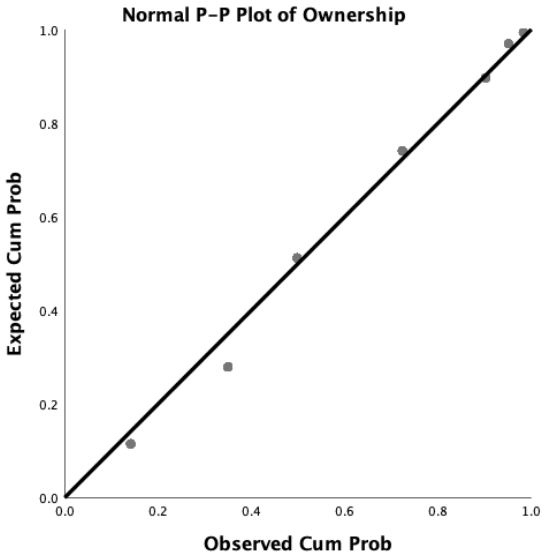
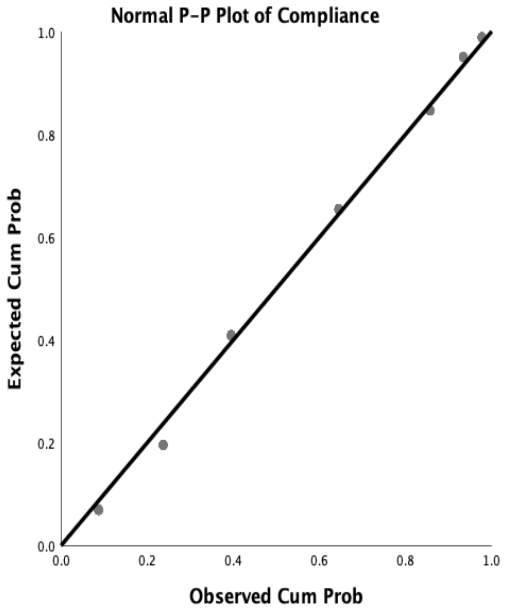



**Figure 14: Multivariate Normal P-P plot of Regression Standardised Residual for Security Compliance**



# Appendix L. Items Results Statistical Analysis

| Items | Mean | Standard Deviation | Kurtosis | Skewness |
|---|---|---|---|---|
| **TM1** | 1.778 | 0.827 | 1.734 | 1.156 |
| **TM2** | 2.274 | 0.92 | -0.7 | 0.186 |
| **TM3** | 2.688 | 1.187 | -0.626 | 0.461 |
| **TM4** | 2.056 | 0.715 | -1.042 | -0.083 |
| **TM5** | 1.925 | 0.777 | -0.899 | 0.277 |
| **SP1** | 2.105 | 0.852 | 0.508 | 0.64 |
| **SP2** | 2.237 | 0.845 | -0.365 | 0.24 |
| **SP3** | 2.162 | 0.863 | -0.359 | 0.352 |
| **SP4** | 1.959 | 0.851 | 0.439 | 0.742 |
| **SET1** | 2.086 | 0.753 | -0.236 | 0.174 |
| **SET2** | 2.82 | 1.241 | -1.032 | 0.264 |
| **SET3** | 1.741 | 0.733 | 0.968 | 0.853 |
| **SET4** | 1.695 | 0.7 | 1.979 | 1.032 |
| **RA1** | 2.32 | 0.921 | -0.034 | 0.511 |
| **RA2** | 1.65 | 0.7 | 0.502 | 0.872 |
| **RA3** | 1.744 | 0.717 | 0.949 | 0.793 |
| **EC1** | 1.639 | 0.749 | 1.401 | 1.134 |
| **EC2** | 1.602 | 0.74 | 0.888 | 1.129 |
| **EC3** | 1.744 | 0.796 | 0.87 | 0.987 |
| **JS1** | 1.887 | 0.829 | 0.59 | 0.852 |
| **JS2** | 2.004 | 0.748 | -0.488 | 0.264 |
| **JS3** | 2.921 | 1.172 | -0.882 | 0.168 |
| **JS4** | 2.169 | 0.812 | -0.088 | 0.358 |
| **JS5** | 2.335 | 1.032 | -0.06 | 0.698 |
| **JS6** | 1.827 | 0.814 | -0.008 | 0.749 |

| Items | Mean | Standard Deviation | Kurtosis | Skewness |
|---|---|---|---|---|
| **Ope1** | 1.722 | 0.617 | -0.622 | 0.263 |
| **Ope2** | 1.718 | 0.643 | -0.701 | 0.34 |
| **Ope3** | 1.853 | 0.826 | 2.251 | 1.207 |
| **Ope4** | 1.737 | 0.659 | -0.758 | 0.344 |
| **Ope5** | 1.748 | 0.699 | -0.917 | 0.393 |
| **Ope6** | 1.741 | 0.604 | -0.555 | 0.192 |
| **Ope7** | 1.658 | 0.625 | -0.664 | 0.407 |
| **Ope8** | 1.692 | 0.621 | -0.654 | 0.328 |
| **Ope9** | 3.011 | 1.418 | -1.299 | -0.036 |
| **Ope10** | 3.218 | 1.156 | -0.867 | -0.302 |
| **Agr1** | 1.853 | 0.681 | 1.514 | 0.696 |
| **Agr2** | 1.932 | 0.727 | -0.36 | 0.34 |
| **Agr3** | 1.947 | 0.658 | 0.123 | 0.295 |
| **Agr4** | 1.85 | 0.655 | -0.05 | 0.328 |
| **Agr5** | 1.959 | 0.772 | -0.082 | 0.416 |
| **Agr6** | 1.929 | 0.799 | -1.296 | 0.174 |
| **Agr7** | 2.38 | 1.063 | 0.205 | 0.724 |
| **Agr8** | 1.932 | 0.824 | 1.898 | 1.139 |
| **Agr9** | 1.951 | 0.786 | 0.446 | 0.647 |
| **Con1** | 1.782 | 0.647 | 1.713 | 0.664 |
| **Con2** | 1.805 | 0.682 | -0.567 | 0.341 |
| **Con3** | 1.883 | 0.724 | -0.461 | 0.36 |
| **Con4** | 2.038 | 0.765 | -1.042 | 0.037 |
| **Con5** | 1.992 | 0.704 | -0.601 | 0.14 |
| **Con6** | 1.917 | 0.638 | 0.097 | 0.248 |
| **Con7** | 1.838 | 0.672 | -0.207 | 0.353 |
| **Con8** | 1.981 | 0.886 | 0.043 | 0.786 |

| Items | Mean | Standard Deviation | Kurtosis | Skewness |
|---|---|---|---|---|
| **Con9** | 1.974 | 0.743 | -0.393 | 0.319 |
| **Ext1** | 2.158 | 0.724 | -0.84 | -0.13 |
| **Ext2** | 2.06 | 0.686 | -0.503 | 0.063 |
| **Ext3** | 2.154 | 0.758 | 0.109 | 0.151 |
| **Ext4** | 1.925 | 0.727 | -0.911 | 0.175 |
| **Ext5** | 2.169 | 0.708 | -0.749 | -0.128 |
| **Ext6** | 2.917 | 1.327 | -1.103 | 0.153 |
| **Ext7** | 2.553 | 1.076 | -0.258 | 0.437 |
| **Ext8** | 2.098 | 0.779 | -0.936 | 0.019 |
| **Neu1** | 3.526 | 0.97 | -0.193 | -0.522 |
| **Neu2** | 3.075 | 1.154 | -1.006 | 0.029 |
| **Neu3** | 3.218 | 1.3 | -1.133 | -0.101 |
| **Neu4** | 2.917 | 1.251 | -1.009 | 0.099 |
| **Neu5** | 3.244 | 1.021 | -0.247 | -0.164 |
| **Neu6** | 3.613 | 1.002 | -0.157 | -0.493 |
| **Neu7** | 3.218 | 1.185 | -0.834 | -0.252 |
| **Neu8** | 3.639 | 1.106 | -0.063 | -0.691 |
| **SA1** | 1.733 | 0.683 | -0.845 | 0.396 |
| **SA2** | 1.966 | 0.732 | -0.963 | 0.111 |
| **SA3** | 1.541 | 0.607 | -0.518 | 0.652 |
| **SO1** | 1.53 | 0.626 | -0.414 | 0.764 |
| **SO2** | 1.729 | 0.69 | -0.867 | 0.415 |
| **SO3** | 1.692 | 0.657 | -0.738 | 0.426 |
| **SC1** | 1.523 | 0.632 | -0.365 | 0.812 |
| **SC2** | 1.962 | 0.745 | -1.196 | 0.061 |
| **SC3** | 1.883 | 0.724 | -1.08 | 0.181 |

# Appendix M. Total-Item Correlation

**Table 1: Item-Total Correlations of Top Management**

| Item | Corrected Item-Total Correlation | Cronbach's Alpha if Item Deleted |
|---|---|---|
| TM1: Top management perceives information security as an important organisational priority. | 0.440 | 0.543 |
| TM2: In my organisation, all levels of leadership are always involved in key information security activities. | 0.494 | 0.508 |
| TM3: Top managers give strong and consistent support to the security programme. | 0.236 | 0.680 |
| TM4: Top managers provide the required resources for training and learning to enable me to comply with information security requirements. | 0.421 | 0.559 |
| TM5: The involvement and support from top management have a significant role in establishing the security culture. | 0.395 | 0.566 |

**Table 2: Item-Total Correlations of Security Policy**

| Item | Corrected Item-Total Correlation | Cronbach's Alpha if Item Deleted |
|---|---|---|
| SP1: The information security policy clearly states what is expected of me with regard to the safeguarding of information. | 0.626 | 0.738 |
| SP2: The contents of the information security policy prescribed by the organisation are easy to understand. | 0.721 | 0.690 |

| Item | Corrected Item-Total Correlation | Cronbach's Alpha if Item Deleted |
|---|---|---|
| SP3: The information security policy is applicable to the information I use in my daily tasks. | 0.657 | 0.722 |
| SP4: The written information security policy is important to create an effective security culture. | 0.445 | 0.823 |

**Table 3: Item-Total Correlations of Security Education and Training**

| Item | Corrected Item-Total Correlation | Cronbach's Alpha if Item Deleted |
|---|---|---|
| SET1: The security-related training programme explains what is expected of me, as well as the related security requirements, policies and how to behave securely from the start of employment. | 0.394 | 0.164 |
| SET2: I received adequate information security training appropriate for my daily job duties. | 0.099 | 0.553 |
| SET3: I believe that it is necessary to have security refresher training on security or any updates in the organisation. | 0.233 | 0.32 |
| SET4: The appropriate security education and training contribute to create an effective security culture. | 0.245 | 0.313 |

**Table 4: Item-Total Correlations of Risk Analysis and Assessment**

| Item | Corrected Item-Total Correlation | Cronbach's Alpha if Item Deleted |
|---|---|---|
| RA1: I believe the risk assessment processes of the organisation are adequate to identify risks that negatively impact on information security. | 0.285 | 0.745 |

| Item | Corrected Item-Total Correlation | Cronbach's Alpha if Item Deleted |
|---|---|---|
| RA2: It is important to understand the security threats, vulnerabilities, and be alerted of any risks inherent to information assets | 0.517 | 0.382 |
| RA3: The security risk analysis and assessment are important to have an effective security culture. | 0.493 | 0.408 |

**Table 5: Item-Total Correlations of Ethical Conduct**

| Item | Corrected Item-Total Correlation | Cronbach's Alpha if Item Deleted |
|---|---|---|
| EC1: It is important to have a clear ethical code of conduct and direction in protecting sensitive and confidential information by applying related regulations. | 0.693 | 0.84 |
| EC2: It is important to take care when talking about work or confidential information in public places. | 0.756 | 0.784 |
| EC3: The security-related ethical code of conduct is important for creating an effective security culture. | 0.757 | 0.782 |

**Table 6: Item-Total Correlations of Job Satisfaction**

| Item | Corrected Item-Total Correlation | Cronbach's Alpha if Item Deleted |
|---|---|---|
| JS1: I feel satisfied with the kind of work I do in this job. | 0.518 | 0.642 |

| Item | Corrected Item-Total Correlation | Cronbach's Alpha if Item Deleted |
|---|---|---|
| JS2: I feel I am being paid a fair amount of money for the work I do. | 0.480 | 0.659 |
| JS3: I am satisfied with chances for promotion and rewards. | 0.278 | 0.761 |
| JS4: I am satisfied with the benefits I receive. | 0.571 | 0.623 |
| JS5: I feel satisfied with the organisation’s level of supervision. | 0.581 | 0.606 |
| JS6: I like my co-workers. | 0.496 | 0.703 |

**Table 7: Item-Total Correlations of Extraversion**

| Item | Corrected Item-Total Correlation | Cronbach's Alpha if Item Deleted |
|---|---|---|
| PT1: Is talkative. | 0.556 | 0.404 |
| PT6: I see myself as someone who is reserved. | 0.488 | 0.431 |
| PT11: Is full of energy. | 0.526 | 0.408 |

| Item | Corrected Item-Total Correlation | Cronbach's Alpha if Item Deleted |
|---|---|---|
| PT16: Generate a loaf of enthusiasm. | 0.446 | 0.439 |
| PT21: Tends to be quit. | 0.420 | 0.449 |
| PT26: Has assertive responsibility. | -0.229 | 0.734 |
| PT31: Is sometimes shy, inhibited. | -0.013 | 0.608 |
| PT36: I see myself as someone who is outgoing, sociable. | 0.526 | 0.405 |

**Table 8: Item-Total Correlations of Agreeableness**

| Item | Corrected Item-Total Correlation | Cronbach's Alpha if Item Deleted |
|---|---|---|
| PT2: I see myself as someone who tends to find fault with others. | 0.610 | 0.738 |
| PT7: Is helpful and unselfish with others. | 0.639 | 0.732 |
| PT12: Starts quarrels with others. | 0.538 | 0.748 |

| Item | Corrected Item-Total Correlation | Cronbach's Alpha if Item Deleted |
|---|---|---|
| PT17: Has a forgiving nature. | 0.517 | 0.750 |
| PT22: I see myself as someone who is generally trusting. | 0.533 | 0.746 |
| PT27: Can be cold and aloof. | 0.244 | 0.787 |
| PT32: I see myself as someone who is considerate and kind to almost everyone. | 0.201 | 0.810 |
| PT37: Is sometimes rude to others. | 0.533 | 0.745 |
| PT42: Likes to cooperate with others. | 0.540 | 0.744 |

**Table 9: Item-Total Correlations of Openness**

| Item | Corrected Item-Total Correlation | Cronbach's Alpha if Item Deleted |
|---|---|---|
| PT5: Is original, comes up with ideas. | 0.664 | 0.640 |
| PT10: Is curious about many different things. | 0.371 | 0.679 |

| Item | Corrected Item-Total Correlation | Cronbach's Alpha if Item Deleted |
|---|---|---|
| PT15: Is ingenious, a deep thinker. | 0.337 | 0.682 |
| PT20: I see myself as someone who has an active imagination. | 0.558 | 0.652 |
| PT25: Is inventive. | 0.574 | 0.647 |
| PT30: Values artistic, a esthtics. | 0.521 | 0.660 |
| PT35: Prefers work that is routine. | 0.458 | 0.668 |
| PT40: Likes to reflect, play with ideas. | 0.561 | 0.654 |
| PT41: I see myself as someone who has few artistic interests. | 0.180 | 0.751 |
| PT44: Is sophisticated in art, music or literature. | 0.077 | 0.749 |

**Table 10: Item-Total Correlations of Conscientiousness**

| Item | Corrected Item-Total Correlation | Cronbach's Alpha if Item Deleted |
|---|---|---|
| PT3: I see myself as someone who does a thorough job. | 0.453 | 0.830 |
| PT8: Can be somewhat careless. | 0.639 | 0.811 |

| Item | Corrected Item-Total Correlation | Cronbach's Alpha if Item Deleted |
|---|---|---|
| PT13: Is a reliable worker. | 0.602 | 0.815 |
| PT18: Tends to be disorganised. | 0.626 | 0.812 |
| PT23: I see myself as someone who tends to be lazy. | 0.625 | 0.812 |
| PT28: Preservers until the task is finished. | 0.660 | 0.810 |
| PT33: Does things efficiently. | 0.558 | 0.820 |
| PT38: Makes plans and follows through with them. | 0.421 | 0.839 |
| PT43: Is easily distracted. | 0.411 | 0.836 |

**Table 11: Item-Total Correlations of Neuroticism**

| Item | Corrected Item-Total Correlation | Cronbach's Alpha if Item Deleted |
|---|---|---|
| PT4: Is depressed blue. | 0.457 | 0.904 |
| PT9: I see myself as someone who is relaxed, handles stress well. | 0.783 | 0.876 |

| Item | Corrected Item-Total Correlation | Cronbach's Alpha if Item Deleted |
|---|---|---|
| PT14: Can be tense. | 0.708 | 0.884 |
| PT19: Worries a lot. | 0.744 | 0.880 |
| PT24: Is emotionally stable, not easily upset. | 0.660 | 0.888 |
| PT29: Can be moody. | 0.665 | 0.888 |
| PT34: Remains calm in tense situations. | 0.806 | 0.874 |
| PT39: I see myself as someone who gets nervous easily. | 0.646 | 0.889 |

**Table 12: Item-Total Correlations of Security Awareness**

| Item | Corrected Item-Total Correlation | Cronbach's Alpha if Item Deleted |
|---|---|---|
| SA1: I am aware of the information security policies and security aspects relating to my job, for example, a password policy. | 0.509 | 0.516 |
| SA2: I am aware of ongoing initiatives about security awareness. | 0.466 | 0.581 |

| Item | Corrected Item-Total Correlation | Cronbach's Alpha if Item Deleted |
|---|---|---|
| S3: It is important to raise awareness about information security with employees. | 0.452 | 0.596 |

**Table 13: Item-Total Correlations of Security Ownership**

| Item | Corrected Item-Total Correlation | Cronbach's Alpha if Item Deleted |
|---|---|---|
| SO1: Protecting information security is the responsibility of every employee. | 0.547 | 0.726 |
| SO2: It is important that individuals are involved in the development of security policies. | 0.590 | 0.680 |
| SO3: It is important to have a sense of ownership regarding the organisational security. | 0.639 | 0.623 |

**Table 14: Item-Total Correlations of Security Compliance**

| Item | Corrected Item-Total Correlation | Cronbach's Alpha if Item Deleted |
|---|---|---|
| SC1: It is important to follow the information security policies and practices such as not sharing passwords to enhance the security culture. | 0.451 | 0.516 |
| SC2: The organisation enforces adherence to the information security policy. | 0.431 | 0.538 |
| SC3: I believe that the attention should be drawn on incidents of not adhering to the security policies and requirements. | 0.432 | 0.534 |

# Appendix N. Items Cross Loading

| | Agr | Con | EC | Ext | JS | Neu | Ope | RA | SA | SC | SET | SO | SP | TM |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Agr1** | **0.811** | 0.221 | 0.210 | 0.006 | 0.113 | 0.050 | 0.235 | 0.210 | 0.244 | 0.315 | 0.209 | 0.330 | 0.155 | 0.217 |
| **Agr2** | **0.814** | 0.173 | 0.226 | 0.002 | 0.076 | -0.05 | 0.262 | 0.152 | 0.231 | 0.215 | 0.160 | 0.240 | 0.069 | 0.128 |
| **Agr3** | **0.703** | 0.192 | 0.166 | 0.068 | 0.078 | -0.04 | 0.207 | 0.131 | 0.158 | 0.181 | 0.078 | 0.240 | 0.043 | 0.079 |
| **Agr4** | **0.550** | 0.045 | 0.158 | 0.064 | 0.158 | -0.04 | 0.150 | 0.097 | 0.179 | 0.140 | 0.105 | 0.136 | 0.139 | 0.067 |
| **Agr5** | **0.658** | 0.157 | 0.181 | -0.04 | 0.060 | 0.029 | 0.052 | 0.236 | 0.185 | 0.179 | 0.136 | 0.208 | 0.172 | 0.094 |
| **Agr6** | **0.440** | 0.120 | 0.200 | -0.05 | 0.049 | 0.035 | 0.070 | 0.091 | 0.104 | 0.149 | 0.182 | 0.061 | 0.130 | 0.140 |
| **Agr7** | **0.450** | 0.168 | 0.156 | -0.06 | 0.118 | 0.050 | 0.146 | 0.072 | 0.091 | 0.204 | 0.162 | 0.070 | 0.123 | 0.045 |
| **Agr8** | **0.762** | 0.147 | 0.212 | -0.05 | 0.100 | 0.040 | 0.158 | 0.165 | 0.193 | 0.253 | 0.176 | 0.266 | 0.127 | 0.193 |
| **Agr9** | **0.745** | 0.155 | 0.231 | -0.05 | 0.020 | 0.000 | 0.225 | 0.133 | 0.256 | 0.192 | 0.159 | 0.231 | 0.064 | 0.109 |
| **Con1** | 0.258 | **0.717** | 0.265 | 0.092 | 0.175 | -0.03 | 0.396 | 0.240 | 0.207 | 0.323 | 0.281 | 0.327 | 0.213 | 0.118 |
| **Con2** | 0.156 | **0.730** | 0.180 | 0.088 | 0.103 | -0.01 | 0.195 | 0.171 | 0.109 | 0.186 | 0.138 | 0.201 | 0.107 | 0.004 |
| **Con3** | 0.071 | **0.693** | 0.113 | 0.069 | 0.062 | -0.09 | 0.149 | 0.082 | 0.091 | 0.141 | 0.157 | 0.162 | 0.113 | 0.000 |
| **Con4** | 0.042 | **0.679** | 0.049 | -0.01 | 0.045 | -0.12 | 0.087 | 0.093 | 0.087 | 0.147 | 0.129 | 0.208 | 0.108 | 0.078 |
| **Con5** | 0.063 | **0.644** | 0.010 | 0.024 | -0.03 | -0.14 | -0.01 | 0.008 | -0.03 | 0.067 | 0.111 | 0.161 | 0.079 | 0.032 |
| **Con6** | 0.156 | **0.772** | 0.074 | 0.067 | 0.009 | -0.14 | 0.081 | 0.104 | 0.128 | 0.186 | 0.191 | 0.175 | 0.143 | 0.085 |
| **Con7** | 0.215 | **0.730** | 0.118 | 0.048 | 0.006 | -0.04 | 0.172 | 0.135 | 0.149 | 0.180 | 0.148 | 0.167 | 0.112 | 0.106 |
| **Con8** | 0.130 | **0.452** | 0.129 | 0.051 | 0.045 | 0.024 | 0.050 | 0.210 | 0.156 | 0.170 | 0.133 | 0.210 | 0.143 | 0.108 |
| **Con9** | 0.140 | **0.410** | 0.136 | 0.019 | 0.023 | 0.032 | 0.073 | 0.082 | 0.145 | 0.140 | 0.121 | 0.300 | 0.130 | 0.215 |
| **EC1** | 0.195 | 0.171 | **0.856** | 0.140 | 0.191 | 0.013 | 0.237 | 0.456 | 0.416 | 0.528 | 0.403 | 0.406 | 0.321 | 0.381 |
| **EC2** | 0.232 | 0.121 | **0.898** | 0.176 | 0.214 | -0.05 | 0.202 | 0.492 | 0.454 | 0.538 | 0.448 | 0.468 | 0.408 | 0.336 |
| **EC3** | 0.299 | 0.230 | **0.896** | 0.150 | 0.266 | -0.03 | 0.315 | 0.533 | 0.454 | 0.518 | 0.500 | 0.449 | 0.463 | 0.378 |
| **Ext1** | -0.028 | 0.036 | 0.108 | **0.721** | 0.057 | 0.106 | 0.069 | 0.116 | 0.104 | 0.140 | 0.033 | 0.029 | 0.104 | 0.059 |
| **Ext2** | 0.069 | 0.112 | 0.096 | **0.767** | 0.053 | -0.04 | 0.084 | 0.058 | 0.070 | 0.164 | 0.015 | 0.024 | 0.033 | 0.057 |
| **Ext3** | -0.014 | 0.055 | 0.085 | **0.751** | 0.018 | 0.042 | 0.130 | 0.056 | 0.108 | 0.118 | 0.047 | -0.06 | 0.120 | 0.001 |
| **Ext4** | 0.011 | 0.085 | 0.200 | **0.800** | 0.062 | 0.026 | 0.085 | 0.058 | 0.113 | 0.191 | 0.063 | 0.038 | 0.097 | 0.101 |
| **Ext5** | 0.002 | 0.049 | 0.150 | **0.802** | 0.056 | 0.057 | 0.091 | 0.117 | 0.209 | 0.152 | 0.067 | 0.028 | 0.153 | 0.031 |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Ext6** | 0.013 | 0.035 | 0.200 | **0.403** | 0.053 | -0.04 | 0.084 | 0.058 | 0.070 | 0.164 | 0.015 | 0.024 | 0.033 | 0.057 |
| **Ext7** | 0.020 | 0.057 | 0.168 | **0.424** | 0.033 | 0.020 | 0.190 | 0.042 | 0.134 | 0.126 | 0.025 | 0.055 | 0.137 | 0.066 |
| **Ext8** | -0.056 | 0.042 | 0.129 | **0.752** | 0.019 | 0.039 | 0.140 | 0.019 | 0.032 | 0.131 | 0.034 | 0.003 | 0.067 | 0.043 |
| **JS1** | 0.082 | 0.102 | 0.198 | 0.049 | **0.775** | -0.02 | 0.236 | 0.197 | 0.319 | 0.315 | 0.232 | 0.275 | 0.327 | 0.301 |
| **JS2** | 0.160 | 0.067 | 0.191 | 0.041 | **0.708** | -0.06 | 0.146 | 0.216 | 0.293 | 0.287 | 0.230 | 0.271 | 0.283 | 0.278 |
| **JS3** | 0.050 | 0.044 | 0.101 | 0.022 | **0.380** | -0.04 | 0.129 | 0.250 | 0.232 | 0.250 | 0.216 | 0.219 | 0.266 | 0.800 |
| **JS4** | 0.056 | 0.037 | 0.183 | 0.114 | **0.705** | 0.008 | 0.114 | 0.245 | 0.177 | 0.273 | 0.192 | 0.206 | 0.207 | 0.246 |
| **JS5** | -0.020 | 0.044 | 0.198 | 0.053 | **0.784** | 0.012 | 0.213 | 0.233 | 0.119 | 0.334 | 0.186 | 0.219 | 0.340 | 0.278 |
| **JS6** | 0.122 | 0.103 | 0.163 | -0.06 | **0.709** | -0.07 | 0.271 | 0.180 | 0.229 | 0.322 | 0.216 | 0.263 | 0.316 | 0.212 |
| **Neu1** | 0.139 | -0.046 | 0.100 | 0.016 | 0.030 | **0.460** | 0.056 | 0.046 | -0.03 | 0.045 | 0.210 | 0.037 | 0.034 | 0.025 |
| **Neu2** | 0.061 | -0.112 | -0.020 | -0.11 | -0.02 | **0.877** | 0.038 | -0.03 | -0.03 | -0.09 | -0.11 | -0.09 | -0.01 | -0.014 |
| **Neu3** | 0.050 | -0.087 | -0.040 | 0.012 | 0.024 | **0.854** | 0.003 | -0.03 | -0.07 | -0.08 | -0.06 | -0.06 | -0.01 | 0.013 |
| **Neu4** | -0.055 | -0.109 | 0.030 | 0.044 | -0.06 | **0.818** | 0.023 | 0.054 | -0.02 | -0.03 | -0.06 | -0.07 | 0.054 | 0.027 |
| **Neu5** | -0.025 | -0.080 | -0.071 | 0.083 | -0.06 | **0.863** | 0.037 | -0.08 | -0.15 | -0.07 | -0.12 | -0.12 | -0.10 | -0.010 |
| **Neu6** | 0.050 | -0.092 | -0.027 | 0.012 | 0.018 | **0.400** | 0.021 | 0.032 | -0.03 | 0.066 | 0.234 | 0.053 | 0.043 | 0.010 |
| **Neu7** | 0.025 | -0.053 | 0.080 | 0.055 | -0.03 | **0.851** | 0.044 | -0.04 | 0.001 | -0.02 | -0.09 | -0.06 | -0.08 | 0.092 |
| **Neu8** | 0.050 | -0.092 | -0.027 | 0.012 | 0.018 | **0.415** | 0.060 | 0.034 | 0.020 | -0.04 | -0.07 | -0.02 | 0.053 | 0.030 |
| **Ope1** | 0.217 | 0.135 | 0.206 | 0.078 | 0.226 | -0.02 | **0.840** | 0.192 | 0.177 | 0.251 | 0.171 | 0.252 | 0.148 | 0.125 |
| **Ope2** | 0.262 | 0.456 | 0.294 | 0.145 | 0.217 | 0.039 | **0.592** | 0.243 | 0.250 | 0.376 | 0.268 | 0.297 | 0.211 | 0.157 |
| **Ope3** | 0.170 | 0.135 | 0.150 | 0.090 | 0.230 | -0.02 | **0.434** | 0.216 | 0.164 | 0.248 | 0.117 | 0.101 | 0.236 | 0.127 |
| **Ope4** | 0.145 | 0.164 | 0.204 | 0.091 | 0.150 | 0.021 | **0.729** | 0.153 | 0.201 | 0.197 | 0.147 | 0.189 | 0.229 | 0.100 |
| **Ope5** | 0.190 | 0.049 | 0.085 | 0.046 | 0.181 | 0.041 | **0.727** | 0.106 | 0.098 | 0.132 | 0.076 | 0.147 | 0.121 | 0.016 |
| **Ope6** | 0.112 | 0.085 | 0.226 | 0.096 | 0.191 | -0.05 | **0.711** | 0.173 | 0.136 | 0.210 | 0.187 | 0.162 | 0.245 | 0.140 |
| **Ope7** | 0.127 | 0.097 | 0.146 | 0.041 | 0.123 | 0.019 | **0.615** | 0.066 | 0.170 | 0.197 | 0.126 | 0.200 | 0.147 | 0.099 |
| **Ope8** | 0.168 | 0.130 | 0.147 | 0.045 | 0.220 | -0.03 | **0.764** | 0.163 | 0.162 | 0.202 | 0.137 | 0.238 | 0.148 | 0.080 |
| **Ope9** | 0.173 | 0.261 | 0.130 | 0.030 | 0.140 | 0.056 | **0.421** | 0.105 | 0.150 | 0.140 | 0.125 | 0.140 | 0.133 | 0.060 |
| **Ope1** | 0.113 | 0.160 | 0.300 | 0.080 | 0.130 | -0.11 | **0.510** | 0.170 | 0.122 | 0.243 | 0.187 | 0.162 | 0.255 | 0.032 |
| **RA1** | 0.112 | 0.031 | 0.221 | 0.077 | 0.144 | 0.072 | 0.230 | **0.510** | 0.256 | 0.275 | 0.254 | 0.209 | 0.305 | 0.279 |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **RA2** | 0.172 | 0.173 | 0.521 | 0.099 | 0.264 | -0.05 | 0.146 | **0.877** | 0.492 | 0.542 | 0.477 | 0.490 | 0.388 | 0.371 |
| **RA3** | 0.219 | 0.207 | 0.478 | 0.073 | 0.224 | -0.10 | 0.211 | **0.855** | 0.421 | 0.516 | 0.481 | 0.472 | 0.279 | 0.326 |
| **SA1** | 0.244 | 0.158 | 0.368 | 0.119 | 0.260 | -0.01 | 0.214 | 0.364 | **0.797** | 0.453 | 0.358 | 0.431 | 0.524 | 0.449 |
| **SA2** | 0.120 | 0.073 | 0.314 | 0.116 | 0.228 | 0.020 | 0.141 | 0.325 | **0.714** | 0.339 | 0.363 | 0.276 | 0.421 | 0.389 |
| **SA3** | 0.277 | 0.171 | 0.457 | 0.120 | 0.253 | -0.15 | 0.227 | 0.505 | **0.801** | 0.522 | 0.527 | 0.539 | 0.363 | 0.359 |
| **SC1** | 0.249 | 0.250 | 0.584 | 0.138 | 0.334 | -0.17 | 0.267 | 0.623 | 0.544 | **0.824** | 0.482 | 0.643 | 0.378 | 0.402 |
| **SC2** | 0.242 | 0.221 | 0.371 | 0.163 | 0.302 | 0.022 | 0.291 | 0.376 | 0.399 | **0.736** | 0.349 | 0.410 | 0.476 | 0.474 |
| **SC3** | 0.186 | 0.153 | 0.361 | 0.167 | 0.311 | -0.01 | 0.216 | 0.311 | 0.334 | **0.703** | 0.346 | 0.323 | 0.290 | 0.342 |
| **SET1** | 0.189 | 0.165 | 0.275 | 0.024 | 0.279 | 0.004 | 0.131 | 0.267 | 0.406 | 0.345 | **0.659** | 0.349 | 0.472 | 0.454 |
| **SET2** | 0.170 | 0.216 | 0.010 | 0.202 | 0.140 | 0.043 | 0.110 | 0.260 | 0.145 | 0.613 | **0.430** | 0.221 | 0.320 | 0.200 |
| **SET3** | 0.099 | 0.167 | 0.371 | 0.091 | 0.143 | -0.11 | 0.160 | 0.394 | 0.395 | 0.385 | **0.736** | 0.323 | 0.267 | 0.244 |
| **SET4** | 0.166 | 0.222 | 0.463 | 0.019 | 0.213 | -0.11 | 0.236 | 0.523 | 0.396 | 0.421 | **0.788** | 0.376 | 0.322 | 0.300 |
| **SO1** | 0.271 | 0.304 | 0.491 | 0.102 | 0.328 | -0.10 | 0.283 | 0.520 | 0.511 | 0.601 | 0.469 | **0.815** | 0.414 | 0.430 |
| **SO2** | 0.267 | 0.220 | 0.384 | -0.08 | 0.246 | -0.08 | 0.236 | 0.384 | 0.425 | 0.493 | 0.339 | **0.812** | 0.366 | 0.375 |
| **SO3** | 0.287 | 0.219 | 0.348 | 0.031 | 0.259 | -0.09 | 0.261 | 0.410 | 0.423 | 0.454 | 0.366 | **0.838** | 0.315 | 0.362 |
| **SP1** | 0.118 | 0.118 | 0.393 | 0.106 | 0.344 | 0.004 | 0.189 | 0.303 | 0.485 | 0.386 | 0.370 | 0.371 | **0.803** | 0.435 |
| **SP2** | 0.073 | 0.139 | 0.317 | 0.042 | 0.348 | -0.04 | 0.195 | 0.325 | 0.427 | 0.383 | 0.326 | 0.335 | **0.852** | 0.531 |
| **SP3** | 0.076 | 0.131 | 0.282 | 0.158 | 0.325 | -0.03 | 0.171 | 0.227 | 0.422 | 0.342 | 0.372 | 0.306 | **0.804** | 0.468 |
| **SP4** | 0.194 | 0.215 | 0.412 | 0.098 | 0.257 | 0.001 | 0.249 | 0.432 | 0.422 | 0.462 | 0.444 | 0.384 | **0.694** | 0.417 |
| **TM1** | 0.136 | 0.108 | 0.365 | 0.102 | 0.265 | -0.02 | 0.131 | 0.368 | 0.448 | 0.466 | 0.323 | 0.439 | 0.492 | **0.757** |
| **TM2** | 0.098 | 0.042 | 0.289 | 0.086 | 0.274 | -0.02 | 0.097 | 0.250 | 0.314 | 0.373 | 0.251 | 0.306 | 0.459 | **0.751** |
| **TM4** | 0.123 | -0.003 | 0.207 | -0.04 | 0.234 | 0.008 | 0.098 | 0.214 | 0.307 | 0.317 | 0.313 | 0.266 | 0.378 | **0.673** |
| **TM5** | 0.170 | 0.112 | 0.284 | 0.003 | 0.249 | 0.048 | 0.116 | 0.343 | 0.364 | 0.337 | 0.414 | 0.308 | 0.322 | **0.663** |