2017

A Model for Monitoring End-User Security Policy Compliance

Alotaibi, Mutlaq

A Model for Monitoring End-User Security Policy Compliance

by

Mutlaq J. Alotaibi

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

DOCTOR OF PHILOSOPHY

School of Computing, Electronics and Mathematics

Faculty of Science and Engineering

July 2017

COPYRIGHT STATEMENT

A Model for Monitoring End-User Security Policy Compliance

By

Mutlaq J. Alotaibi

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

DOCTOR OF PHILOSOPHY

School of Computing, Electronics and Mathematics

Faculty of Science and Engineering

July 2017

Abstract

A Model for Monitoring Security Policy Compliance

Mutlaq Alotaibi

Organisations increasingly perceive their employees as a great asset that needs to be cared for; however, at the same time, they view employees as one of the biggest potential threats to their cyber security. Organizations repeatedly suffer harm from employees who are not obeying or complying with their information security policies. Non-compliance behaviour of an employee, either unintentionally or intentionally, pose a real threat to an organization's information security. As such, more thought is needed on how to encourage employees to be security compliant and more in line with a security policy of their organizations.

Based on the above, this study has proposed a model that is intended to provide a comprehensive framework for raising the level of compliance amongst end-users, with the aim of monitoring, measuring and responding to users' behaviour with an information security policy. The proposed approach is based on two main concepts: a taxonomy of the response strategy to non-compliance behaviour, and a compliance points system. The response taxonomy is comprised of two categories: awareness raising and enforcement of the security policy. The compliance points system is used to reward compliant behaviour, and penalise noncompliant behaviour.

A prototype system has been developed to simulates the proposed model in order to provide a clear image of its functionalities and how it is meant to work. Therefore, it was developed to work as a system that responds to the behaviour of users (whether violation or compliance behaviour) in relation to the information security policies of their organisations. After designing the proposed model and simulating it using the prototype system, it was significant to evaluate the model by interviewing different experts with different backgrounds from academic and industry sectors. Thus, the interviewed experts agreed that the identified research problem is a real problem that needs to be researched and solutions need to be devised. It also can be stated that the overall feedback of the interviewed experts about the proposed model was very encouraging and positive. The expert participants thought that the proposed model addresses the research gap, and offers a novel approach for managing the information security policies.

Table of Contents

List of Tables

List of Figures

Acknowledgements

First and foremost, I give honour and praise to Allah the Almighty for giving me strength and enabling me to complete this important stage of my life.

In addition, I wish to express my heartfelt appreciation to beloved parents for their kindness and providing me with an abundance of love and support. I can never thank them enough for what they have done for me, may Allah bless them with good health. In this same vein, very deep and special thanks go to my wife, son and daughter, of whom have unfailingly given endless patience, love and support through the PhD journey. To my brothers and sisters, I am grateful for your endless support and help.

Of course, I would like to express my honest gratitude to my Director of Studies, Professor Steven Furnell for providing me with a wealth of help and support during this amazing journey, really this work would have never been completed without his support. I also wish to thank my second supervisor Professor Nathan Clarke for his time and efforts in making the PhD journey easier and better.

I acknowledge with grateful the government of Saudi Arabia, the Minister of Interior, for granting me the scholarship and sponsoring my undertaking of this PhD programme.

Lastly, I would like to thank Plymouth University and special thanks to my colleagues and friends at the Centre for Security, Communication and Network Research.

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 Graduate Committee. Work submitted for this research degree at the Plymouth University has not formed part of any other degree either at Plymouth University or at another establishment. Relevant scientific seminars and conferences were regularly attended at which work was often presented and several papers prepared for publication.

Word count of the main body of thesis: 52,703

Signed _____

Date_____

Chapter One

Introduction

1. Introduction

1.1 Introduction

Information management and its processes have become a significant aspect of modern organisations (Soomro et al. 2016). Both practitioners and researchers are currently concentrating their efforts on information security. The weakest link in the field of information security that has been identified in the literature is the end users (Badie and Lashkari 2012; Al-Omari et al. 2011). Modern organisations value the importance of information security since their daily work has become more and more dependent on their information systems. Thus, organisations self-invest by implementing proper security measures to tackle the different kinds of threats to their security. However, this investment will not deliver the expected returns if the awareness of employees regarding potential security threats is not raised (Bulgurcu et al. 2009). Therefore, as a first line of defence many organisations have implemented information security policies to manage the security of their information assets (Soomro et al. 2016).

Information security policy compliance is one of the main challenges facing organisations today. Although implementing technical and procedural measures clearly helps to improve an organisation's information security, the human factor or the employees' compliance with these measures is the key to success (Furnell & Clarke 2012). However, organisations are now having some issues regarding the extent of employee adherence to policy. According to PwC (2015), three-quarters of large organisations suffered a staff-related breach and nearly one-third of small organisations had a similar occurrence.

Threats from non-compliance of employees with information security policy fall into two categories: unintentional and malicious. In the former category, the threats occur accidently

or due to negligence and are typically attributed to a lack of awareness or carelessness. For example, misbehaving employees can create vulnerabilities by installing unreliable software, which is infected by spyware or a Trojan horse that may enable an external attacker to gain internal access to confidential data (Crossler et al. 2013). In the latter category, the malicious insider, a user abuses his knowledge of the systems or networks to intentionally cause damage. An example of this is when a user exploits his privilege to illegally access sensitive data.

Consequently, non-compliant employees or those who are unaware of information security policy have become a major concern to organisations since they pose a threat to the computing environment security. In Ernst & Young (EY) survey results (2013), 57% of the surveyed organisations considered their employees to be the biggest threat to information security, whilst 38% indicated that unaware or careless employees pose the greatest threat. Moreover, 70% of organisations where security policy was poorly understood had staff-related breaches, whereas only 41% of organisations where the policy was well understood had the same (PwC 2014).

Many factors directly or indirectly shape employees' behaviour and attitudes in relation to complying with the security policies in their organisations, for instance, awareness, education, culture, security monitoring tools, social factors, etc. All these factors can motivate users to comply with security policy. The literature frequently refers to work performed in this domain that aims to shed light on all the factors and their causes and effects.

Lastly, in order to strengthen the human factor, which is the weakest link in the security chain, more consideration should be given to information security policy compliance. Actually, 72% of large and 63% of organisations have provided on-going security awareness

training for their staff (PwC 2015). However, the problem of employees being unaware of their responsibilities in relation to information security is still an open issue.

1.2 Aims & Objectives

This study aims to review the information security policies domain and investigate the obstacles and issues associated with the extent of employee compliance with such security policies. The project seeks to enhance end user adherence to information security policies by proposing a framework for security policy compliance monitoring and targeted awareness raising. This is intended to be achieved through the following objectives:

- **Objective 1:** To assess the state-of-the-art in relation to information security policy usage and compliance, including the problems associated with these policies and the available solutions.
- **Objective 2:** From previous literature understand the issues that surround effective information security awareness.
- **Objective 3:** Reviewing the potential behaviours of users with an information security policy as well as factors that influence their behaviours.
- **Objective 4:** Propose a novel model that aims at enhancing the compliance level of users.
- **Objective 5:** Developing a prototype system to simulate the proposed model using several scenarios.
- **Objective 6:** To conduct a series of expert-based evaluations involving experts from different backgrounds, academic and industry, to gain an insight into the practical effectiveness of the proposed model.

Part of the work presented in this thesis has been already published in a series of peer-reviewed publications, as listed below:

- M. Alotaibi, S. Furnell and N. Clarke, ‘’ TOWARDS DYNAMIC ADAPTION OF USER'S ORGANISATIONAL INFORMATION SECURITY BEHAVIOUR ‘’ In Australian Information Security Management Conference, Australia, 2015, pp. 28-36

- M. Alotaibi, S. Furnell and N. Clarke, ‘’ Information Security Policies: A Review of Challenges and Influencing Factors ‘’In Internet Technology and Secured Transactions (ICITST), Spain, 2016 11th International Conference for (pp. 352-358). IEEE.

- M. Alotaibi, S. Furnell and N. Clarke, ‘’A Novel Model for Monitoring Security Policy Compliance ‘’, Journal of Internet Technology and Secured Transactions (JITST),

1.3 Thesis Overview

In order to address the aforementioned objectives, the remainder of the thesis is organised into a further seven chapters.

The second chapter describes state-of-the-art information security policies with the aim of developing a thorough understanding of them. Types of information security policies and types of information security policy users are both discussed. It looks closely at the current extent of use of information security policies by organisations. Furthermore, approaches used in policy enforcement and monitoring are covered by this chapter. In addition, it provides an overview of some of the current key issues and challenges related to information security policy.

The third chapter presents a review of the literature on information security awareness. It also provides an overview of the current methods used to raise information security awareness, discussing both their advantages and disadvantages. This chapter concludes by outlining persuasive technology and its great value in the information security awareness area.

The fourth chapter discusses user behaviour in relation to information security policy, presenting all the significant behaviours. It then addresses insider threats in more detail in order to gain a thorough understanding of this term. Lastly, the chapter explains the factors that influence user behaviour that is either compliant or non-compliant with such information security policies.

The fifth chapter presents a novel model for monitoring security policy compliance. The novelty of the proposed model depends upon three significant aspects: monitoring, response taxonomy and using a compliance points system. This chapter provides detailed information regarding the model by explaining the main concepts including, the response taxonomy for non-compliance behaviour and using the compliance points system, and to theoretically clarify how it can be implemented. The main concept and idea behind the model is illustrated in this chapter, explaining the details of how it works.

The sixth chapter shows a prototype system that simulates the proposed model in order to provide a clear image of its functionalities and how it is meant to work. The chapter begins by introducing the platform or the environment used to design and program the prototype system. Then some scenarios of potential user behaviour in relation to the information security policies used in the simulation process are explained. Lastly, the prototype system, the simulation process and the results of the simulation, data and charts are illustrated and discussed in more detail during this chapter.

The seventh chapter discusses the evaluation process of the research. The main objective behind this evaluation is to gain quantitative feedback received from experts from different sectors including industry and academic. The chapter begins with an explanation of the evaluation method used and its scope in general as well as the justification of the selected method. A further section gives more details about the experts who participated in this

evaluation and basis of selection them as experts in the field. Finally, the findings of the evaluation process alongside with the experts' feedback is discussed in this chapter.

The eighth chapter highlights the main conclusions of the research. The achievements and limitations of the research are discussed. The chapter also presents a summary of the potential further work as a direction for future research.

Chapter Two

Information Security Policy

2. Information Security Policy

2.1 Introduction

Many researchers have identified computer end users as the weakest link in the information security chain (Bashorun et al. 2013; Da Veiga & Eloff 2010; Siponen et al. 2014; Sohrabi Safa et al. 2016). Therefore, information security policy is considered to be the cornerstone of information security management and an organizational approach that mitigates potential threats from employees. In the workplace, all employees should be made aware of acceptable and unacceptable user behaviour and the first step to achieving this is to implement a proper formal information security policy. Obviously, organizations should realize that having security policies is as significant as having a firewall, intrusion detection system or any other security solutions.

The main aim of this chapter is to provide a comprehensive overview of information security policy and the current practice and experiences related to it, as documented in the literature. A further aim is to investigate the current extent of use of security policies in organizations and the approaches used to assist in policy compliance monitoring. Lastly, key security policy related issues and challenges will also be discussed in this chapter.

2.2 An Overview of Information Security Policy

Security policy is defined in a formal document that addresses acceptable and unacceptable behaviour of users in relation to dealing with information assets in a secure manner (Peltier 2001). It is a part of formal information security control and a baseline statement of the information security tasks which should be followed by the employees. According to SANS (2014), a security policy is typically "*a document that outlines specific requirements or rules that must be met. In the information/network security realm, policies are usually point-specific, covering a single area*". Also, NIST SP 800-53 (2006) defined a security policy as

"*an aggregate of directives, rules, and practices that prescribes how an organization manages, protects, and distributes information*". Knapp et al. (2009) stated that organizations must realize that having policies, processes and procedures is as important as having a firewall, an intrusion detection system, a VPN or any other technical solution. Therefore, implementing such technical measures alone cannot guarantee having a safe environment. Actually, the importance of policies, processes and procedures is more prominent when tackling internal threats or trying to reduce the possibility of incidents that can harm the availability or integrity of the organization's data *(*Knapp et al. 2009) .

As implementation guidance, organizations should establish a set of information security policies, which are approved by top management and distributed and communicated to all employees (ISO 2013). Essentially, an organization needs to identify its security requirements prior to developing its information security policy. Therefore, having a comprehensive perception of the information security requirements can play a significant role in designing proper information security policies that cover all the concerned issues. According to ISO (2013), there are three major sources of the necessary information on security requirements:

- Risk assessments or evaluations of potential risks to the organization and overall business objectives and strategies should be taken into account in this process. Therefore, through a risk assessment, possible threats to the computing environment are identified, the likelihood of occurrence is estimated and the potential impact of the threats is evaluated.
- The legal, regulatory and contractual requirements that an organization and its partners, such as contractors and service providers, need to adhere to and their socio-cultural environment.

- An organization's vision regarding dealing with information assets and the business requirements for information handling, such as storing, processing and communicating, that has been developed by the organization.

For example, the following framework (Figure 2.1) supports the comprehensive process of information security policy and illustrates its elements. In this framework, it can be seen that security policy is influenced by two sources: internal influence, such as management support, and external influence, such as technology advances. Overall, the process of information security policy management includes: risk assessment, development of policy, approval, training and awareness, policy implementation, monitoring, policy enforcement and policy review.

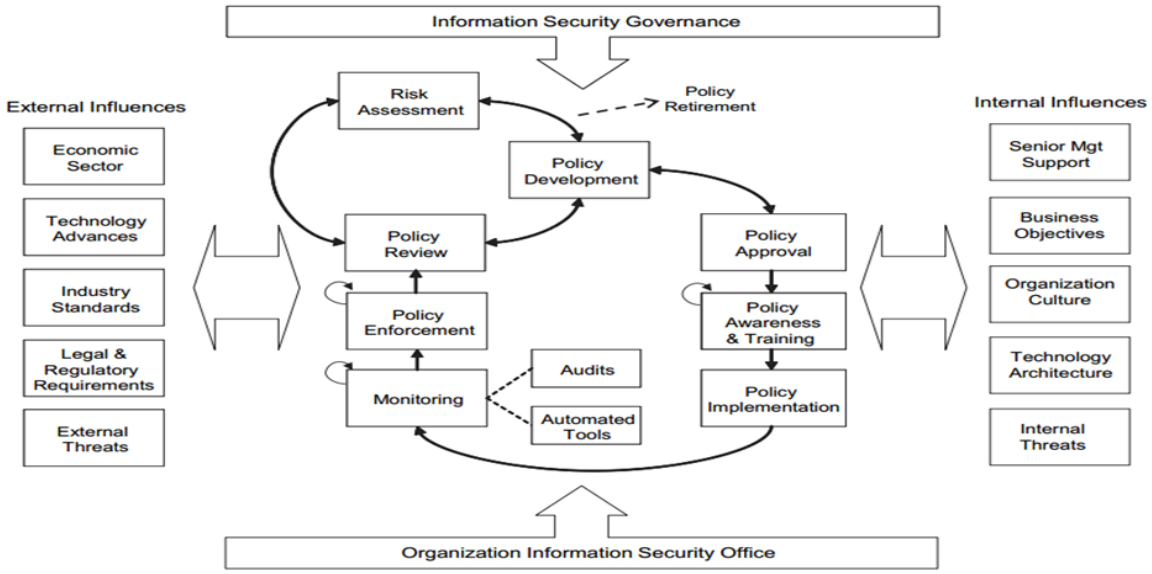


Figure 2.1 Comprehensive information security policy process model (Knapp et al. 2009)

To mitigate the threats to information assets, organizations can use different information security best practices and well-known procedures, which include implementing information security controls or components.

As an example, the standard ISO/IEC 27002 (2013) is published by the International Organization for Standardization (ISO). It concentrates mainly on organizational information

security standards and information security management practices. It provides different types of guidelines and controls that may be needed when information systems are utilised in different situations. Therefore, this standard is considered to be one of the key standards in the field of information security. It includes guidelines for implementing an information security policy, with compliance highlighted, in order to help organizations when designing their own policies. Essentially, a wide range of topics relating to information security policy are covered in ISO/IEC 27002, such as access control, information classification and end user oriented topics. Moreover, it refers to the basic procedures that should be taken into account when monitoring adherence to a security policy.

Similarly, the US National Institute of Standards and Technology (NIST) is responsible for developing standards and procedures for information security. Its 800 series of documents provide elaborate information regarding information security management and its implementation. For example, in 2014 the NIST released a new publication, “SP 800-53”, which provides comprehensive information on the procedures for conducting assessments of security controls. It describes these as: creating and disseminating security policy, monitoring alerts, controlling and accessing data, accessing control management, administration of users’ accounts, authentication, etc.

2.2.1 Type of Information Security Policy Users

Depending on the users’ type, security policies should govern their behaviour to stop them making mistakes, whether willingly or not, that can make them the worst enemy of the information system serving an organization (Vidyaraman et al. 2008). An information security-positive culture is required in an organisation, thereby an information security policy can help to govern users’ behaviours towards compliance. The information security policy works as a critical cornerstone in guiding employee behaviour to direct the compliance with an information security policy. Employees must be aware of and understand the acceptable

and unacceptable behaviours which assist in securing the computing environment of an organisation.

Different types of policy users play different roles and have different responsibilities when dealing with information assets, so each type has a different security policy, which may differ from other policies. The different types of security policy users may include the following (Stahl and Pease 2011; Agostino et al. 2013):

- End users, such as employees, consultants and contractors.
- Management, such as executive management or other management.
- Information system personnel, such as employees, consultants and contractors.
- Customers.
- Suppliers, venders or other partners.

Users of information systems should be encouraged to conform to policies and to follow best practice. Organizations must make sure that they are providing enough training for their users regarding their policies. ENISA (2010) describes the types of users that can be targeted in information security awareness initiatives, as illustrated in Table 2.1:

Table 2.1 Targeted users' types for security awareness (ENISA, 2010)

NO	Target group	Description
1	Home user	Citizens with varying age and technical knowledge who use ICTs for personal use anywhere outside their work environment. This user group can be further divided into different categories: kids, teenagers, youths, adult and silver surfers.
2	Employee	All organisations' personnel. Mangers
3	Executive management	Mangers throughout the organisation responsible for personnel activities and performance. Often not technically oriented, this group needs to be educated and understand the importance of information security. This will allow them to implement the relevant security policies and controls within their business areas.
4	Mid-level manager	Executive managers are the key decision-makers for investment in security.
5	System administrator	Technically inclined personnel, usually responsible for the settings and security of network servers and security systems.
6	Third party	Partners, suppliers, consultants contracted to perform a work in an organisation.

2.2.3 Successful Implementation of Information Security Policies

In order for information security policy and procedures to be implemented successfully, the following requirements, which have been reported in the literature, must be met:

I. Organizational issues that may affect information security policy should be identified (Stahl & Pease 2011). To mitigate the conflict that may occur between information security policy and these organizational issues, it is very important to create an information security policy that suits the organization's business context.

II. Regarding information systems, different types of users play different roles and have different responsibilities (ENISA 2010). These users can be divided into four main categories: management, employees, information system personal and vendors (Stahl and Pease 2011).

III. Organizing information security policies into various meaningful categories, for example, physical security, personal security and information classification and control, helps employees to better understand it (Stahl and Pease, 2011). It is easier to promote a culture of compliance among employees when security policies have been categorized and thus simplified.

IV. Security policy should be reviewed by stakeholders, for example, legal counsel, users and management (Silowash et al. 2012). Gathering feedback from stakeholders on information security policy prior to dissemination is a critical step that must be undertaken. This step ensures that all stakeholders will support the proposed policy and adhere to it.

V. All personnel in the organization should be able to understand the information security policy (Bulgurcu et al. 2010). All users need to be consistently given awareness training and education on the implemented security policy (Yazdanmehr &

Wang 2015). Without such awareness and education, the security policy will have no impact on the employees.

VI. Compliance with security policy should be enforced (Knapp et al. 2009). Otherwise, employees' commitment to the policy will decrease over time. Technology can play a major part in compelling employees to adhere to the security policy, for instance setting a strong password policy through the active directory in the windows environment will make sure that no weak passwords are chosen by users. Furthermore, technology can be used to monitor or log user adherence to security policies.

VII. Periodic review and modification of security policy is highly recommended Silowash et al. (2012). This should occur at least once a year. Technology is constantly changing and developing, and nowadays new information technology, such as cloud computing and social networking, is widely utilised. Therefore, organizations need to review and update their policies to accommodate the new developments.

VIII. It is crucial that organizations design effective information security awareness delivery methods in order to implement successful information security policy (ENISA, 2010; Qudaih et al., 2014).

However, some organizations do not have a clear vision or accurate perceptions about their computing environment and its users. Therefore, they may face difficulties in attempting to meet the previous seven requirements for implementing an information security policy. Evidently, when creating their own information security policy, many organizations merely copy the policies of other organizations and apply them to their own context. Moreover, some implemented information security policies are not reviewed periodically to update them or evaluate their effectiveness, which together with a lack of on-going awareness training for the staff prevents the successful implementation of such security policies

An effective information security policy is contained of many factors. The significant factor is that it must be usable. A security policy will not be used if the users cannot implement the guidelines or regulations within the policy. It should be brief, clearly written and as detailed as possible in order to provide the information necessary to implement the policy. An effective information security policy also takes into account the enforcement, it must be enforceable with security tools where appropriate. Moreover, building an effective information security policy should be mapped to the risk assessment of an organisation.

2.2.4 Types of Information Security Policies

Modern business processes rely heavily upon information systems. As a result, it is necessary to implement different forms of protection of a physical, logical and procedural nature. A wide variety of security policies have been established and implemented in different organizations. Basically, information security policy is divided into two main categories: high level security policy and lower level security policy (Baskerville & Siponen 2002). Firstly, high-level policy reflects security concerns and objectives at highest level of abstraction. For example, the organization states the significance of information resources, and defines personal or management responsible for securing this resource. Secondly, lower-level policies follow a high level policy as a response to the identified risks reflecting the organization objectives, or addressing specific countermeasures. An example of lower-level information security policy is, when employees are asked to change their password every 90 days. Thus, an organization should have a high-level security policy, which provides the guiding context within which other lower level policies would reside.

Generally, some examples of security policies that would help to improve information security management are listed below in Table 2.2:

Table 2.2: Types of security policy

Examples of security policies	
Acceptable Use Policy	Confidential Data Policy
Authentication Policy	Encryption Policy
Data Classification Policy	Incident Response Policy
Email Policy	Password Policy
Backup Policy	Network Security policy
Physical Security policy	Network access policy
Guest Access Policy	Mobile Device Policy
Outsourcing Policy	Remote Access Policy

Equally important are the general security policy templates created and published by the SANS Institute since these can fundamentally assist organisations in implementing their own security policies. SANS institute is considered one of the largest and trusted sources for information security training and certifications. Currently, its programs globally have reached more than 165,000 security professionals and also SANS has published more than 2320 research papers in many information security topics (SANS 2014b). To the best of our knowledge, it is the only institute that freely provides a complete set of information security policy templates. SANS has released around twenty-seven completely updated information security policy templates that reflect real-world experience. Therefore, some of the SANS security policy templates will be used as examples in this chapter.

Accordingly, organizations can and should take advantage of these templates, in one way or another using them when starting to design an information security policy. However, taking those templates and applying them directly to the organization's context would not be of benefit because each organization has its own security requirements that may differ from those of other organizations. Accordingly, the following section briefly illustrates some of the

major SANS information security policy templates with the elements that are of foremost concern to end users (the scope of this research is focused upon end users).

2.2.4.1 Acceptable Use Policy (AUP)

The purpose of this security policy is to outline the behaviour that is acceptable and unacceptable as users interact with computer equipment. This policy is applied to all usage of information systems and resources. All users, including employees, contractors, consultants and other workers, must adhere to this policy. The SANS's list below specifies activities that fall into the category of prohibited or unacceptable use (SANS 2014a):

- Violation of the copyright of any individual or organization. For example, unauthorised use of intellectual property, installation or utilizing of software products that have no licenses to be used (Pirated software).
- Accessing data, systems or accounts for any purpose other than conducting an organization's business, even if there is authorization.
- Bringing malicious programs into the computing environment of an organization. For example, the introduction of viruses, worms, Trojan horses or email bombs into the network or systems.
- Sharing account password with others or revealing account information.
- Utilizing the organization's computing assets to deal with or transmit materials that contain sexual harassment or hostility or that breach workplace laws.
- Security scanning or port scanning, unless prior permission has been given by InfoSec.
- Executing any form of network monitoring, unless this activity is an aspect of an employee's work.
- Providing any information on an organization's employees to any party outside the organization.

- Sending undesired email messages, including resending of “junk mail messages” or any advertising messages to individuals who did not request them previously (Email spam).
- Any form of harassment via email, whether via language frequency or size of message.
- Solicitation via email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies
- Creating or forwarding “chain letters”, “Ponzi” or any “pyramid” schemes.
- Blogging that may cause harm or damage the organization’s reputation or its employees.
- Attributing personal statements or opinions to the organization.

2.2.4.2 Password Protection Policy (PPP)

Password security is considered to be one of the most significant aspects of information security, and it is the first line of defence against attacks from hackers, such as "brute force attack". Therefore, passwords are used to protect identities in the virtual world and as an authentication method for an online appearance. Moreover, following and complying with the best practices and procedures when choosing and managing passwords will help organizations to mitigate against any potential threats or weaknesses. Thus, the main purpose of password protection policy is to establish a standard for creating strong and secure passwords, for good management of those passwords and for the frequency of change of passwords. The scope of the password protection policy will cover all personnel who have or are responsible for an account. As an example, the list below demonstrates some major elements of this policy, as stated in SANS's password protection policy template (SANS 2014a) :

- Password Creation

- All users must comply with the password construction guideless (a special document that guides users on how to choose secure passwords).
- Users must not use the same password for the organization's accounts as for other non-related accounts, such as personal ISP accounts.
- When it is possible, users are advised not to use the same password for various organization accounts.
- User accounts that have system level privileges must have a unique password that differs from the passwords used for other accounts held by that user.

➢ Password Change

- System level passwords, such as those used for NT admin, root and application administration accounts, must be changed at least every four months.
- User level passwords, such as those used for application, web, email and desktop accounts, must be changed every six months, though preferably every four months.
- Password guessing or cracking tools may be utilized on a random or fixed basis by the information security team. If a password is guessed or cracked during this process, the user will be asked to change his or her password for a new one that is compliant with the construction guidelines.

➢ Password Protection

- Users are not allowed to share passwords with anyone.
- Passwords must not be added to or written in an email message, transmitted in any electronic form or revealed to anyone over the phone, via a questionnaire or in a security form.

- Users are not allowed to write passwords down on a piece of paper or store them in any place, such as in a computer file without encryption.
- Users are not allowed to utilize password memorization, which is available in some applications as an additional feature, such as the web browser 'remember password' feature.
- If there is any doubt about the password's security or any suspicion that it has been compromised, the user must immediately change the password and report the incident.

2.2.4.3 Clean Desk Policy (CDP)

Clean desk policies are designed to make sure that all important /confidential materials (e.g. users' computer or sensitive documents) are kept secure or removed from the end user's workplace when these items or materials are not in use or the user leaves his or her workplace. Therefore, the main aim of this kind of information security policy is to increase users' awareness of the minimum requirements for maintaining a clean desk. In other words, it provides guidance regarding how users should leave their workplaces, directing them to clean their desks at the end of each working day. Employees' compliance with a clean desk security policy will benefit the organization by reducing the potential risks associated with the information theft or security breaches that may occur when information is left on desks in plain view. The list below, taken from SANS's clean desk policy template, explains some elements of clean desk policy (SANS 2014a) :

- Employees must ensure that all sensitive information and material, whether in hardcopy or electronic form, is kept secure when they leave their workstations.
- When a workplace is not occupied, computer devices must be locked or shut down.
- At the end of each working day, computer workstations must be shut down.

- Sensitive or important information must be kept secure, by being removed from the desk or locked in a drawer, when the workplace is not occupied.
- Keys that are used to access any important or sensitive information must not be left on an unattended desk.
- Laptops must be kept secure by using a locking cable or locked away in a drawer.
- Passwords or any information about an employee's account must not be written on a sticky note nor left written in an accessible location
- Printouts that contain any sensitive information must be removed from the printer's storage.
- Unwanted sensitive documents must be disposed of by using the organization's official shredder or being placed in a secure disposal bin.
- Electronic storage devices, such as USB and DVDs that contain restricted information should be kept secure.
- Employees need to keep printers and fax devices clean from paper when they finish work.

2.2.4.4 Email Use Policy (EUP)

Today's organizations are very reliant on email usage in the performance of daily tasks. However, the misuse of email services can lead to many privacy, legal and security risks for an organization. Thus, it is very important for any organization to make sure that all its employees have an adequate understanding and perception of its implemented email use policy. The following list highlights some important elements of email usage policy (SANS 2014a):

- The organization's email account should be fundamentally utilized for business that is related to the organization.

- All data within email messages and attachments must be secured in compliance with Data Protection standards.
- Email should be retained only if it qualifies as an organization's business record and there is a legitimate business reason for continuing to keep the information included in the e-mail.
- The organization's email system must not be utilized to create or distribute any offensive or disruptive messages. For example, offensive comments about age, disabilities, sexual orientation and religious beliefs. Employees who receive any email with this content must report the matter to their supervisor.
- Employees are not allowed to automatically forward the organization's email to any third party email service, such as Yahoo and Hotmail, etc.
- Employees are not allowed to utilize third party email and storage services to perform the organization's business.
- Sending chain letters or joke emails from an organization email account is prohibited.
- There will be no privacy expectation for any employee in anything sent, received or stored in an organization's email system.
- The organization's email messages may be monitored without any prior notification.

2.2.4.5 Internet Usage Policy (IUP)

The Internet is the world's biggest information network, and information and resources can be acquired easily through this large network. In other words, it is a global infrastructure which is organized into thousands of sub networks connected to millions of computer devices. Today's organizations use Internet services due to communication with others parties via the Internet being cost effective and high performance. Moreover, cloud technology has

encouraged organizations to store their applications and data in servers that are accessible via Internet services.

However, threats that come from the usage of the Internet will continue to be a major concern for many organizations. According to (PriceWaterhouseCoopers PwC 2014), 75% of organizations were victims of viruses or malicious software in 2013. Therefore, Internet connectivity may present the organization with new threats and increase the likelihood of breaches in its information security. In addition, it is common in the information security domain to consider end users as the weakest link in the information security chain.

Organizations should thus address the concerns over Internet usage, especially with regard to end users, and apply a strong information security policy that controls users' behaviour when using the Internet. The following list highlights some important components of Internet usage policy (SANS 2014a):

- Employees are not permitted to participate in any online activities that are likely to harm the organization.
- Employees must not download, visit or view any illegal materials on the Internet.
- Employees must not introduce any malware software into the organization's network.
- Personal use of the Internet must not cause a significant increase in resource demand.
- Employees must not download unauthorized software or files for use without prior authorization from the IT department and their manager.
- The Internet must not be used for personal financial gain by the employee.
- Employees are not allowed to play any games on the Internet.
- Use of the Internet for personal activities, such as online banking, private email or shopping, should be reasonable and limited.

- Use of online action sites, gambling and social networks, such as Facebook, Flicker, LinkedIn, Bebo and YouTube, is not allowed.
- The forwarding of chain letters is not allowed.
- The acceptance of promotional gifts is not allowed.

2.3 The Current Extent of Use of Information Security Policy

An information security breaches survey conducted by PriceWaterhouseCoopers (PwC 2014) implied that most large organizations now implement their own documented security policy (as illustrated in figure 2.2). More encouragingly, the information security policy adoption level within small businesses increased from 54% in 2013 to 60% in 2014. Another survey conducted by E&Y Global Information Security (2013) reported that information security policies were owned at the highest organizational level in 70% of all organizations. This result is a good indication that the majority of organizations are aware of the importance of information security policy. The size of an organisation (large or small) can be decided based on number of employees or revenue. For example, small organisation – Less than 50 employees and large organisation more than 250.

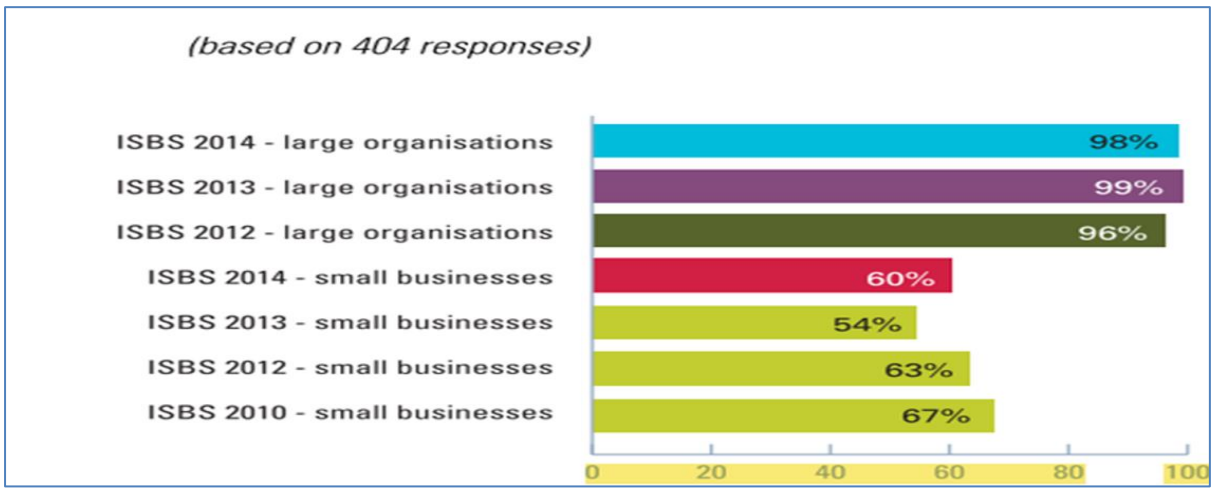


Figure 2.2: Organisations with a formally documented security policy (PwC 2014)

However, having such a policy in place is not a guarantee that employees will adopt the required behaviour; they may not behave as they are expected to due to a lack of understanding of the policy's content. Essentially, in the aforementioned survey, approximately 25% of the respondents believed that their members of staff understood their policies well, while approximately 20% of the respondents believed that their staff's level of understanding of their security policies was poor.

Another survey conducted by PwC (2012) revealed that the number of small businesses using written security policies steadily increased during 2011. The number of organizations having a formal security policy reached about two-thirds of the total. However, the situation is different in large organizations, which for the most part have a security policy in place. Despite the fact that security is a very high priority, only one in seven organizations have adopted and implemented a written security policy. Most of the surveyed organizations were small and more inclined to depend on word of mouth than written policy. The survey included mobile computing usage policy and found that 58% of large organizations have established a policy for mobile computing, while only 27% of small organizations have done so. Essentially, these policies cover the use of smart phones as well as tablets by the staff and the required steps needed to mitigate the associated risks.

Table 2.3 reveals some consolidated statistical information that explains the current extent of use of information security policy and the key policy-related issues over the last four years. The information in this table was gathered mainly from two global surveys performed by PWC and EY. They survey organizations across the world on areas concerning information security and breaches, and they usually produce a new survey report every year.

Table 2.3: Summary of information security policy and key policy-related issues

Source	Security Policy implementation	Threats by employees	Security awareness promotion	Security governance and compliance
The E&Y Global Information Security Survey (2011)	Some organizations adjusted their security policy with the introduction of new technologies e.g. 57% for mobile computing, 77 % for sensitive data.		52% of organizations increased security awareness for mobile computing. and 69% of organizations did so for sensitive data.	53% of organizations limited or denied access to social sites. 66% of organizations did not implement tools to prevent data leakage.
The E&Y Global Information Security (2012)	Some organizations adjusted their security policy with the introduction of new technologies e.g. 52% for mobile computing, 45% for social media and 72% for sensitive data.	37% of organizations viewed careless or unaware employees as the most likely threat.	Organizations increased security awareness in various areas: 40% social media, 40% mobile computing, 68% sensitive data.	45% of organizations limited or denied access to social sites, whilst 57% implemented security mechanisms regarding sensitive data.
Information Security Breaches Survey, PWC (2012)	96% of large and 63% of small organizations had a formally documented information security policy.		46% of small organizations provided on-going security awareness training for their staff.	
The E&Y Global Information Security (2013)	70 % of all organizations indicated that information security policies were owned at the highest organizational level.	57% of organizations considered employees the most likely source of an attack, with 38% viewing careless or unaware employees as the most likely threat.	Security awareness and training was mature in 30% of organizations, undeveloped in 41% and non-existent in 29%.	28% of organizations had mature security governance, while 13% had not yet developed this.
Information Security Breaches Survey, PWC (2013)	99% of large and 53% of small organizations had a formally documented information security policy.		58% of large and 48% of small organizations provided on-going security awareness training for their staff	
The E&Y Global Information Security (2014)		57% of organizations considered employees the most likely source of an attack, with 38% viewing careless or unaware employees as the most likely threat.		
Information Security Breaches Survey, PWC (2014)	98% of large and 60% of small organizations had a formally documented information security policy.	70% of organizations where security policy was poorly understood had staff-related breaches versus, whereas only 41% of organizations where the policy was well understood had the same.	68% of large and 54% of small organizations provided on-going security awareness training to their staff.	45% of large organizations restricted staff access to the Internet at work, whereas 50 % of small organizations restricted staff access to the Internet at work
Information Security Breaches Survey, PWC 2015	98% of large organisations and 60% of small organisations have a documented information security policy	75% of large organisations suffered a staff-related breach and nearly 31% of small organisations had a similar occurrence. 72% of companies where the security policy was poorly understood had staff related breaches.	For large organisations, on-going security training has increased up to 72% , and for small organisations, up to 72%	77% of large organizations block access to inappropriate websites not including social networking sites and 40% of small organizations do the same. 37% of large organizations block access to inappropriate websites including social networking sites 14% of small organizations

Thus, from above table, nearly all large organizations now have a formally documented information security policy, whereas more than half of small organizations have implemented the same. However, only half of all organizations have a security policy for new technologies e.g. mobile computing and social media. Encouragingly, around three quarters of the organizations surveyed have a security policy for sensitive data. Roughly more than half of organizations consider their employees to be a major threat to their information security, and almost a third of them view careless or unaware employees as the most likely threat. Employees' good understanding of security policy positively affects the overall security of an organization. This is seen in PWC (2014) where the number of staff related breaches decreased by 30% in organizations whose employees better understood their security policy. Only around half of organizations provide their staff with continuous awareness and training activities. Almost half of all organizations restrict their employees' access to the Internet, whilst almost half of all organizations limit or deny access to social sites.

Organisations increasingly perceive their employees as a great asset that needs to be cared for; however, at the same time, they view employees as one of the biggest potential threats to their cyber security. Employees are widely acknowledged to be responsible for security breaches in organisations, and it is important that these are given as much attention as are technical issues. A significant number of researchers have argued that noncompliance with information security policy is one of the major challenges facing organisation. Researchers have mentioned three types of non-compliance behaviour: malicious behaviour, negligent behaviour and unawareness. The main motivation for malicious behaviour is malicious intent to bring harm to an organisation's information assets (Furnell & Thomson 2009; Da Veiga & Eloff 2010), whereas negligent behaviour is intent to violate an organisation's security policy but not to harm that organisation (Greitzer et al. 2014). The third type of non-complaint behaviour is due to unawareness, whereby end users are unaware of the importance of

information security and the relevant organisational requirements. Khan et al.'s (2015) research indicated that more than fifty percent of employees are unaware of the existence of an information security policy in their organisation. Moreover, Greitzer et al. (2014) state that users tend to dislike the active controls that are imposed on their PCs, and this can be seen in many organisations.

2.4 Approaches in Policy Enforcement and Monitoring

As reported in the literature Pahnila et al. (2007); Siponen and Vance 2010), although information security policies are in place to protect different information systems assets, staff members are not readily complying with them to cut down on the destruction, misuse and abuse of these important assets.

Implementing monitoring tools can help to identify security policy breaches that may occur. These tools can monitor the on-going transactions and the different system logs to highlight any breaches. Without these tools, it is difficult to measure staff compliance with policies (Knapp et al. 2009). Breaches will not be identified unless their nature is very clear and has some visual effects (e.g. a virus attack or outbreak). Hence, implementing these monitoring tools enhances the level of compliance and aids the enforcement process due to users' perception that they are being monitored. However, these monitoring tools and resources are not widely implemented in organizations (Knapp et al. 2009).

Organizations can include a clause in an "Acceptable Use Policy" document that is signed by employees stating that monitoring tools will be used to check and measure their compliance. Thus, the policies must contain areas describing best practice while using the different IT facilities, network services and/or email systems. They must also outline the consequences of not following best practice.

Nowadays, the Internet has become extremely important to organizations' business and indeed to individuals' lives. However, the majority of organizations have concerns about information security, especially in relation to new technologies, such as mobile computing and social networks. According to Symantec (2014), usage of social networks has spread rapidly, and the burden of preventing attacks falls primarily on the user. In reality, large organizations tend to restrict Internet access more than small organizations. Actually, as reported in EY's (2012) survey, 95% of large organizations use blocking software to restrict access to inappropriate websites, while only 50% of small organizations do so. Totally blocking Internet access is not an option anymore as users may need to access the Internet for work purposes, so organizations grant access to users who need it but block inappropriate services and websites. The widespread use of social networks has forced large organizations to block them instead of just monitoring them.

Another example of user non-compliance, as reported by Wilson (2010), is major data leaks, which happen on a daily basis as a result of staff working from home or outside normal offices and uploading files to their home email or other social media while not using the required secure methods. Wilson added that in order to use files on their home machines, users tend to use file-sharing cloud software that does not offer enough protection.

To this end, a variety of technical solutions can be implemented in order to monitor users' adherence to their organization's information security policy; some of these act as prevention from violation, such as password policy via Microsoft Window's active directory, while others act as a monitoring solution, such as logs analysis. The following section highlights some potential solutions to the problem of users not adhering to the information security policy of their organization:

According to remote working, many organisations using secure remote access, such as virtual private networks (VPNs). Create a secure connection to the organisation network will help monitoring the information security policy for the remot working.

2.4.1 User Account Management

There is no doubt that a weak password is one of the greatest vulnerabilities for any organization. Unfortunately, organizations and employees alike often pay less attention to the password strategy, and that explains why many users get into trouble. According to (PriceWaterhouseCoopers PwC 2014), most staff related security incidents involve unauthorised access to the systems by using someone else's account or password, as shown in Figure 2.3.

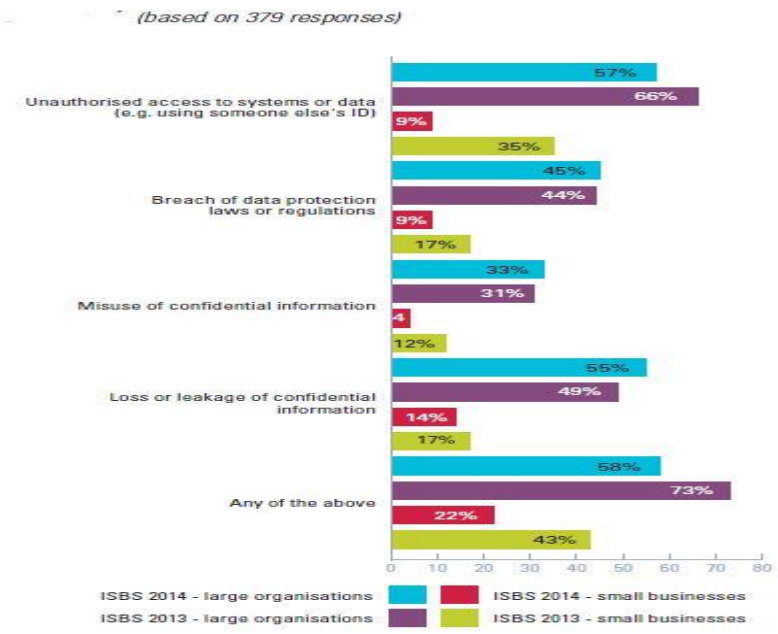


Figure 2.3: staff related incidents did organizations suffer (PwC 2014)

For example, an Active Directory (AD) is a service that is provided by Microsoft to manage Windows domain networks. This service is available in the Windows server operating system

and includes a set of processes and services. For example, the administration of the network's users and their accounts are performed through AD's service.

As a solution, the Active Directory can play a significant role in setting policies at a system level and enforcing these policies on the password usage. Such password security policies may include: enforce password history, password age, password length, password complexity and account lockout. Table 2.4 illustrates password security policy:

Table 2.4: Password security policy

Policy	Setting	Description
Enforce password history	20 remembered	This policy prevents users from using the same password twice in a period of time. For example, in the case of 20 remembered, when the user has changed his or her password 20 times, then he or she will be able to use the same password. The new password must not be one of the past 20 passwords.
Maximum password age	40 days	Password must be changed after 40 days
Minimum password age	3 days	Password cannot be changed in less than a 3 day period
Minimum password length	12 characters	Length of password must be 12 characters
Password complexity	Enable	Certain requirements will be applied to the password. For example, the password must not be the same as the username, it must not be the same as or part of the full name and it must contain at least one symbol or character.
Store password using reversible encryption	Disabled	This should always be disabled because enabled it will stores a password in plain text.

2.4.2 Monitoring Software

The comprehensive umbrella that is named endpoint-security includes employee monitoring and malware protection as well as policy enforcement procedures in addition to assets tracking. The endpoint-security concept is achieved in large organizations by having suitable

software on servers along with suitable software on end-user machines. Due to less resources being available in small businesses, this can be achieved by installing a piece of software from the end-user machines that works with the software installed in the cloud (remotely) to monitor compliance with policies and to provide protection for end-user machines (Strohmeyer 2011). The most secure technique used to monitor an end-user PC is to install a piece of software as a host that works with a server or an appliance (*ibid*).

Alternatively, cloud-based services can do the job. For example, Symantec Cloud is a cost-efficient service when compared with the server choice that offers a single management interface to monitor users' compliance with the setup policies in a very flexible manner (Strohmeyer 2011). In addition, these cloud services are updated automatically to offer an enhanced service to block malware and offer more protection and thus prevent security breaches that can cause information leaks.

2.4.3 Data Loss Prevention

One of the initiatives that emerged in 2006 and gained popularity in early 2007 is DLP (Filkins & Radcliff 2008). Data loss prevention (DLP) puts together a plan that guarantees users do not send confidential, sensitive or critical information outside the expected local official network (Takebayashi et al. 2010). DLP contains a description of software products to control the data exchange on a network that can be utilized by network administrators. Companies such as Symantec have cited DLP as a comprehensive solution for data security that helps in managing and protecting data wherever it is used or stored. It can also help in the monitoring of data usage. DLP contains the necessary defined policies, and it has the requirements needed for monitoring the usage of confidential and sensitive data wherever the data exists or whenever it is exchanged within an organization. Most of the DLP solutions contain these three important objectives (Filkins & Radcliff 2008):

1. Extracting a list of the important and confidential information assets across an enterprise.
2. Monitoring and controlling any transaction or exchange that occurs on the identified assets across the enterprise network.
3. Monitoring and controlling any exchange that occurs on the identified assets when residing on the user's machines.

2.4.4 Security Information and Event Management (SIEM)

A Security Information and Event Management (SIEM) system provides a centralized view of all logs by collecting them from the different devices and applications on a network. Additionally, SIEM systems can be used to comply with regulatory bodies regarding data retention, which is also helpful for e-discovery purposes and forensic investigations. SIEM systems not only collect logs but also correlate and analyse the collected data and thus save time and money, which is considered to be one of the important advantages of such a tool (Chuvakin 2010)

In a survey by Shenk (2012), 82% of the respondents stated that the main reason for using SIEM tools was to detect and track suspicious behaviour by collecting the appropriate logs from the different resources, while 54% of the respondents had used SIEM systems to detect more complicated attacks and threats.

Generally, SIEM tools can be used by network administrators as a monitoring dashboard to provide a general view of the daily work activities on the monitored network. Administrators can predefine thresholds and rules to facilitate the monitoring of the activities on the network.

2.5 Key Security Policy Related Issues and challenges

Nowadays, organizations continue to face challenges in relation to encouraging user adherence to implemented security policy, for instance Internet usage policy (Saran and

Zavarsky 2009). Many tools and methods have been used to increase the compliance of end users, such as user signed policies, monitoring tools, logon pop-ups, website restrictions and disciplinary action. However, the effectiveness of such information security policy is still threatened by user non-compliance, as explained in the following subsections. Figure 2.4 gives an overview of the challenges associated with security policies:

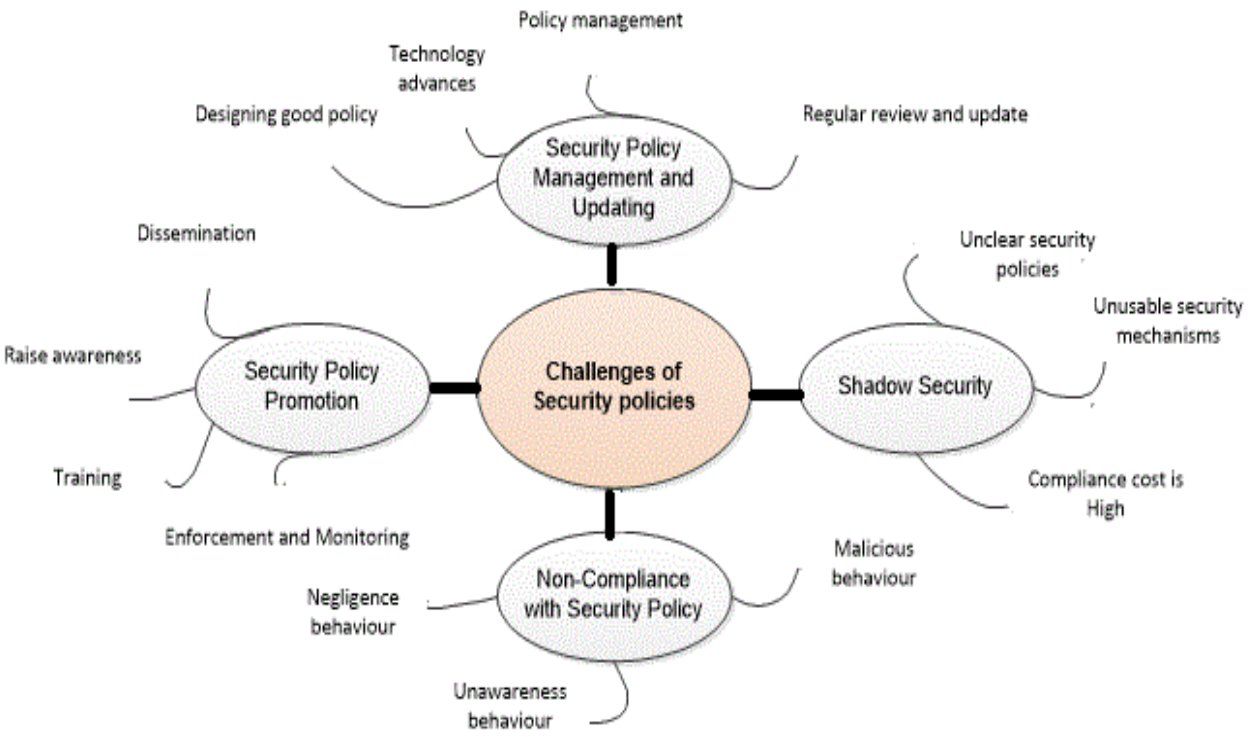


Figure 2.4: Information Security Policy Challenges

2.5.1 Security Policy Management and Updating

Usually, security solutions, such as security policy, procedures, controls and training, are neglected by many organizations, not being continuously reviewed or even updated (Colwill 2009). According to Silowash et al. (2012), organizations may face challenges when attempting to implement best practice in relation to information security, as follows:

- Designing good policy: It can be a challenge for many organizations to create an information security policy that covers all the significant issues, such as flexibility, fairness, legislation and fit to the organization.
- Policy management: Organizations must consistently review and update policies to ensure that they are still meeting all the organization's needs and ensure that updates are disseminated to all employees.

Moreover, a survey conducted by the Global consulting firm on privacy and IT security found that organizations struggle to manage their information assets security (Protiviti 2014). The most significant finding from this survey was that one out of three surveyed organizations did not have a documented data security policy. Therefore, there is a critical gap that may indicate a disconnection between data governance and organization management. In addition, despite the new opportunities provided by the cloud revolution, only 24% of the respondents had a cloud acceptable usage policy in place. Evidently, this gives an indication that many organizations ignored the importance of updating their information security policies.

2.5.2 Security Policy Promotion

The implementation of a good information security policy will not be effective unless there is a comprehensive plan to promote it and raise awareness of it among employees. Hence, organizations should be encouraged to promote, communicate, enforce and maintain information security policy.

However, organizations face challenges associated with the promotion and dissemination of their information security policies. In (Economist Intelligence Unit EIU 2009b) survey, most of the IT managers claimed that information security policies had been developed by their organizations to overcome many concerns, for example, use of PCs, applications and

websites. However, only a few of these organizations had seriously instilled this culture into their employees. This is supported by PwC (2014), who state that:

"Although there are more written policies in place to guide employees' behaviours towards security, we haven't yet seen this translate into better understanding of these policies".

A survey carried out by Enterprise Management Associates (EMA) revealed that more than half of the members of staff in enterprise organizations did not participate in any kind of security awareness training (Prince 2014). This was the result of surveying 600 employees, 56% of whom did not receive any kind of training on the security policy adopted by their organization. The study confirms that the absence of training results in violations of the policy and the occurrence of behaviour that poses a risk to the organization. For instance, in the survey, 33% of the staff indicated that they were using the same password for personal and work devices. In another example, 59% of the respondents in the survey were using the cloud to store work information, which rendered it inaccessible to the organization itself at times. However, 48% of the surveyed members of staff indicated that the effectiveness of security awareness training had been measured by their organizations. The significance of the awareness of information security policy will be covered in more detail during the next chapter (chapter 3).

2.5.3 Non-Compliance with Security Policy

Non-compliance with information security policy is primarily considered to be a human problem rather than a technical issue, for example a lack of security tools. Therefore, the main solutions are possibly non-technical, for example awareness and training, and these can obviously contribute to mitigating the potential threats from non-compliant users.

Negligence of users or human error was the major cause of the worst breaches in 2013 (PriceWaterhouseCoopers PwC 2014). Further to this, another report by PwC (2012) revealed

that 75% of organizations have suffered from staff-related breaches due to a lack of understanding of security policy.

A study conducted by Saran and Zavarsky (2009) upon approximately 2000 employees in an insurance company found that even if a policy is re-released for the staff to sign or a reminder pop-up or email is sent to them, they may not engage with the policy since they can sign without reading or just ignore the pop-up or email. Hence, educating and training staff about policy is crucial if non-compliance is to be eliminated.

Tom Wilson (2010) stated that users tend to dislike the active controls that are imposed on their PCs, and this is commonly seen in many organizations. The reason for hating these controls is due to them being a group of no commands (e.g. no Google apps, no Facebook, no Skype, etc.). He also added that in reality, users tend to find a way around these controls to do what they want to do. Therefore, it is better to convince users to use policies and to enforce them firmly.

Theoretically, many factors influence employee behaviour in relation to information security policy and may contribute to non-compliance behaviour. These influential factors can be grouped into human and organizational factors (more information about these factors is provided in chapter 4).

2.5.4 Shadow Security

Traditionally, organizations manage the security of their information assets via mechanisms and a security policy that employees are expected to comply with. There are two main categories regarding the expected behaviour of employees in relation to such security policies: compliance and non-compliance.

However, a third type of employee security policy behaviour has been identified: shadow security (Kirlappos et al. 2015). Shadow security is defined by Kirlappos et al. (2014) as "*employees going around IT to get the IT services they want on their own*". In other words, employees implement their own security solutions when they believe that compliance is beyond their capacity or will affect their productivity.

For example, when an organization creates and implements a strong password security policy, such as 12 characters in length and a combination of upper letters and symbols, some employees will find it difficult to remember the password. Employees in this case will comply with the policy but play around with it by writing the password on a note and putting it under the keyboard.

In the aforementioned example, an employee is considered to be complaint with password policy; however, there is also a shadow security policy, and this may threaten an organization's security. If it does not manage the situation appropriately, the risks may include:

- Creation of a false sense of security: the risks associated with the shadow security policy are not usually perceived by the employees who play around with the main security policy (Kirlappos 2016). Thus, the employee does not understand the risk that the organization may be at due to this behaviour.
- Ineffective communication of policy to the management: Security policies need to be reviewed and evaluated in a timely manner; however, shadow security can make this task more difficult (Kirlappos et al. 2015). If management is made aware of security policy related issues, appropriate support to resolve these issues can be given.
- Spreading of non-compliance culture: The presence of shadow information security behaviour may lead to the emergence of a non-compliance culture within an

organization as a whole (Veiga & Eloff 2009). Usually, organizations attempt to change their employees' behaviour, but shadow security may act as an additional level of resistance against the adoption of the desired security behaviour(Kirlappos & Sasse 2014).

- No employee feedback about the implemented policies: If employees play around with the implemented security policy, they may not provide feedback on the shortcomings of that policy and suggest alternative solutions (Dang-Pham et al. 2014).

To mitigate the effects of shadow security, organizations should pay attention to reducing compliance costs. Unusable security mechanisms or unclear information security policies may not provide efficient protection for an organization because employees will attempt to find ways to play around with those solutions that are undesirable in his or her opinion.

Employees ignore information security solutions that require a great deal of effort with no or little benefits (Sikolia et al. 2014). Hence, organizations need to be able to discover the shadow information security behaviour of their employees, where and when this behaviour is created and under what circumstances. Kirlappos et al. (2015) indicated the importance of measuring shadow security behaviour, adding that the use of matrices to measure employee behaviour has limitations.

Put simply, organizations encourage shadow security by their ignorance and many security policies are created based on an incomplete picture. Therefore, unusable security solutions usually lead to errors, which in turn create vulnerabilities. However, the problem of unusable security solutions can be mitigated by engaging employees in systems design. The feedback from the end users about such information security policies can be critical in limiting shadow security behaviour.

2.6 Conclusion

Nearly all large organizations have a formally documented information security policy, whereas merely more than half of small organizations have implemented the same (PWC 2015). However, employees' compliance with the information security policy is one of the main challenges facing today's organizations. Practically, there are two major countermeasures assisting in reducing the probability of users' non- compliance: technical solutions such as monitoring or enforcement tools, and non-technical solutions, such as awareness and training. It is well known that organizations tend to concentrate more on technical solutions when it comes to information security rather than considering the vital human factor.

However, providing security awareness and training for employees on different security issues including security policies, is the key to guaranteeing or at least enhancing their security compliance. Despite the great benefits of such information security awareness campaigns, obstacles exist that make the successful implementation more challenging. For instance, users become careless of security awareness activities as a result of bombarding them with too much security awareness messages and warnings.

There is a need to understand the potential behaviours of user with the information security policy by performing insider risk assessment. As mentioned previously, dealing with the human factors is not only a technical issue and therefore more focus should be given to the awareness and training. Therefore, the enhancement of awareness and training programs can assist in the promotion of security policy. As such, the following chapter will focus attention upon information security awareness and related issues.

Chapter Three

Information Security Awareness

3. Information Security Awareness

3.1 Introduction

Information security awareness can be defined as a process for making employees aware of an information security. In other words, making an organisation's staff members informed of the information security related rules and regulations (Khan et al. 2011). The accumulation of such knowledge amongst employees and the attitude they thus have to information security will fortify an organisation's protection against physical or information security incidents (Bashorun et al. 2013).

Security awareness goals can be achieved when employees' behaviour is based on the best practice that they are advised to follow during information security policy dissemination and the awareness programmes conducted by their organisation (Siponen et al. 2014). It is understood that organisations tend to concentrate more on technical solutions when it comes to information security rather than considering the vital human factor, which is considered the weakest link in an organisation's line of defence. As a result, good security practices should be promoted amongst staff members, and their knowledge should be updated continuously to achieve sustainable security awareness.

3.2 IT Security Learning Continuum

Organisations have now become more conscious of the importance of making their employees aware of information security, and thus they have expended a lot of time, effort and money on this area. They have created and implemented information security policies to direct employees' behaviour towards the right practices. However, having a policy does not mean that an organisation is completely protected against undesired behaviours. According to the global information security survey (PwC 2015), of all the surveyed organisations where security policy was poorly understood, 72% experienced a staff related breach. Moreover

they stated that, "*Whilst having a policy is important in setting out an organisation's objectives in information and cyber security, there are clear benefits in making sure that it is understood and implemented accordingly.*"

Therefore, increasing employees' knowledge about the organisation's security policies plays a very important role in the successful implementation of such policies. On the surface, awareness raising, education and training may seem like similar concepts to be used in increasing employees' knowledge; however, there is a subtle difference between the three terms (ENISA, 2010). According to (Bowen et al. 2006), information security learning is a continuum, which starts with fundamental awareness, builds cumulatively into training and lastly evolves into education. The continuum in figure 3.1 illustrates the conceptual relationship between the three terms.

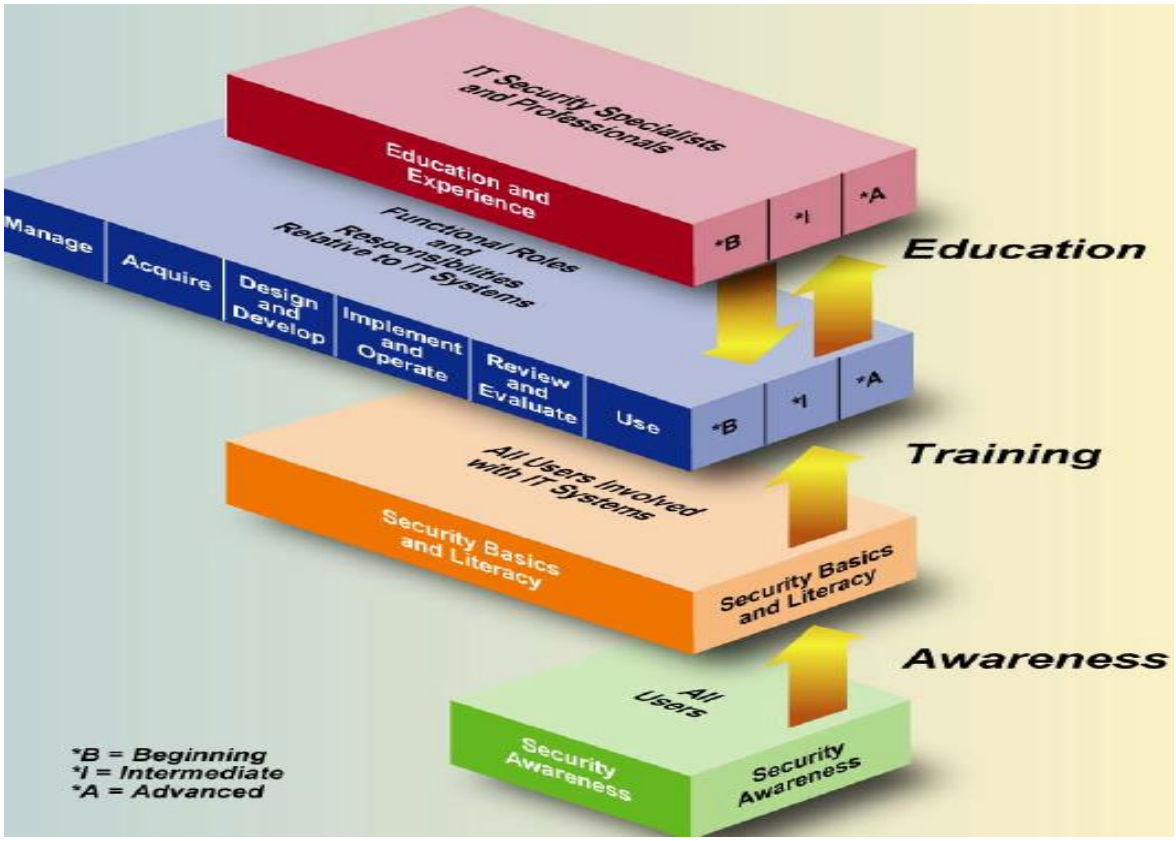


Figure 3.1: Simplifying the meaning of: Awareness, Training and Education

In the previous model, there are three stages to the IT security learning continuum: awareness, training and education. The first stage is ‘security awareness’. This is located at the bottom part of the security learning continuum and is the basic type of learning that all employees need to start with. The ‘security basics and literacy’ layer is a transitional step between the awareness stage and the training stage, and it ensures that all employees have a basics knowledge of information security. The second stage, training, is represented by two layers ‘security basics and literacy’, and ‘functional roles and responsibilities’. At this stage, employees need training on the security basics and to develop special knowledge about security threats, vulnerabilities and countermeasures. The final stage, education, is represented by the ‘education and experience’ layer, which is aimed at employees who work in the field of IT security. The main aim of this stage is to develop the capacity of employees to perform complex or multi-disciplinary tasks. IT security professional need to be kept up to date with the advances of technology and changing threats. To illustrate this section, Figure 3.2 is a simplified version of the three-stage model that involves awareness, training and education.

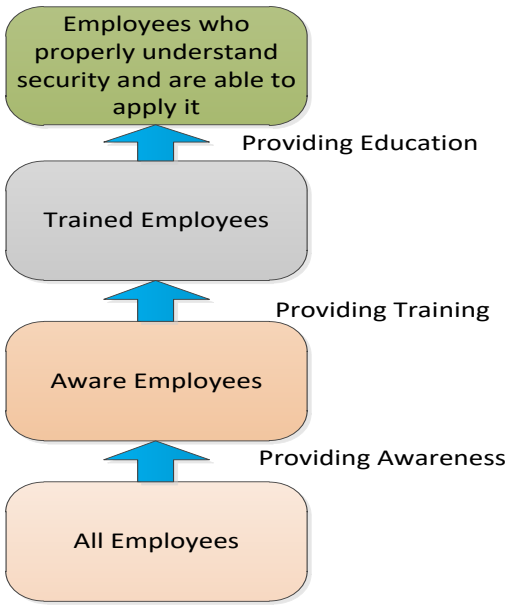


Figure 3.2: Simplifying the meaning of: Awareness, Training and Education

3.2.1 Awareness

Security awareness involves activities that have been designed to change an employee's behaviour so that it falls within the information security boundary. Bowen et al. (2006) indicate that the main aim of security awareness is to draw users' attention to information security. They also add that by increasing awareness, employees will be able to recognise information security threats and identify the best steps for dealing with such concerns. ENISA (2010) contends that security awareness aims to enhance employee behaviour and attitude towards secure practises within their systems. In other words, awareness focuses upon employee knowledge of specific security issues or a set of concerns. Moreover, Bulgurcu et al. (2010) describe information security awareness as an employee's general knowledge about information security, including his/her perception of the security policy of his/her organisation.

3.2.2 Training

Training mainly seeks to provide employees with the requisite security skills in relation to specific or selected security topics. Training an employee on a particular task will help him to perform this function. According to ENISA (2010), training programmes should be selected and implemented according to the learning objectives set by the organisation. For example, the process of teaching an employee how to use antivirus software is considered to be security training.

It is important to understand the distinction between training and awareness raising (Bowen et al. 2006). Training aims to teach employees skills that assist them in performing a particular task, whilst awareness aims to draw the attention of employees to a security issue or a set of issues. Any skills acquired during training are built on a foundation of awareness.

3.2.3 Education

Education is considered to be the top level of knowledge development, and it is more specialised in terms of the learning method, which involves more in-depth schooling. For example, a course or degree programme in a particular domain provided by a university or an institute is considered to be education. In the information security domain, education is provided for employees who are specialised in information security to promote the security profession. According to Bowen et al. (2006), "*Education integrates all of the security skills and competencies of the various functional specialties into a common body of knowledge and strives to produce IT security specialists and professionals capable of vision and pro-active response*".

In conclusion, Learning is a continuum; it starts with awareness, builds to training, and can evolve into education. Awareness is having knowledge of a situation or fact. Security education is specific to those who wish to make security a career. Training provides employees with the requisite security skills in relation to specific or selected security topics

3.3 Current Information Security Awareness Raising Methods

According to Abawajy (2014), information awareness delivery methods can be divided into three main categories: instructor led, conventional and online. Firstly, the instructor led method involves formal presentations and training sessions. Secondly, employee conventional methods utilise posters and leaflets, etc. Thirdly, online delivery uses technology to deliver security awareness to employees, for example, computer based awareness programmes. Table 3.1 illustrates the aforementioned categories:

Table 3.1: Information security awareness methods

Categories	Methods
Conventional	Posters, stickers, leaflets, employee newsletter
Instructor led	Formal presentations or training sessions
Online delivery	Electronic articles or emails
	Web based security awareness triaging
	Security alert message e.g. logging messages
	Game based method

Similarly, ENISA (2010) suggests methods that can be useful when attempting to enhance employee awareness of aspects of information security. These methods are listed below:

- **Reading materials**: Employee awareness is increased by reading security policy, posters, newsletters, web sites, email messages and handbooks.
- **Policy-based**: The organisation sends a warning message to those who have not adhered to its security policy if it has been violated in any way.
- **Event-based**: Special events held for improving awareness, such as induction training, face-to-face training, tests, quizzes and automated questionnaires, especially after a major security incident.
- **Video-based**: Users attend security awareness sessions via the use of visual aids, such as video tapes, web based sessions, video games and computer based training (CBT).
- **Message awareness tools (Trinket)**: Promoting awareness through items that employees use in the work place, such as pens, key fobs, clocks, pop up calendars stickers and notepads. An example of this method is writing the message "Do not share your password" on top of calendar stickers.

- **Management support**: Awareness and training support from management or the information security team. They can play a significant role in the awareness process by creating a scheme of rewards or sanctions for those who are within the boundary of the security policy.

Moreover, situations and events that can occur in any organisation can result in the launching of information security awareness activities. ENISA indicates some important events and situations that may mean the security awareness of employees needs to be enhanced. These are listed below:

- New regulations or laws.
- New information security policy and updates or changes to it.
- Implementation of new technology, products or services.
- New employees or outsourced personnel.
- New risks, etc.

The National Institute of Standards and Technology (NIST) (2005) divided the methodologies for information security awareness programs into: information security awareness training, computer based information security awareness, and awareness services and reminder tools.

- **Information security awareness training:** This is considered to be the most effective method used to gain users' attention (NIST 2005). The subject and content of the awareness material is explained in an effective way. Usually, a security awareness audience is categorised into three classes: management, end users and technical staff.
- **Computer based information security awareness:** This is a self-learning approach**;** a computer application is designed and made available on the network at any time so

that end users can access it easily and then learn the topics that are of interest to them by themselves at their leisure.

- **Awareness services and reminder tools:** Reminder tools are used to keep end users updated on information security awareness topics, reminding them from time to time. As examples of reminders tools are: multimedia presentations, security booklets, security posters, computer screen savers, email shots, promotional items with security issues and security newsletters.

Although many methods are used to raise employees' awareness about information security, it is crucial that organisations ensure their effectiveness (Chen et al. 2008; Abawajy 2014; Khan et al. 2011). The literature discusses methods that can assist in increasing the effectiveness of such information security programmes or messages (May 2008):

- **Focus on personality**: Make awareness messages relate to the employees' personal life. For example, demonstrate that clicking on an unknown link received in an email may result in the theft of private data.
- **Match awareness messages to the audience**: Segment employees into classes, so each category will receive appropriate awareness messages. For example, when conducting targeted awareness for technical staff, the awareness material should include all the technical jargon.
- **Keep it short**: It is difficult for employees to understand too much information at once. Therefore, if it is kept short, it will be easier for employees to grasp the aim of the awareness information.
- **Make it interesting**: It is important to attract the employees' attention and motivate them to be interested. For example, utilising humour can effectively contribute towards encouraging employees to read more.

- **Utilise real examples**: Instead of using theoretical examples of security incidents, it is very effective to give employees real examples of security incidents and learn from these.
- **Make it part of everyday business:** Make employees conscious of their daily activities through the use of a variety of awareness methods, such as posters or emails. For example, putting an awareness poster in the workplace to remind employees about shoulder surfing attacks will make them look around before they key in their password.
- **Utilise the right delivery method**: The employees' education level clearly varies, and it is important to use the awareness method that fits the employees.

3.4 Key Challenges to the Effectiveness of Awareness Delivery Methods

Despite the presence of the best information security awareness programmes, obstacles exist that make the successful implementation of awareness activities more challenging. These common obstacles are explained below (ENISA, 2010; Qudaih et al., 2014; Banfield 2016)

- **Implementation of new technology**: It is well known that the adoption of new technology requires a new level of user understanding or a change in user behaviour in order that the user is capable of using this technology. This is not the issue. The awareness programmes are usually obsolete and not up to date due to the rapid development of information technology. Furthermore, at the specialist level, the awareness team may not be up to date or even have adequate knowledge regarding new technology and how to make employees more aware of the organisation's security policy.
- **On size fits all**: Some security awareness programmes are designed to fit all employees. This can lead to employees disregarding everything they have learnt due

to information overload. Therefore, the audience should be divided into classes in order to deliver targeted messages to each class. In addition, the awareness programmes should be designed specifically for the user classes, with each segment focusing on a particular awareness programme.

- **Too much information**: This is quite a common problem when organising awareness programmes, even after segmenting users into classes and sending targeted messages. Security awareness programmes seek to deliver as much information as they can. As a result, employees may get bored, with their enthusiasm for learning waning.
- **Lack of organisation:** Most security awareness delivery processes are inconsistent. It is necessary for awareness programmes to develop consistent communication with the audience.
- **Failure to follow up:** It is quite often observed that there is great enthusiasm at the beginning of any new security awareness campaign; however, after a period of time, this enthusiasm may dwindle or even disappear. Consequently, regular monitoring and updating of awareness programmes is highly recommended in order to evaluate what has been achieved. For instance, it is important to listen to employees and gather feedback from them in order to update awareness activities so they can fulfil the needs of employees.
- **No explanation of why:** Employees need to be educated as to why awareness is important; this concept is usually not fully understood by those organising information security awareness initiatives. An employee who fully understands why many types of behaviour are risky may alter his/her behaviour as a consequence, and employees need to be made aware of this.

- **Lack of management support:** This has a very important impact on information security awareness programmes. Managers have the power to deliver effective messages, and it is their responsibility to do so as a part of their role

3.5 The Significance of Information Security Awareness

The widespread increase in dependence on information technology in the daily work activities of employees at many organisations makes keeping this technology secure more of a challenge. If we view employees as the weakest link in the information security chain, awareness campaigns are the first line of defence. Moreover, an increased usage of Internet services results in threats to the security of information and many information security concerns. For this reason, many researchers and institutes have strongly emphasised the importance of information security awareness (Sherif et al. ;2016; Haeussinger & Kranz 2013; Bullee et al. 2015)

3.5.1 The need for security awareness

There is an increased need for information security awareness amongst end users in order to ensure that security culture is a part of their daily work. Therefore, it very important to make employees at all levels aware of their responsibilities regarding information security. This means encouraging users to be aware of the associated risks and motivating them to avoid these risks. Hence, security awareness teaches end users how to protect the organisation's information and how to take reasonable steps to prevent security breaches. The main aim of information security is to make positive changes to the end user's behaviour or correct current behaviour to make it compatible with the desired behaviour.

Therefore, information security awareness acts as a preventive measure, and many international standards, such as ISO 27005 COBIT, have referred to it as a prerequisite. Thus, if organisations aspire to a certification form of those standards, then it is necessary to

initially implement information security awareness plans. The main role of information security awareness can be summarised by the following points:

- To reduces the number of security incidents.
- To comply with international standards or best practice in information security.
- To cover all management concerns over the security of its information and systems.
- To comply with regulatory requirements.

The aforementioned points make clear the huge advantages of promoting information security awareness within organisations. Furthermore, it is widely known that in making end users aware of information security and the potential threats, the number of security risks will be reduced (Bauer et al. 2013).

3.5.1 End-users still unaware of information security

Increasingly, organisations perceive their employees as a great asset that needs to be cared for; however, at the same time they believe that employees are one of the biggest sources of threats to their cyber security (Nostro et al. 2014). Therefore, organisations often provide awareness and training to keep their employees sufficiently informed about the security requirements they should follow.

However, in spite of the great effort made by many organisations to promote information security awareness, employees are still unaware of security requirements (Parsons et al. 2014). This claim is strongly supported by the PwC (2015) report, which indicates that 75% of large organisations suffered a staff-related breach and nearly 31% of small organisations had a similar occurrence. The staff-related breach increased from 58% a year ago for large organisations and from 22% for small organisations, indicating that the problem is growing. Also, the report added that 72% of companies where the security policy was poorly understood had suffered staff related breaches.

Despite the rapid development in information security technology and protection tools, such as antivirus, firewalls and auditing tools, employees still partake in risky behaviour. Thus, it is not surprising that employees are one of the major underlying causes of breaches in information security. Apparently, the human factor is still the weakest link in the information security chain, while there is a movement and increase in the number of security threats. Table 3.2 below gives some examples of the lack of awareness among end users.

Table 3.2: The lack of security awareness among end users

Study Type	Results	Source
Annual survey and technical report.	• 72% of companies where the security policy was poorly understood had staff related breaches. • 75% of large organisations suffered a staff-related breach and nearly 31% of small organisations had a similar occurrence.	Information Security Breaches Survey, PWC (2015)
Annual survey and technical report.	• 57% of organisations considered employees the most likely source of an attack, with 38% viewing careless or unaware employees as the most likely threat. Compared to external threats, 46% of organizations saw the hacktivists as the most likely source of an attack.	The E&Y Global Information Security (2014)
Explorative study to investigate employee security awareness levels.	• 40.9% of respondents know the existence of information security policy. • 67.2 of employees are unaware of the password policy. • 52% of employees have given away passwords. • 77% of employees have left their computer unattended. • 74% of employees have clicked on unknown links. • 34% of employees have used inappropriate methods to store passwords.	Chan & Mubarak (2012)
Explorative study to investigate the knowledge and practice relationship between workplace and home environments.	• 37% of participants have logged off their computers whenever they leave a computer system. • 61% of participants never share their passwords. • 9% of participants change their password regularly.	Talib et al. (2010)

As illustrated above in Table 3.2, many end users are still unaware of the importance of information security and relevant organisational requirements. This is supported by of Chan and Mubarak (2012), who found that more than a half of employees are unaware of the existence of information security policy in their organisation. Apparently, password security policy receives little attention from employees, with 67.2% of employees being unaware of the password policy of their organisation. Moreover, very few employees (around 9%) change their password regularly. Furthermore, only around a third of employees adhere to a clean desk policy, which advises them to log off their computers when they leave their workstations.

Just over half of organisations consider their employees to be a major threat to their information security, and almost a third of them view careless or unaware employees as the most likely threat. Thus, employees' thorough understanding of security policy positively affects the overall security of an organisation. This is reflected in the PwC (2015) report, which found that 72% of the organisations where the security policy was poorly understood had staff related breaches.

3.5.2 The need for effective information security awareness methods

Employees must have an adequate level of awareness of the importance of information security and how to protect themselves against the increased threats. Technology solutions alone cannot provide complete protection. Therefore, employees' being aware of security requirements plays a supplementary role in the protection process.

Increasingly, organisations have paid attention to the importance of employees' awareness of information security. A variety of awareness delivery methods have been used to raise employees' awareness of how to protect themselves against cyber threats. Moreover, many organisations have allocated costly budgets to information security awareness campaigns.

Unfortunately, organisations still face threats and breaches originating from their employees. Non-compliance with security policies, whether due to deliberate behaviour or a lack of awareness, is still rife. This indicates the ineffectiveness of such awareness methods in terms of changing undesired behaviour of employees. These ineffective awareness methods have meant that organisations face challenges in terms of changing the noncompliant behaviours.

Chan and Mubarak (2012) conducted research to explore and investigate employees' awareness and knowledge of information security within an Australian organisation. The online survey was distributed, and around 308 responses were received. In this study, only 38.8% of the general staff were aware of their organisation's information security policy. A surprising result of this study was that around 77.3% of the participants had left their computers unattended or unlocked, and this was considered to be against the organisation's clean desk security policy. In addition, 59.1 % of the participants had no idea that an information security policy existed. Three main issues were cited based on the outcomes of this study: lack of knowledge of security concepts, lack of awareness of security policies and lack of information security awareness. The following table illustrates some significant results regarding the behaviour of employees' who took part in the study.

Table 3.3: Employee Behaviours (Chan & Mubarak 2012)

Action	Performed Action	Responses	%
Given away passwords or logged someone on using own password	Yes No	163 145	52.9% 47.1%
Left computer unattended and unlocked	Yes No	238 70	77.3% 22.7%
Used inappropriate methods for storing passwords	Yes No	105 203	34.1% 65.9%
Clicked on unknown links embedded in third party emails	Yes No	228 80	74.0% 26.0%
Amended data without confirming accuracy or authenticity	Yes No	24 284	7.8% 92.2%
Disclosed work related information on social networking sites	Yes No	23 285	7.5% 92.5%

(Khan et al. 2011) emphasise the importance of information security awareness programmes in order that users can understand their organisation's rules and regulations. However, they argue that such awareness programmes do not necessarily guarantee that every user will understand and obey the guidelines. To examine this issue, they measured the effectiveness of some methods currently used in information security awareness, as illustrated below in Table 3.4:

Table 3.4: The effectiveness of Information security awareness methods (Khan et al. 2011)

Tool or method	Knowledge	Attitude change	Subjective norms	Attention	Change in behaviour	Overall effectiveness (5)
Education Presentation	√	√	✘	√	√	**4**
Email Messaging	√	√	✘	√	✘	**3**
Group Discussion	√	√	√	√	√	**5**
Newsletters	√	√	✘	✘	✘	**2**
Video Games	✘	√	✘	√	✘	**2**
CBT	√	√	✘	✘	✘	**2**
Posters	√	√	√	✘	✘	**2**

Moreover, the mentioned awareness methods were evaluated based on their advantages and disadvantages, which appear in the following Table 3.5:

Table 3.5: Evaluation of security awareness delivery methods (Abawajy 2014)

	Methods	Advantages	Disadvantages
Conventional	Posters, stickers, leaflets, employee newsletter.	• Periodic information. • Can deliver more than one message at the same time.	• Too much information. • Often considered as spam.
Instructor led	Formal presentations or training sessions.	• Personally monitoring. • Instructional methods can be managed. • Employees' questions will be answered during the session.	• Expensive. • Some employees find it boring. • Depends on instructor experience.
Online delivery	Electronic articles or emails.	• Effective if employee reads it. • Not expensive • Periodic information.	• Often considered as spam. • Understood only by reading.
	Web based security awareness triaging.	• Friendly and flexible. • Employees can learn at their own place.	• Employees complete a training session within a minimum time • Leads to a feeling of isolation. • Becomes monotonous. • Fails in challenging employees.
	Security alert message e.g. logging messages	• Awareness message when there is a need.	
	Game based method	• Can challenge and motivate employees.	• Expensive and complex to implement. • Does not specifically reflect the security policy of an organisation.

To summarise, when conducting vital comprehensive security awareness training, organisations should concentrate on the weak points identified by assessing the information security awareness of their staff in order to raise the level of employee commitment to and support for the whole process (Bashorun et al. 2013). IT security is a continuous process rather than a project; therefore, IT security plans should be studied on a continuous basis, and professional teams should put policies and procedures in place supported by enough security awareness programmes. Furnell and Thomson (2009) indicate that the fact that most

employees do not pay enough attention to information security results in the organisation being vulnerable to significant security threats.

Providing training for employees on different security issues and how to best deal with them is the key to guaranteeing their security compliance. Therefore, the learning of users is a vital factor in guaranteeing more compliance with security policy. If users are convinced that security is necessary, they will appreciate that information security can help them as they go about their daily work. Consequently, security policy should be promoted during security awareness sessions to ensure more compliance. In order to guarantee more effectiveness, the security awareness programme should be built based on a well-considered strategy. During effective awareness programmes, users should be made aware of the following (Kenneth J. Knapp et al. 2009):

- A security policy is in place.
- The best ways for staff to access the security policy.
- The best practices to use to comply with it.
- How compliance will affect the operations of the organisation.
- The importance of protecting information assets.
- What the consequences of non-compliance are.

Equally important, a number of researchers have emphasised that for an awareness programme to be successful and effective, organisations need to target user behaviours (Northcutt 2014); (Peltier 2005). Moreover, organisations need to create awareness of the factors that cause threats or help make employees unaware of such threats.

3.6 Persuasive technology

Persuasive computing technology can influence people's attitudes and bring about some constructive changes in many domains, such as marketing, health, safety and the environment. Marketing is perhaps the most significant domain in which persuasive technology is used to encourage customers to buy products and services. For instance, in online shopping, Amazon's website has utilised this concept to encourage people to buy new products. When a customer is browsing for a specific item and showing some interest in it, persuasive computing technology will be used to offer the customer similar items which may be of interest to them. In the information security domain the application of persuasive technology could be of great value.

Thus, persuasive technology is fundamentally about learning to automate a change in behaviour (Fogg 2009). Actually, persuasive technology is interactive and it functions as tools, media and social actors (Fogg 1998). Table 7 explains these three functions of persuasive technology.

Table 3.6:The three functions of the Persuasive technology (Fogg 1998)

SN	Function	Essence	Persuasive affordances
1	Persuasive technology as a tool	Increases capabilities	• Reduces barriers (time, effort, cost). • Increases self-efficacy. • Provides information for better decision making. • Changes mental models.
2	Persuasive technology as media	Provides experiences	• Provides first-hand learning, insight, visualization, resolve. • Promotes understanding of cause/effect relationships. • Motivates through experience, sensation.
3	Persuasive technology as a social actor	Creates relationships	• Establishes social norms. • Invokes social rules and dynamics. • Provides social support or sanctions.

Persuasive technology can be used as a tool, such as in utilising systems or computer applications, in order to increase the capabilities of humans to perform actions they could not previously perform, thus facilitating the process. Persuasive technology as media can convey either sensory content, such as real-time video and simulations, or symbolic content, such as text, icons and data graphs. Finally, persuasive technology as a social actor can reward people with positive feedback, modelling target behaviour or attitudes and providing social support. Therefore, in order to raise information security awareness, technology persuasion can be utilised in three ways: as a tool, media and social actor.

Many strategies are used to influence, encourage, motivate and educate employees in relation to raising their awareness of important information security issues. Persuasive technology strategies may include: simplification, tunnelling, personalization, monitoring, conditioning and suggestion (Qudaih et al. 2014; Yeo et al. 2008; Nostro et al. 2014)

- **Simplification**: Simplify a process and decrease it to the minimum number of actions. Simplifying users' security responsibilities will assist them in understanding the required information security tasks. Therefore, security tasks need to be made easy by reducing them to as few steps as possible.
- **Tunnelling:** Provide guidance and support users, motivating them along the way. Use a sequence of tasks to make sure that users follow each step of the intervention process.
- **Personalization**: Personalise information for each user. A more personal approach, with customised information, is more persuasive than general information.
- **Monitoring:** A user's status or performance should be directly reported to the user himself. This will possibly help the user to correct behaviour in a secure manner and

in the line with the organisation’s information security rules. persuasion through observation

- **Suggestion**: Intervening at the right time. Context awareness will be used in this strategy.
- **Conditioning:** Reinforcing target behaviours. Typically, users underestimate the potential threats or risks in their cyber space and thus do not believe in the importance of behaving securely. Applying different methods of reinforcement can help form the desired behaviour or change current behaviour into more secure habits.

Qudaih et al. (2014) have indicated that using persuasive technology to disseminate policies and procedures can lead to effective information security awareness programmes. Distinguishing between groups of employees and only presenting information that is relevant to that particular audience is also a helpful technique.

A study by (Yeo et al. 2008) used the principle of persuasion technology (tunnelling strategy was used) to improve the information security awareness of end users. They evaluated the effectiveness of web-based programmes, which were developed in order to change the behaviour of users towards security awareness issues. Three significant aspects of information security were investigated in this study: password management, email management and virus protection. The research hypothesis was "there are no significant differences between pre-program and post-program attitudes towards the aforementioned aspects of security management”. The participants were 30 students (acting as end users), and they were required to complete the same instrument before and after attending the web-based programme. The research instrument, which was designed based on the theory of planned behaviour (TPB), measured users' beliefs by using a structured questionnaire. The study findings indicated that web-based programmes change participants' attitude and behaviour in

terms of security awareness issues in the investigated aspects: password, email and virus management.

3.7 Conclusions

This chapter has focused comprehensively on information security awareness and related issues. Various types of awareness methods have been reviewed to culminate in an overall comparison that has included the disadvantages and advantages of each type. Applying effective information security awareness programmes can be a challenging task; some obstacles still exist, such as the ‘on size fits all’ strategy, which may be easy to design and implement but is less effective. Moreover, finding a way to target the right employees at the right time is still a problem that needs to be solved.

Non-compliance with information security policies is a human issue rather than a technical one, and therefore using persuasive technology will help in the enhancement of such awareness programmes. Targeted awareness raising for employees who need increased awareness of a particular issue is one example of the use of persuasive technology.

In conclusion, it would be useful to study the potential behaviours of employees dealing with their security policies and the factors that affect their behaviour. To that end, the next chapter investigates the potential behaviours of policy users and then elaborates upon the human and organisational factors that may influence such employees.

Chapter Four

Users' Behaviour with Information Security Policies and the Affected Factors

4. Users' Behaviour with Information Security Policy and the Affected Factors

4.1 Introduction

The weakest link in the field of information security identified in the literature is the organization's employees (Metalidou et al. 2014). Modern organizations value the importance of IS since their daily work has become more and more dependent on their information systems. Information security policy compliance is one of the main challenges facing organizations today. Although implementing technical and procedural measures clearly helps to improve an organization's IS, the human factor or the employees' compliance with these measures is the key to success (Furnell & Clarke 2012). However, many organizations are now facing security issues associated with the extent of employee adherence to policy.

The main aim of this chapter is to provide a comprehensive overview of the characterization of user behaviour with organizational information security policy. A further aim is to investigate user behaviour in relation to information security policy. Moreover, the organizational and human factors that may influence the user's intention to comply with IS policy will also be discussed. Lastly, this paper will attempt to cover insider threats in relation to security policy.

4.2 User behaviour with information security policy

In the information security field, the human factor is the vulnerability considered to be the most unpredictable one. In addition, the human factor is characterized by being the most variable and thus the hardest to control. When organizations deal with the human factor, the procedure for placing staff with the right level of commitment to the policies of Information technology (IT) should contain an assessment of the security behaviour of individual

members of staff. According to Colwill (2009), organizations may believe that implementing more advanced technical controls will minimize the risk associated with the human factor. However, they should understand that this factor still poses the greatest threat and increases their vulnerability and thus consider a balance between technical and non-technical controls, maintaining a holistic perspective (Jones & Colwill 2008). As described in RSA/IDC research (Grant, 2009), security incidents that are caused accidently by insiders occur more frequently and can cause more harm than insider attacks executed with malicious purpose. As a result, organizations should fully comprehend the different types of compliance with the established IT security policies.

A number of studies have suggested that when the level of compliance with and acceptance of the established security policies and controls amongst the members of staff in an organization is measured, the success of those policies can be anticipated. Members of staff can show different levels of compliance. Furnell & Thomson (2009) name eight levels of compliance, starting with 'culture' and ending with 'disobedience'. These levels of compliance are associated with the security behaviour of employees. Figure 4.1 shows the different levels of user behaviour:

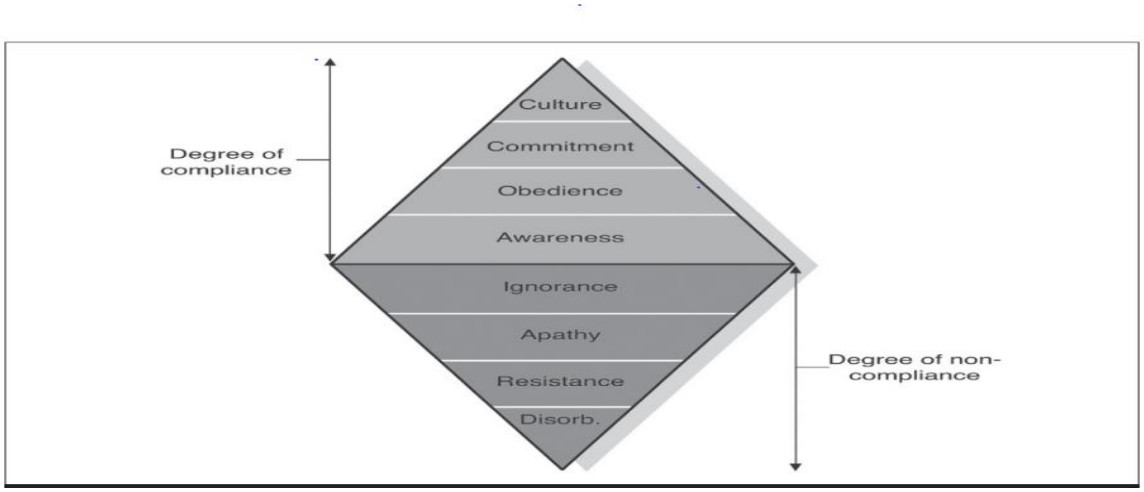


Figure 4.1:Expected distribution of compliance and non-compliance within an organization (Furnell and Thomson, 2009)

The following elaborates on Furnell & Thomson (2009) categories:

- **Culture (compliance)**: Security is a natural party of users' daily behaviour.
- **Commitment (compliance)**: Security is not part of the natural behaviour of users, but if they are given enough guidance and shown leadership, they will acknowledge the need and make an effort to comply.
- **Obedience (compliance)**: Users need to be given instructions rather than just guidance and leadership in order to comply.
- **Awareness (compliance)**: Users are aware of security but are not fully complying and not showing the required behaviour.
- **Ignorance (non-compliance)**: Users are unaware of security issues at this level and represent a higher risk of accidental adverse effects.
- **Apathy (non-compliance)**: Users are aware of the role they should play at this level but are not willing to show compliance as part of their behaviour.
- **Resistance (non-compliance)**: Users are aware of the role they are expected to play in security but are working against the aspects of the required practices they do not agree with.
- **Disobedience (non-compliance)**: Users intentionally break the rules and deliberately fail to comply with security and its established controls.

Alfawaz et al. (2010) mentioned that the success of IS in any organization is foremost related to employees' behaviour. Their study proposed four models to categorize user security behaviour, as follows:

- **Not knowing-not doing:** In this model, the user has no idea about the information security of an organization and does not have an understanding of the security requirements. As a result, the user will violate the security rules or not perform the right

behaviour. Usually, this situation occurs when a security policy is not in place or not delivered to the user in the correct way.

- **Not knowing-doing**: In this model, the user does not have an understanding of the security policy and is not provided with the IS requirements of an organization; nevertheless, the user performs the right behaviour by following the rules. Although the security policy is not in place or not properly delivered, the user shows awareness of the security requirements as they should be.
- **Knowing-not doing:** In this model, the user knows the necessary information about the security policy of his or her organization and has the required skills and knowledge; however, the user neglects to perform the right behaviour or violates the security policy. For example, even though there is a well-defined security policy in place and the user has knowledge about it, he or she intentionally ignores the security procedures regarding downloading Internet software.
- **Knowing-doing:** In this model, the security policy is in place and well delivered to the user; as a result, the user is carrying out the right behaviour. Therefore, the user's intention is not to violate the information security policy by following the required security rules.

4.3 Insider threats

Before presenting information on insider threats and their relation to information security policy, it is necessary to define the term 'insider'. An insider can be defined as an individual who has been granted privileged access to the computing environment (Nostro et al. 2014). This may include employees, partners and contractors who legally have the right to use the organization's information technology systems. Every employee or user of an organization is given a specific access level to perform his or her job and carry out their responsibilities. The users of information security policy can be divided into four major categories: pure insider,

insider associate, inside affiliate and outside affiliate (Roy Sarkar, 2010). Figure 4.2 illustrates the grouping of insider threats.

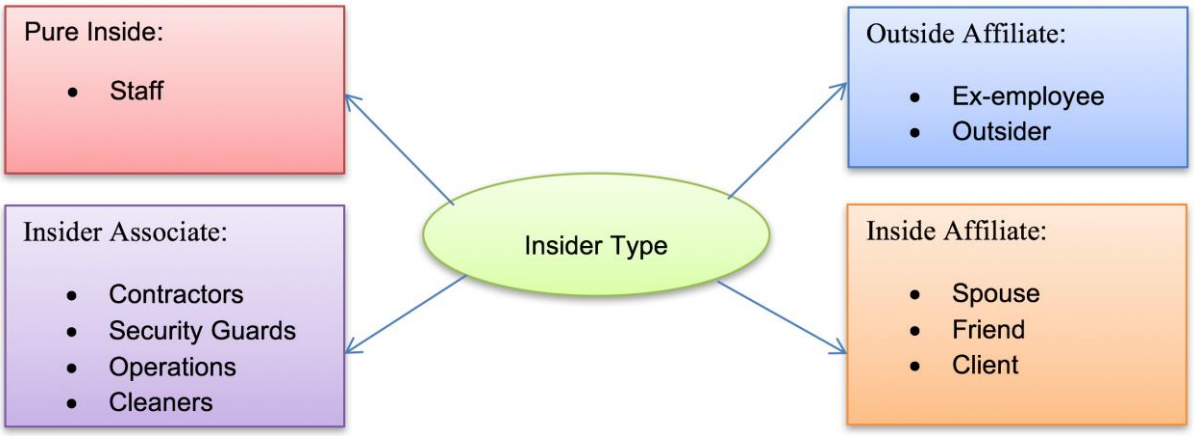


Figure 4.2: Grouping of insider threats

Insider threats are affected by a wide variety of issues: technical, organizational and behavioural, and should be tackled by technical controls, policies and procedures (Silowash et al., 2012). The possibility of insider threats causing damage to an organization has become real and substantial. Therefore, in recent years an increasing amount of literature has focused on the threats that may come from the inside an organization. Furthermore, several reports have indicated that threats from the inside, intentional and unintentional, have been one of the biggest threats to the security of information over the past decade (Yayla, 2011). For instance, in a survey conducted by CSI Computer Crime and Security (2009) 66% of the participants associated some of their losses with non-malicious insiders, while 16% of the participants believed that all of their losses were the result of the behaviour of non-malicious insiders (Richardson, 2009).

According to Magklaras and Furnell (2002), insider misuse can be accidental or intentional and labelled as unintentional insider threats (UIT) and intentional insider threats (IIT). The following diagram (Figure 4.3 explains the different types of insider threats.

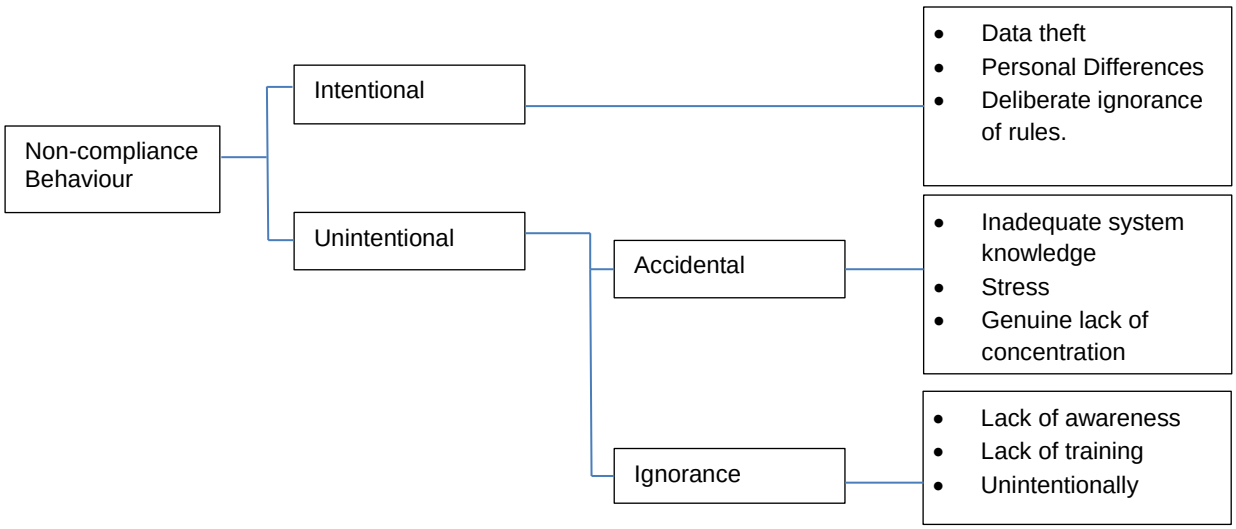


Figure 4.3: Non-compliance behaviour types

4.3.1 Intentional insider threats (IIT)

Intentional insider threats (IIT) involve an intentional misuse of computer systems by authorized users who have access to those systems and networks. The main motivation for this sort of threat is malicious intent to bring harm to an organization's information assets. Consequently, the malicious insider deliberately violates the availability, integrity and confidentiality of the computing environment of an organization. The most notable aspects of IIT are data leakage, espionage and the sabotage of information technology.

4.3.2 Unintentional insider threats (UIT)

Unintentional insider threats can be the result of non-malicious users making errors or of a failure in their performance that may affect information security (CERT® Division 2013). Human errors or mistakes made when dealing with information assets are a good example of unintentional threats that inadvertently violate IS policy in any organization. A significant number of organizations and security experts have emphasized the threats that come from inside the organization itself and 40% believe users' mistakes, such as data leaks or others

errors, are the greatest concern (AlgoSec, 2013). Greitzer et al. (2014) provide a comprehensive definition of UIT:

"*An unintentional insider threat is a current or former employee, contractor, or business partner who has or had authorized access to an organization's network, system, or data and who, through action or inaction without malicious intent, unwittingly causes harm or substantially increases the probability of future serious harm to the confidentiality, integrity, or availability of the organization's resources or assets, including information, information systems*".

An UIT incident typically occurs due to the behaviour of a non-malicious user when he or she is unaware of the IS requirements or as a result of committing an error. In a thorough analysis of UIT, Greitzer et al. (2014) identified various types:

- **DISC**: This kind of threat takes place as a result of a violation of confidentiality of information without malicious intent, such as when an employee inadvertently discloses confidential information to those who are not allowed to see it. For example, publicly disseminating sensitive information on a website, sending an e-mail to the wrong recipient or dealing negligently with sensitive information.
- **UIT-HACK**: This is an external attack via unaware users. An outside attacker uses tricks to deceive the insider user in order to achieve a malicious aim using malware and spyware. This is known as social engineering, and an infamous example of this is a phishing attack.
- **PHYS**: This is improper or accidental disposal of non-electronic records. The insider user is negligent in dealing with physical records, for example losing or discarding papers that contain sensitive information.

- **PORT**: This threat is a result of inadequate awareness when dealing with portable devices, such as laptops, smart phones, PDA, portable memory devices and CDs. An incident can occur as a consequence of lost, discarded or stolen data storage devices.

4.3.3 The difference between intentional and unintentional

As mentioned previously, violation of IS policies is associated with intentional behaviour, deliberate or non-deliberate. Firstly, intentional behaviour that leads to non-compliance with information security policy is due to the malice of the insider user. Thus, the user intentionally does not adhere to the information security policy of his or her organization in order to cause damage. However, not all intentional behaviour that leads to non-compliance is considered to be malicious. An example of this is a user intentionally violating an implemented information security policy due to a lack of awareness or even carelessness. Users whose unintentional behaviour leads to non-compliance may not be aware of security policies. Therefore, there are three main reasons for users unintentionally violating IS policy: awareness, negligence and errors (Elmrabit et al. 2015). The table below illustrates the main differences between the two categories of insider threats:

Table 4.1: The differences between the two categories of insider threats

Behaviour	Type	Description	Examples
Unintentional Behaviour	Unintentional without malicious objective	Inadvertent Violation: User errors or careless of implemented information security policy.	• Making sensitive or confidential information available to unauthorized people. • Sending email contents on sensitive data to the wrong recipient. • Storing information in an inappropriate location. • Non business related Web browsing. • Accidently deleting or modifying critical data.
	Intentional without malicious objective	Intentional violation without malicious motivation: user intentionally violate the implemented information security policy but without the intent to harm the organization.	• Sharing others' passwords. • Sharing sensitive information. • Improper disposal of information • assets. • Downloading or storing malicious software. • Hacker exploits users in a tricky way to provide information or a password they should not. • If the user is using a peer-to-peer file-sharing program to download music, this behaviour could inadvertently give outsiders access to confidential files on the computer.
Intentional Behaviour	Intentional with malicious objective	Intentional violation with malicious motivation: user intentionally violates the implemented information security policy with the intent to harm the organization.	• Inappropriate access or sharing of sensitive information.

4.3.5 Common insider threat indicators

An insider threat to an organisation's security may be exsting or developing over a period of time with some indications that can be categorized into indirect or "direct (EY 2016). Thus, each category of insider risk inductions needs different types of mechanisms of tracking. Direct risk indicators are abnormal activities that not within the daily work activities. For example, an employee downloads a large volume of date. However, indirect risk indications

are patterns of human behavior that require analysis to find suspicious behaviours. For example, a user is sudden overuse of negative emotive words.

The following points are some common insider threat indicators (EY 2016):

- Decline in work performance
- Irresponsible social media habits
- Attempting to bypass controls of an orgnisation's security
- Maintaining access to sensitive data after a user get a termination notice
- Visible disgruntlement toward employer or coworkers
- Addicted violation of an organization policies
- Utilizing of unauthorized external storage devices
- Requests for clearance or higher-level access without need

4.3.4 Insider threat mitigation

Insider threats can be mitigated but are not an easy problem to solve. They can be countered via multiple stages of defence that may consist of policies, procedures and technical controls (Silowash et al., 2012). Further to this, management needs to have an obvious vision regarding some significant aspects that can impact upon the organization, including its users, organisational culture, security policy and procedures, and technical environment.

Researchers have mentioned several factors that lead to insider threats, including the implementation of inappropriate security policy to protect the organization's information and its technology. However, having a suitable and up to date information security policy will not guarantee that violation of the policy does not take place because of human factors. Therefore, human factors are considered to be the key issue. Organizations need to

implement a detailed information security policy that covers all areas concerning cyber security and correlate this with the relevant human factors.

There is a direct relationship between the problems faced by many organizations and insufficient information security awareness and training efforts (Furnell, 2006). Security awareness and training can play a supplementary role alongside information security policy in reducing the number of potential insider threats (Munshi et al., 2011). If there is a comprehensive and effective information security culture in an organization and the users are applying it, this will make a difference.

In many organizations, security policy, procedures, guidelines, controls and training are not updated on a regular basis. In the (Economist Intelligence Unit EIU 2009a) survey, some IT specialists emphasized that their organizations had formal information security policy to regulate the usage of information resources by employees. However, only 21% of the surveyed organizations had given their employees suitable training on their information security policy. Worryingly, only 20% of the surveyed organizations had plans to increase security awareness in the future.

In their study of unintentional insider threats, Greitzer et al. (2014) highlight the importance of controlling those who unintentionally expose their organization to risks. In their work, they pointed out the problem and its potential causes and then suggested some mitigation strategies. One of their key findings was that poor situational awareness mainly increases the probability of human errors, such as mistakenly opening a phishing email. A summary of their UIT mitigation strategies is as follows: enhance the awareness of unintentional threats, increase motivation to avoid UITs, continuously train employees to perceive possible threats (e.g. phishing or social media threats), improve usability of security software and encourage employees to follow security policies and procedures.

4.3.6 Insider threat detection techniques

Over last decade, insider threat been extensively studied but still considered to be unsolved problem. In fact, many security incidents committed by users were detected after the fact by analysing user access logs.

In literature, many techniques have been designed and proposed in order to assist in detecting insider threat, the following is a summary of those techniques.

- **Anomaly based approaches:** based on documents accessed. Detecting misuse by monitoring user activity and classifying it as either normal or anomalous. Attempts to detect any type of misuse that falls out of normal behaviour (Sanzgiri & Dasgupta 2016) .
- **Role based access control:** analysing of user behaviour to see if it is expected. Matching user's behaviour with rules that specify violating behaviour of each role (Park & Giordano 2006).
- **Scenario based:** Ensemble based unsupervised technique and used structural and semantic information of an organization (Sanzgiri & Dasgupta 2016) .
- **Using decoys & honeypots:** decoy documents and honeypot techniques is used to lure and identify malicious user (Bowen et al. 2009).
- **Risk analysis using psychology cal factor:** case studies and real-world insider attacker symptoms are used to detect insider threats (Bowen et al. 2009). Moreover, personality indicators and language usage in text are used to detect insider threats by this technique (Greitzer et al. 2013).
- **Risk analysis using workflow: "**Organizational Structure and Workflow: To predict what characteristics cause security violations by system call analysis and signature" (Sanzgiri & Dasgupta 2016) .

- **Improving defence of the network:** using attack trees to strengthen the network security (Mathew et al. 2008).
- **Improving defence by access control: "**Extended Access Control based on abstraction of generalized attributes of data and people" (Greitzer et al. 2013).
- **Process control to dissuade insiders:** User's activities are audited and monitored of up to 60 days. This technique helps to streamline and improve incident response (Guido & Brooks 2013)

4.4 Factors that influence user's behaviour

Multiple research studies have attempted to identify the different reasons for the various levels of compliance with IT policies. In Kraemer et al. (2009), the authors highlight the way in which organizational and human factors have a direct relationship with technical computers and information security (CIS) vulnerabilities. The authors state that CIS vulnerabilities can be a result of factors other than technological or programming mistakes and that stakeholders should be more aware of the various roles that human and organizational factors can play in relation to CIS vulnerabilities. According to Badie & Lashkari (2012), the human factor is the most important factor affecting the security of computers. They categorize the factors that affect the security of computers into human and organizational factors.

4.4.1 Organizational factors

Although compliance with IS policy is first and foremost a human issue, organizational factors found to be influencing user's compliance have been explored in several studies. The following are some of the important the user's factors that may influence user compliance with information security policy:

- **Information Quality (Data flow)**

It is very important for any organization to have a comprehensive process of information security management. Inadequate information security policies or procedures can negatively contribute towards non-compliance with information security requirements. Moreover, poor communication or directions regarding these security procedures can impact upon user behaviour. Hence, inadequate organizational procedures may lead to a lack of skills, knowledge and ability to deal with information security requirements (Greitzer et al. 2014).

In the literature, information quality is generally seen as a factor strongly related to employees' compliance with information security policy. Pahnila et al. (2007) have proposed a theoretical model that contains the factors that explain users' information security compliance and one of those factors was the information security policy quality. In their research, 245 users have been surveyed to empirically support the proposed model. As a result, their study found that information quality has a significant effect on actual information security security policy compliance.

Likewise, Bulgurcu et al. (2010) have investigated the impact of information security policy quality on users ' intention toward compliance. In the research model, they proposed three quality dimensions: clarity, adaptability, and consistency. They conducted an online survey to collect data and to test their model, the participants was 464. Hence, their study highlighted the significant of the three information security policy quality toward employee's compliance with the security rules and regulations.

- **Motivation**

  According to Parsons et al. (2010), organizations must motivate their employees and convince them to embrace security practices and behaviour. Organizations must try to identify what motivates theirs staff to comply. As reported in Koh et al. (2005), when

security issues are shared and decision-making involves the employees of an organization, the level of employee motivation is raised.

Motivation can be used as a useful tool that helps in encouraging users to comply with the information security policy. A good example of the motivation is reward, defined as a tangible or intangible gift that granted to a complaint employee with the requirements of information security policy. This may include, an increase in salary, monetary or nonmonetary rewards, promotions, appreciation letter. In addition, rewards as an incentive have been utilized in some other areas, such as education, organizational behaviour and psychology, and it is considered to have a significant impact in changing behaviour (Bulgurcu et al. 2010).

Several studies have revealed that rewards exert a significant impact on an employee's perception of the benefit of compliance. For instance, Bulgurcu et al. (2010) empirically investigated the role of rewards to drive an employee to comply with requirements of the security policy. They tested their proposed model by collecting data via web-based questionnaire survey (sample of 464). Their research found that, rewards has a significant role to encourage users to comply with their security policy.

Perhaps, motivation means, such as rewards, may not necessary leads users to believe of that the security policy requirements are mandatory. However, rewards can still be utilized as a useful tool that encourages users towards compliance. Users should be informed that thy will be rewarded for their good behaviour with security policy.

- **Sanctions**

Existing literature have highlighted the importance of sanction in changing users behaviour towards compliance with the security policy and a number of studies have

offered empirical support. Bulgurcu et al. (2010) investigated the role of sanction on encouraging employees; randomly selected 464 responses were used to conduct the study. Their research results indicated that sanction are one of the important factors that influence the actual compliance of employees with the established security policies. A study conducted by Cheng et al. (2013) investigated the impact of sanctions on employees' compliance with information security policy, the study was conducted on 917, found that sanctions are one of the most important factors affecting the actual compliance of employees with established security policies

Similarly, a study conducted by Harris & Furnell (2012) on the influence of sanction on employees' compliance with IS policy, particularly using shaming as a deterrence technique. The quantitative methodology have been used this in study and 113 participants was surveyed, which are currently employed or previously had been employed in organization that have a formal security policy. As a result, 71% of the participants indicated that they would be more likely to follow IS policy, if their employers are willing to shame those who do not comply.

An example of a sanction is when an employee is penalized for her or his password being found written on a sticky note that is easily located on her or his desk. The severity of the imposed sanction can vary between organizations, but the employee will be subject to a severe penalty if he or she has been caught posting the password in a visible spot.

- **Awareness raising and training**

IS awareness is the level of understanding between members of staff regarding the role of IS and the level of security within their organization. The awareness level is achieved by conducting training and educating the staff regarding the role that they

can play in the success of security and the required changes in their behaviour to achieve that. Shaw et al. (2009) have argued that most of the current information security awareness programs fail to fill the gap between behaviour and perception. Some researchers believe that awareness of security policy counters the intention to misuse (D'Arcy & Hovav 2007;Al-Omari et al. 2011).

However, organizations are now facing difficulties in terms of maintaining defence measures and training users to keep up to date with the changing strategies used by malicious attackers (Sheng et al., 2010). An example of this can be seen in phishing attacks; organizations can easily decrease the probability of the success of such phishing attempts through anti-phishing education. Therefore, a productive and healthy working environment can be achieved by adopting a proactive approach to increasing security awareness in order to mitigate insider threats (Greitzer et al., 2014). The major aim of proactive mitigation strategies is to contribute towards increasing user awareness and motivation.

Previous studies on Information security have highlighted the important of security awareness on employees' behaviour. According to Bulgurcu et al. (2010), for investigating the impact of security awareness on employees intention to comply, an empirical study among 464 of employees has been conducted. This study found that awareness has a signification influence on employee's intention towards compliance. Another research, Puhakainen & Siponen (2010) have carried out an action research (a host company in Finland) to validate the training program for security policy compliance. There was four phases: identifying the problem, planning the training, delivering the training, and evaluating the results. In their research they developed a training program based on two theories: the universal constructive instructional theory and the elaboration likelihood model. Among 16 participants, the study suggests that

awareness and training program has as an impact on users' motivation to comply with security policy.

Chan & Mubarak (2012) in their study on 308 employees have concluded that a "lack of awareness and knowledge of policies may have allowed for staff to violate such policies".

- **Computer monitoring**

  The success of security countermeasures as a deterrence method relies foremost on users' action and their awareness of the existence of the security tools. Such security monitoring and auditing tools can be utilized in enforcing security policy in order to change unwanted behaviour. Therefore, once users are fully aware of these tools, would help to encourage their behaviour towards compliance.

  A number of studies have empirically provided evidence for the relation between computer monitoring and the complaint behaviour. These studies (Greene & D Arcy 2010) (D'Arcy et al. 2009b) found that an individual's information security compliance is influenced by computer monitoring and auditing tools. As such, monitoring tools assist in mitigating non-compliance behaviour.

- **Persuasions**

  Persuasion is part of our live and parcel of the human interaction. Fogg (2003) has explained persuasive technology (PT) as "interactive computing systems designed to change people's attitudes and behaviours". Persuasive computing technologies can influence people's attitudes and bring some constructive changes in many domains such as marketing, health, safety, and environment. Marketing is perhaps the most significant domain, in which the persuasive technologies are used to encourage customers to buy products and services

With regard to information security, the results of an empirical study by Yeo et al. (Yeo et al. 2008) suggest the significance of persuasive technology in changing end-users' behaviour. Furthermore, Qudaih et al. (Qudaih et al. 2014) indicate that using persuasive technology to disseminate policies and procedures can lead to effective information security awareness programmes.

In summary, the organizational factors are associated with an organization itself and these factors impacts differs from user to another. Table 4.2 shows a summary of the organizational factors and their influence on user behaviour.

Table 4.2: Summary of the organizational factors and their influence on user behaviour

Factor	Description	Empirical support	Sources
Information Quality (Data flow)	The facilitating conditions and information quality have a significant impact on user compliance behaviour.	✓ Theoretical model (Participant:245)	Pahnila et al. (2007)
		✓ Theoretical	(Greitzer et al. 2014)
		✓ Theoretical model (Participant:464)	(Bulgurcu et al. 2010)
Motivation	Motivation such as rewards has a significant impact on a user perception of the benefit of compliance.	✓ Theoretical model (Participant:464)	(Bulgurcu et al. 2010)
		✓ Theoretical	Parsons et al. (2010)
Sanctions	Sanctions are one of the important factors that affect the actual compliance of employees with the established IS policies.	✓ Theoretical model (Participant:464)	(Bulgurcu et al. 2010)
		✓ Questionnaire (Participant:113)	(Harris & Furnell 2012)
		✓ Questionnaire (Participant:917)	(Cheng et al. 2013)
Awareness & training	There is a direct influence of information security awareness on user compliance behaviour.	✓ Theoretical model (Participant:464)	(Bulgurcu et al. 2010)
		✓ Action research (Participant:16)	Puhakainen & Siponen (2010)
		✓ Questionnaire (Participant:308)	(Chan & Mubarak 2012)
Computer monitoring	Computer monitoring tools are negatively associated with information security policy non-compliance intention.	✓ Theoretical model (Participant:223)	Greene & D Arcy (2010),
		✓ Survey (Participant:304)	(D'Arcy et al. 2009b)
Persuasion	Persuasion technology can raise security awareness	✓ Experiment + Survey (Participant:30)	(Yeo et al. 2008)
		✓ Theoretical	(Qudaih et al. 2014)

4.4.2 Human factors

Achieving compliance with information security policy would not be an easy task without the interaction of users, and therefore controlling user behaviour in relation to these policies is the key to success. In the literature, several human factors have been investigated by many researchers and reported to have an impact on user behaviour, whether negative or not. Below are some of the factors that may influence the user's intention to comply from the perspective of the author:

- **Perception (Situation Awareness)**

  Perception is considered to be a key component of human behaviour and a major part of intelligence (Proctor 2006). In other words, human interpretation or recognition with sensory information has a considerable impact upon user behaviour. Yenisey et al. (2005) stated that the perception of IT users has a great impact on their behaviour and decisions. A study by Huang et al. (2011) regarding users' perception of IS found that their perception is determined by several factors, such as awareness, knowledge, controllability, severity and possibility. If there is a gap between the real level of in=formation security and the security perception of end users, their behaviour and decisions will be influenced accordingly Huang et al. (2011).

  Essentially, having a complete image and full awareness of what is occurring in the IS space will positively impact upon the ability of users to recognise potential threats. In his theoretical situational awareness (SA) model, Endsley (1995) categorised SA as follows:

  - **Level 1 (perception)**: The first step to gaining situation awareness is perception of status, attributes and dynamics of the environments and its relevant elements.

- **Level 2 (comprehension)**: The next step in SA formation includes understanding elements of level 1 via pattern recognition processes, interpretation and evaluation. Level 2 SA requires the integration of this information to understand how it will affect the objectives and goals of the individual. This includes a comprehensive picture of the world or that part of the world of interest to the individual
- **Level 3 (projection):** The highest level of SA and action can be taken at this stage. The accumulated knowledge of level 1 and level 2 will be translated into an act, which results from perception of the situation.

Situational awareness can be considered as knowledge about a particular domain. Generally, having adequate SA leads to effective decision-making and assists in reducing the potential user error rate. In other words, unintentional insider threats, such as errors, might be correlated with poor understanding of SA rather than poor decision-making. In the computer world, when users have incomplete or inadequate SA, the organizational risks will be increased by user errors that may lead to computer systems failures. Therefore, employees should be kept up to date with the latest threats patterns and their security requirements. An example of this is a user being unaware of a phishing campaign, which may lead to failure to maintain network security. This is a result of non-perception (Level 1).

- **Personality**

In psychology, five traits are often used to describe human personality: openness, agreeableness, extraversion, conscientiousness and neuroticism. Table 4.3 shows these personality traits and the characteristics they may form.

Table 4.3: personality traits and the poles of characteristics they form (Costa and McCrae 1985)

Openness	Conscientiousness	Extraversion	Agreeableness	Neuroticism
Fantasy Aesthetics Feelings Actions Ideas Values	Competence Order Dutifulness Achievement Striving Self-Discipline Deliberation	Warmth Gregariousness Assertiveness Activity Excitement Seeking Positive Emotion	Trust Straightforwardness Altruism Compliance Modesty Tender-mindedness	Anxiety Hostility Depression Self-Consciousness Impulsiveness Vulnerability to stress

According to (Shaw et al. 1999), there are six main characteristics that have a direct influence on malicious users behaviour:

- False sense of entitlement
- Personal and social frustrations
- Ethical flexibility
- Reduced loyalty
- Lack of empathy

A Study performed by (Shropshire et al. 2006) investigated the nature of the relationship between these personality traits and information security compliance behaviour. The research sample was one hundred and twenty users. The research model was based on the five major personality traits, and the final result was that conscientiousness and agreeableness have a significant impact on user compliance with IS.

Another study designed by Mcbride et al. (2012) to provide such knowledge about individual personality tails that shape behaviour and impact users intention to comply with security policy. They implemented and empirically validated a comprehensive

theoretical model that aim to assessing the impact of personality factor. Among 481 participants the ultimately result of research was that more Open, Conscientious, and Agreeable participants were more likely to comply with the security policy. Conversely, participants who have more Extroverted and Neurotic were more likely to violate IS policy.

- **Technology democracy**

  The systems and applications that are used at work and at home have converged and interweaved over recent years. Some applications that were used in home environments are now used in business systems as well. This will pose a challenge to the status quo of the technology used in the organization (Colwill 2009). As reported by (Economist Intelligence Unit EIU 2009b) users demand more freedom to use a wider variety of applications and devices to do their work more effectively, which can be classified as asking for more 'technology democracy'. According to Colwill (2009), when more mixing between the work environment and the home environment occurs, it is expected that employees will be more likely to demonstrate ignorant behaviour regarding security. As demonstrated by the National Computing Centre (Mohamed 2009), staff members are more likely to fail to establish a boundary between their work and home environments, and they can fall into the trap of 'trusting innocence' and start posting personal and business information on social networks.

  In the (EU 2009) survey, it was demonstrated that the training and guidelines offered in addition to the set security policies and controls were failing to keep up with changes. Most of the executives who took part in the survey claimed that although their organizations had written IT policies to control and organize the use of websites, applications and devices, only a few of them had interacted with employees to make sure they understood and complied with these guidelines. Only 21% of these

organizations gave their employees training on the use of personal communication devices and only 17% provided training on the use of social networks. Most worrying is that only 20% of the organizations were planning awareness campaigns for their staff in the future.

- **Cultural factors**

  According to (Colwill 2009), organizational culture and regional/national culture must be considered when analysing insider threats since these two factors directly affect the effectiveness of levels of information protection and behaviour. Usually, it is difficult for westerners to understand some of the cultural, religious and societal pressures of others communities. According to Crossler et al. (2013), the majority of Behavioural InfoSec research has been conducted within western cultures, which limits its applicability to other cultures; however, some studies have been conducted within Asia and elsewhere. To elaborate more regarding the cross-cultural differences, the Chinese culture is an example of a highly collectivistic one, while the American culture is an example of a highly individualistic one. At another level, the culture within an organization or corporate culture must be analyzed to comprehend how employees behave. This corporate culture can exist even though members of the organization are not consciously aware of its existence (Furnell & Thomson 2009). Hence, the key challenge is to add security culture to organizational culture when the former is not a fundamental part of the latter.

- **Gender**

  Munshi et al. (2011) have argued that gender in relation to insider threats is rarely investigated in the academic literature. However, the importance of gender as an

influence on behaviour has been cited in the academic literature in the form of reported incidents. In Hanley et al.'s (2011) study 94% of insider incidents were committed by males. Research by Cappelli et al. (2009) attained similar results. However, some reports argue that both genders pose an equal threat to information security. For instance, a study by Kowaski et al. (2008) found that 50% of insider threats were associated with females and 50% with males.

- **Satisfaction**

  Satisfaction or employee satisfaction is defined as an employee's overall feeling of well-being at work. It is widely believed that employee who is satisfied with his or her employer is more likely to comply with organization's information security policy. Therefore, users who report positive feelings about their organizations are expected to have a big picture regarding their responsibilities especially in term of the compliance with IS policy.

  A number of studies investigated the relation between job satisfaction and the compliance of employees. These studies provide empirical support for the positive impact of job satisfaction on compliant security behaviour. For example, Greene & D Arcy (2010) examined the influence of job satisfaction factor on user's security policy compliance decision. In their theoretical research model they postulate that satisfaction is positively associated with security compliance intention. The research model was tested on 223 survey participants and the result suggested that job satisfaction contribute to the information security policy compliance. Hence, there is a link between job satisfaction and compliant behaviour; higher job satisfaction will motivate users to comply.

- **Habits**

  A habit is automatic or unintentional behaviour, as opposed to conscious behaviour. Thus, automaticity is the key element of the habit constrict. Usually, habits can be evaluated by measuring previous behaviour or behavioural frequency. Habit theory suggests that people perform many actions without making conscious decisions and then get accustomed to performing these actions. There is an argument that habits explain information technology usage. It is argued that the actual behaviour of users is highly influenced by their technology usage habits. In this vein, some researchers are of the opinion that habitual behaviour explains information security policy non-compliance. Pahnila et al. (2007) investigated the factors that impact upon users' compliance via a theoretical model; one of these factors was the users' habits. Empirical support was provided for their model by over 245 participants from a Finnish company. The study showed that users' habits have a significant impact on intention to comply with information security policy. Another study by Herath & Rao (2009) came to the same conclusion regarding the impact of habits on user behaviour. Therefore, it is very important for any organisation to get its employees into the right habits; safe ones that help them to comply with information security policy. Changing users' behaviour or breaking old habits of dealing with information assets is not straighforward. However, organisations can mitigate this issue by: identifying the problem, finding solutions and monitoring the effectiveness of those solutions.

In summary, human factors are associated with the user and the impact of these factors differs from user to another. Table 4.4 shows a summary of the human factors and their influence on user behaviour.

Table 4.4: Major human factors that influence user's behaviour

Factor	Description	Empirical support	Sources
Perception (Situation Awareness)	Human interpretation or recognition of sensory information has a considerable impact upon user behaviour. Perceived benefit of compliance.	✓ Theoretical	(Proctor 2006)
		✓ Expermint (Participant:64)	(Huang et al. 2011)
Personality	There is a relationship between these personality traits and information security compliance behaviour. For example, carelessness can make user incompliance.	✓ Survey +Experiment (Participant:481)	(Mcbride et al. 2012)
		✓ Theoretical model (Participant:120)	(Shropshire et al. 2006)
Technology democracy	Users demand more freedom to use a wider variety of applications and devices to do their work more effectively, which can be classified as asking for more 'technology democracy'	✓ Theoretical	Colwill (2009)
		✓ Online Survey (Participant:390)	(EU 2009)
		✓ Theoretical	(Mohamed 2009)
Cultural factors	Organizational culture and regional/national culture must be considered when analysing insider threats since these two factors directly affect the effectiveness of levels of information protection and behaviour. Culture lead to increased compliant security behaviour	✓ Theoretical	Colwill (2009)
		✓ Survey (Participant:232)	Greene & D Arcy (2010)
		✓ Theoretical	(Furnell & Thomson 2009)
Gender	There is an opinion that males are more likely to be non-compliant with information security policy than females.	✓ Technical report about violations, In the 550 extracted cases, 94 % of the insiders were male	(Hanley et al. 2011)
		✓ Technical report	Cappelli et al. (2009)
Satisfaction	Job satisfaction increases the intention of user to comply to IS policy.	✓ Survey (Participant:118)	Xue et al. (2011),
		✓ Survey (Participant:232)	Greene & D Arcy (2010)
Habits	Habits, have a significant effect on employees' compliance with IS policy.	✓ Theoretical model (Participant:245)	(Pahnila et al. 2007)
		✓ Theoretical model (Participant:312)	(Herath & Rao 2009)

4.5 Conclusion

As mentioned in the introduction, information security policy is considered to be the first line of defence against any potential threats posed by employees. In the workspace, all employees should be encouraged to be aware of what constitutes acceptable and unacceptable behaviour,

and the first step to achieving this is the implementation of proper formal information security policy. Organizations should realize that having security policies is as significant as having a firewall, intrusion detection system or any other security solution**.**

Organizations should pay more attention to the possibility of insider threats and the impact that they may have on their computing environment. The procedure of placing staff according to their level of commitment to information security policy should contain an assessment of the security behaviour of individual members of staff. In this regard, the level of user compliance with the security policy, which differs from one user to another, has been highlighted here as reported in the literature. Moreover, some important factors that may impact upon the user's behaviour in relation to security compliance have also been explained.

To conclude, organizations repeatedly suffer harm from employees who are not obeying or complying with their information security policies. As such, the human element is still the weakest link in the information security chain, causing an increase in the number of security threats. In the literature, a number of factors have been studied to have a direct impact on user behaviour in relation to information security policy, such as awareness, monitoring, motivation, deterrence, and persuasion.

According to the awareness factor, awareness raising has a significant influence on an employee’s intention to comply. However, information security policies are promoted through traditional information security awareness methods, although these delivery methods have some shortcomings in their effectiveness as mentioned in the previous chapter. There is a need of delivering an effective awareness method to the end users based on their actual behaviours. Therefore, by subjecting user to continuous and targeted awareness, the level of user’s compliance would raise, each user will be subjected to targeted awareness if they do not comply.

A monitoring factor also has a significant impact; security monitoring and auditing tools can be utilised to change unwanted behaviour in order to enforce information security policy. Therefore, once a user is fully aware of being monitored by security monitoring tools, would help to encourage their behaviour towards compliance. However, security monitoring tools are not integrated or work in one framework in order to monitor and process users' behaviours. Moreover, organisations use these tools only to enforce their security policies, without using the concept of response taxonomy for non-compliance behaviour. For example, categorise a response to the non-compliance behaviour into two categories: awareness raising and enforcement, in which the response severity can be escalated from the first category.

Furthermore, the use of persuasive factor in motivation behaviour change has recently gained the attention of many researchers as it is a useful approach to promoting behaviour change, and it is now being applied in many domains, such as marketing. Personalising persuasive strategies, each user is given targeted security awareness based on their behaviour (events), and the awareness type will focus mainly on the part of the security policy that they have violated rather than on all the security policy.

Motivation and deterrence also has a significant impact on users' perception of the benefits of compliance. Rewards and sanctions can be used as motivation and deterrence, respectively. A good example on that would be utilizing the concept of scoring points system, but not yet used within the security policies domain. Therefore, it would be an effective method, using a compliance points system to reward compliant behaviour, and penalise noncompliant behaviour.

In the next chapter, a holistic model is proposed for raising the level of compliance amongst end-users. The factors of awareness, monitoring, motivation, deterrence, and persuasion are used in one model. The proposed model is build based on two main concept: a taxonomy of

the response strategy to non-compliance behaviour, and a compliance points system. The response taxonomy is comprised of two categories: awareness raising and enforcement of the security policy. The compliance points system is used to o motivate deter users to be compliant with the policy, as well as, measuring their compliance rate with the security policy or any element of it.

Chapter Five

A Model for Monitoring End-User Security Policy Compliance

5. A Model for Monitoring End-User Security Policy Compliance

5.1 Introduction

With the aforementioned challenges and influencing factors of a successful implementation of an information security policy (described in the previous chapters), the necessity for a dynamic response to user behaviour is becoming more apparent. The author has proposed a novel model, which aims at increasing the compliance level of a user by monitoring and measuring their behaviour. The model is intended to provide a comprehensive framework for raising the level of compliance amongst end-users, with aims of monitoring, measuring and responding to users' behaviour with an information security policy. In addition, a scoring points system (compliance points system) is used to apply supplementary rules within the proposed model. The goal of utilising the compliance points system is to motivate users to be compliant with the policy, as well as measuring their compliance rate with the security policy or any element of it. By using this model, each element of the security policy is measured, which provides organisations with a clear vision about their security policies. For example, an organisation can determine which element of its policy has a minimum or maximum number of violations during a certain period of time.

The model for monitoring user's security policy compliance is a holistic framework to mitigate the problem of non-compliance with information security policies, by continuously monitoring users' behaviour in relation to the policies and help organisations in raising compliance levels of their users. This model can be customised to suit an organisation's needs, that may differ from one organisation to another.

The foremost aim of this framework is to increase users' awareness of the importance of following information security policies. Continuously subjecting users to targeted awareness and monitoring their adherence to information security policies should enhance the

effectiveness of such awareness efforts. The novelty of the proposed framework depends upon three significant aspects: monitoring, a response taxonomy and using a compliance points system. All of these aspects are utilised to enhance the awareness and compliance of end-users.

This chapter provides detailed information regarding the model of dynamically monitoring user behaviour using a compliance points system, and to theoretically clarify how it can be implemented. The main concept and idea behind the model is illustrated in this chapter, explaining the details of how it works.

5.2 Information security policies and monitoring user behaviour

The proposed model is built upon two major aspects: information security policy and behaviour of users (monitoring user behaviour).

5.2.1 Information security policies

Security policy is defined as ‘a formal document that describes the acceptable and unacceptable behaviour of users in relation to how they deal with information assets in a secure manner’ (Disterer 2013) . Computer users should have a clear vision of the basic prevailing security policy that is in their organisations. An example of security policy types may include: acceptable use policy, confidential data policy, email policy, password policy, clean desk policy, internet usage policy and physical access policy. Each type or category of an information security policy contains many elements (known as policy elements), which are a set of statements in which each element describes a particular issue or behaviour that a user should adhere to. For instance, Table 5.1 comprises 20 elements from different categories or types of security policies (SANS 2014a).

Table 5.1: Examples of security policy elements

Category	Policy Elements
Clean desk policy	Computer workstations must be locked when workspace is unoccupied.
	Employees are not allowed to remove or disable anti-virus software.
	Passwords must not be left on notes posted on or under a computer, and must not be left written down in an accessible location.
	Electronic storage devices, such as USBs and DVDs that contain restricted information, should be kept secure.
	Computer workstations must be shut down completely at the end of the working day.
Password policy	User level passwords, such as those used for application, web, email and desktop accounts, must be changed every four months.
	Passwords must not be added to or written in an email message, transmitted in any electronic form or revealed to anyone over the phone, via a questionnaire or in a security form.
	All passwords should meet or exceed the following guidelines: contains at least 12 alphanumeric characters, contains both upper and lower case letters, at least one number and at least one special character.
	Users are not allowed to utilise password memorisation, which is available in some applications as an additional feature, such as the web browser 'remember password' feature.
Internet usage policy	Employees must not download, visit or view any illegal materials on the internet.
	Employees must not undertake deliberate activities that wastes staff effort or networked resources.
	Personal use of the internet must not cause a significant increase in resource demand.
	Employees must not download unauthorised software or files for use without prior authorisation from the IT department and their manager.
	Employees must not play any games on the internet.
	Employees must not download copyrighted material, such as music media (MP3) files, film and video files (not an exhaustive list) without appropriate approval.
Email usage policy	The organisation's email account should be fundamentally utilised for business that is related to the organisation.
	"The organisation's email system must not be utilised to create or distribute any offensive or disruptive messages. For example, offensive comments about age, disabilities, sexual orientation or religious beliefs.
	Sending chain letters or joke emails from an organisation email account is strictly prohibited.
	Employees must not send unprotected, sensitive or confidential information externally.
	Forwarding of the organisations confidential messages to external locations is not allowed.

All elements of the information security policies in Table 5.1 are used as examples in the proposed model to demonstrate how it works. The proposed model suggests each element of the security policy should be handled separately, with user's behaviour regarding each element tracked and monitored. A scoring points system (compliance points system) is used to track compliance levels of users over time. Specifically, the compliance points system concept grants points for compliant behaviour, and deduct points for unacceptable behaviour.

Moreover, a best practice approach for ITIL and COBIT 5 (services for information security management) can be intergraded in the proposed model. The Information Technology Infrastructure Library (ITIL) is a framework of best practices that promote quality computing services in IT sector. ITIL can help companies assess their risks, and put procedures in place to log and respond to incidents. And it is widely used for the implementation of information security within an organization (Sheikhpour & Modiri 2012).

COBIT 5 (Control objectives for information and related technologies) is s a good practice or a framework for the governance and management of the organisation's information technology. Provides a comprehensive framework that assists organisations to achieve their aims and deliver value through effective management and governance of the organisation's information technology (ISACA 2012).

5.2.2 Monitoring user behaviour

Security events (violations of the security policy) are recorded using two methods: from security monitoring and control devices (e.g. in cases where a user spends a lot of time on social networks or has not changed his password for a long time) or manually from security reports or line managers (e.g. in cases where a user leaves their computer unlocked). The event sources may include, but are not limited to:

- Line managers: who can input manually reports of any behaviour that does not comply with the information security policy, such as a user writing down their password or leaving their computer unlocked.
- Internet usage: many organisations believe that threats coming from the internet are the biggest concern. When employees use social networks, downloads and cloud storage services without complying with the security policy that has been specifically created for internet usage, there is a potential threat to an organisation. a local agent on a network traffic or proxy can gather data about a user's behaviour regarding the internet usage policy.
- Email usage: a local agent on an exchange server can gather data about a user's behaviour regarding the email usage policy.
- Application level, such as active directory: an active directory is a database that keeps track of all user accounts and passwords. A local agent on the active directory or applications level can gather data about user behaviour regarding the password policy.
- User machine: The most secure technique used to monitor an end-user PC is to install a piece of software as a host that works with a server or an appliance (Strohmeyer 2011). a local agent installed on the user's computer can monitor their behaviour regarding policy elements such as turning off any anti-virus software.

Many sources, such as a web gateway, an active directory, SIEM, network traffic, auditing tools and the user's computer can be used to collect data about users' behaviour within the computing environment. Monitoring a user's compliance with the information security policies will depend upon the nature of each element of the policy. Table 5.2 illustrates some elements of the security policy and the potential methods to monitor user compliance of these elements:

Users' privacy is very important aspect that an organisation should be aware of it. Therefore, the users should be informed that the monitoring process will not breach their privacy, it only for find specific behaviour or noncompliance behaviour. For example, in case of password policy, user's password itself will not be monitored, only the creation date and attributes of passwords will be monitored.

Table 5.2: Potential methods of monitoring user compliance with policy elements.

Policy elements	Indicator	Data source required	How the data source is used to provide indicator
Computer workstations must be locked when workspace is unoccupied.	Unattended workstations identified.	Manual, through manager observation.	Line manager, or personnel from an information security department, will manually input the event of an unattended workstation.
		Local agent in user's computer.	WIN 32 API (Application Programming Interface), is a set of functions and data structures that a Windows program uses to ask Windows to do something from WIN 32, such as finding out the last time any input was given to the system, from the keyboard, mouse, etc. This is possible by using a function called *GetLastInputInfo*. Another important function in the same frame is called *OpenDesktop*. A call to the OpenDesktop API (using the *DESKTOP_SWITCHDESKTOP flag*), followed by a call to the *SwitchDesktop* API (using the handle returned by *OpenDesktop*) will determine which condition, locked or unlocked, exists in Windows. By using these two functions, the duration of idle time of an unlocked computer could be extracted from WIN API.
Passwords must not be left on notes posted on or under a computer, and must not be left written down in an accessible location.	Observation of users writing passwords down.	Manual, through managers or IT department observations.	Line manager, or personnel from an information security department will manually input the event of a password being written down and left in an accessible location.
Electronic storage devices, such as USB and DVDs containing restricted information must be kept secure.	Storage devices that are unsecure or unsafe identified.	Manual, through managers or IT department observations.	Line manager, or personnel from an information security department will manually input the event of unsecured devices being identified.
The organisation's email account should be fundamentally utilised for business that is related to the organisation.	Any misuse of an organisation's email identified.	Email exchange server (Email Gateway)	Monitoring and cataloguing all users email addresses, both sent and received. Personal messages can be monitored by determining recipients from the business contact list on the email exchange server, and examining the message content.

The organisation's email system must not be utilised to create or distribute any offensive or disruptive messages. For example, offensive comments about age, disabilities, sexual orientation or religious beliefs.	Misuse of an organisation's email by creating or distributing offensive or disruptive messages identified.	Email exchange server (Email Gateway)	Monitors for key words to flag a suspicious alert, leading to manual intervention to assess validity before the system records it as an information security policy violation.
Sending chain letters or joke emails from an organisation email account is strictly prohibited.	Chain or joke messages identified.	Email exchange server (Email Gateway)	Monitoring message content using a content filter agent, working against a list of black words or phrases.
Employees must not download, visit or view any illegal materials on the internet''.	Any attempts to visit prohibited websites by the user identified.	Web Proxy	Web proxy is an intermediary between a user's web browser, e.g. Internet Explorer, and the internet, storing a copy of frequently used webpages. Therefore, it has a cache memory to do so It can be used to improve security by performing web content filtering.
		Network traffic	Monitoring external internet activity and tracking access attempts against blacklisted sites. An organisation can configure its firewall to report on websites accessed, according to user name and/or computer name. Enterprise-level perimeter firewalls, such as Microsoft's ISA Server, Cisco PIX, and CheckPoint Firewall-1, either have built-in reporting features or have add-ons available to provide reports of websites accessed through the firewall and from what account and computer they were accessed.
Personal use of the internet must not cause a significant increase in resource demand.	High traffic volume by the user for personal usage identified.	Network traffic	Monitoring a white list of web addresses irrelevant to the organisations business, e.g. BBC, to see how much network traffic is generated towards these sites.
Employees must not download unauthorised software or files for use without prior authorisation from the IT department and their	Unauthorised software on a user's computer identified.	Local agent in a user's computer.	Obtain system information through Windows Management Instrumentation (WMI) calls. The WMI class and property keeps information about what occurs on a machine. Use the ExecQuery method to query the Win32Reg_AddRemoveProgram class. This query returns a collection consisting

manager.			of all the software installed on the computer.
Employees must not play any games on the internet.	Evidence of user having played an online game identified.	Local agent in a user's computer.	Examine cached Web files. Usually Internet Explorer keeps useful information all the websites that have been visited by a user. The agent can be instilled locally in the user machine against a black list of games websites.
		Monitor web access at the firewall or through network traffic	Monitor external internet activity and track access attempts to blacklisted sites.
User level passwords, such as those used for application, web, email and desktop accounts, must be changed every six months.	Stale passwords identified.	• Active directory • On each application level • Email exchange server.	Identifying a passwords last date of change. Each password or account has a set of specific attributes, including the last set date that can be used to investigate any stale passwords. In the active directory (AD) there is a special attribute called''pwdLastSet'' that gives information about passwords ages for each user. It would be easy to use script to query the AD user objects and the''pwdLastSet'' attribute.
Passwords must not be added to or written in an email message, transmitted in any electronic form or revealed to anyone over the phone, via a questionnaire or in a security form.	Written passwords identified.	Email exchange server	Monitors for key words to flag a suspicious alert leading to manual intervention to assess validity before the system records it as an information security policy violation. Therefore, an agent can be instilled in the email exchange server to monitor message content against a list of key words or phrases.
Users are not allowed to utilise password memorisation, which is available in some applications as an additional feature, such as the web browser 'remember password' feature.	Investigate if a user has used a password memorisation tool.	Local agent in a user's computer.	The internet browser can be monitored to decide if the user has utilised password memorisation feature or not. Many internet browsers such as Internet Explorer, Gaoogle Chrome and Firefox keep information about users' accounts, such as Origin ULR, account name, password itself, created time and password length.

5.3 Overview of the model

The proposed model aims to enhance the compliance level of users based on two main concepts: taxonomy of the response strategy for non-compliant behaviour, and utilisation of the compliance points system.

Organisations can choose the suitable response taxonomy for non-compliance behaviour that covers their needs. However, in the proposed model the response taxonomy is suggested to comprise two categories as a default setting:

Category 1: Raising awareness of the security policy

Category 2: Enforcement of the security policy

Following the compliance points system, an employee who complies and shows desired behaviour will earn points, but non-compliant behaviour will result in removal of points.

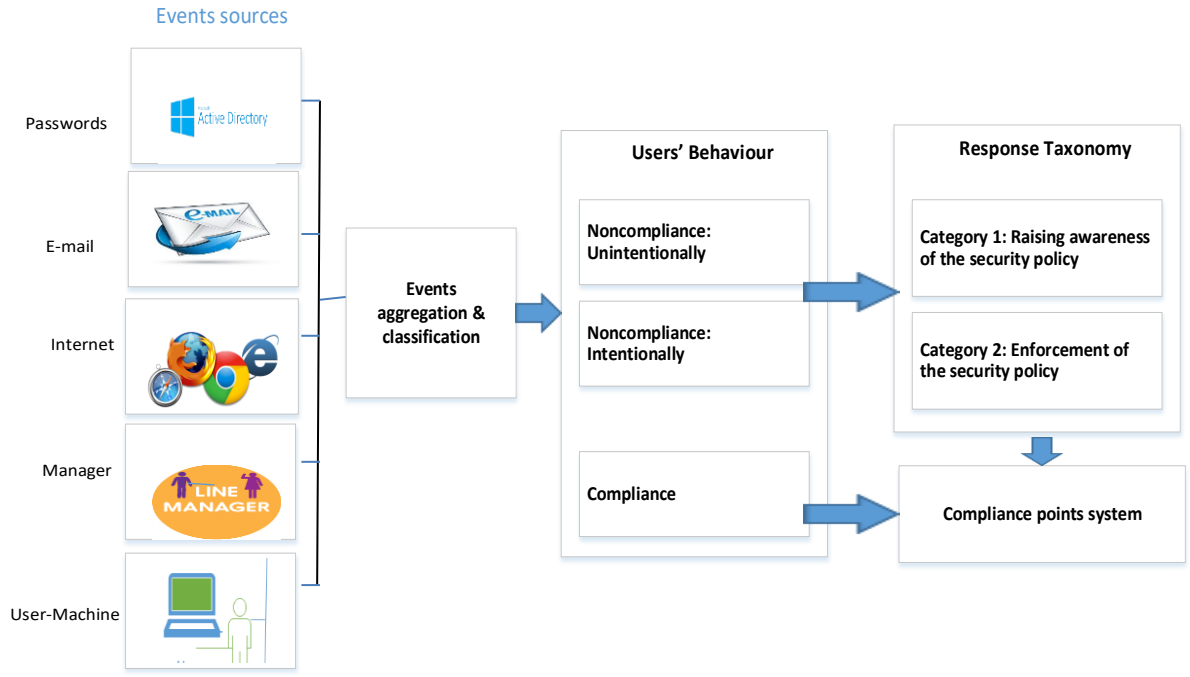


Figure 5.1: Outline of proposed model

5.3.1 Users' behaviour

Three potential user behaviours regarding the information security policies have been identified: unintentional non-compliance, intentional non-compliance and compliance. These behaviours are considered throughout the proposed model.

1- Compliance behaviour: user shows the desired behaviour of compliance with the information security policy.
2- Unintentional non-compliant behaviour: non-malicious user behaviour, resulting from a lack of awareness of the information security policy.
3- Intentional non-compliance behaviour: user deliberately violates the information security policy, established through frequent non-compliance of the same action within a set time period.

5.3.2 Response taxonomy for non-compliance behaviour

Employee violations of security policies are considered as a key concern for organizations. Many organisations currently use the traditional methods to promote and increase users' awareness of the security policies. However, these methods have their limitations, which have been discussed previously during this research, such as one fit all. Furthermore, enforcing an information security policy using technical solutions, which is one level of the response to a user's behaviour, is widely used in many organisations. However, simply one level or only enforcing the policies may inappropriate way to encourage users to be compliant. Therefore, the targeted response to the user behaviour using multi levels of responses, which is escalated from raising awareness until the enforcement of the policy may change the culture of the users towards the compliance.

Thus, a response strategy will be in place for non-compliant behaviour, to raise awareness and enforce the information security policy. The framework has two categories of response for non-compliant behaviour: (1) Raising awareness of the security policy, (2) Enforcement of the security policy. Each category is composed of sub-responses, which are designed to increase severity levels in a gradual manner, as shown below:

Category 1: Raising awareness of the security policy (two levels of escalation)

- Level 1: Yellow Warning and a security policy reminder issued in writing (Basic raising of awareness).
- Level 2: Orange Warning and web-based awareness training or video-based awareness reminder (Advance raising of awareness).

Category 2: Enforcement of the security policy (three levels of escalation)

- Level 3: Red Warning.
- Level 4: User's manager informed of situation.
- Level 5: Direct intervention and enforcement of the security policy by reducing IT privileges, limiting access or blocking access completely.

This model proposes five levels of response to non-compliance behaviour, in which the severity of the response to any violation is escalated from Level 1 to Level 5. However, organisations can customize these levels of response to the number that suits their individual needs, for example an organisation may wish to have three level of responses rather than five.

5.3.3 Compliance points system

The main aim of compliance points is to encourage users to be compliant with their information security policy. It is also used as an indicator of the current compliance level of each user with each element of the security policy. The compliance points' system relies upon two major aspects: Firstly, a user compliant with the information security policy earns

points as a reward for good behaviour, and their compliance points' credit accumulates after each compliance action. Secondly, any violation of an information security policy results in reducing points from any they may have accumulated.

Each element of the information security policy has its own compliance points' tracker. Using a separate tracker on each element is useful for promoting targeted awareness, based on monitoring the compliance level for each element. There is also an overall aggregated value of compliance points for each user regarding the whole information security policy.

Users should be notified about the monitoring process and they should know about their compliance points and consequences they may counter in case of noncompliance behaviour. Therefore, an organisation should have a plan to deliver all this information to the users.

Compliance rates of users are used as triggers for certain actions or responses within the proposed framework. For instance, continual earning of compliance points or a high level of compliance rate is a significant sign of an employee's adherence to the security policy. However, a trend in losing compliance points is a sign of non-compliant behaviour, either intentional or unintentional. The current level or state of compliance points can be used to launch motivational actions or rewards for that behaviour, which may include:

- Gratitude letter or email for being a compliant employee.
- Informing Human Resources (HR) to update an employee file.
- Awarding an employee with a mention on a board of excellence (Staff Excellence Award).
- Awarding a bonus or voucher for use in organisations facilities.

5.4 A model for monitoring end-user security policy compliance

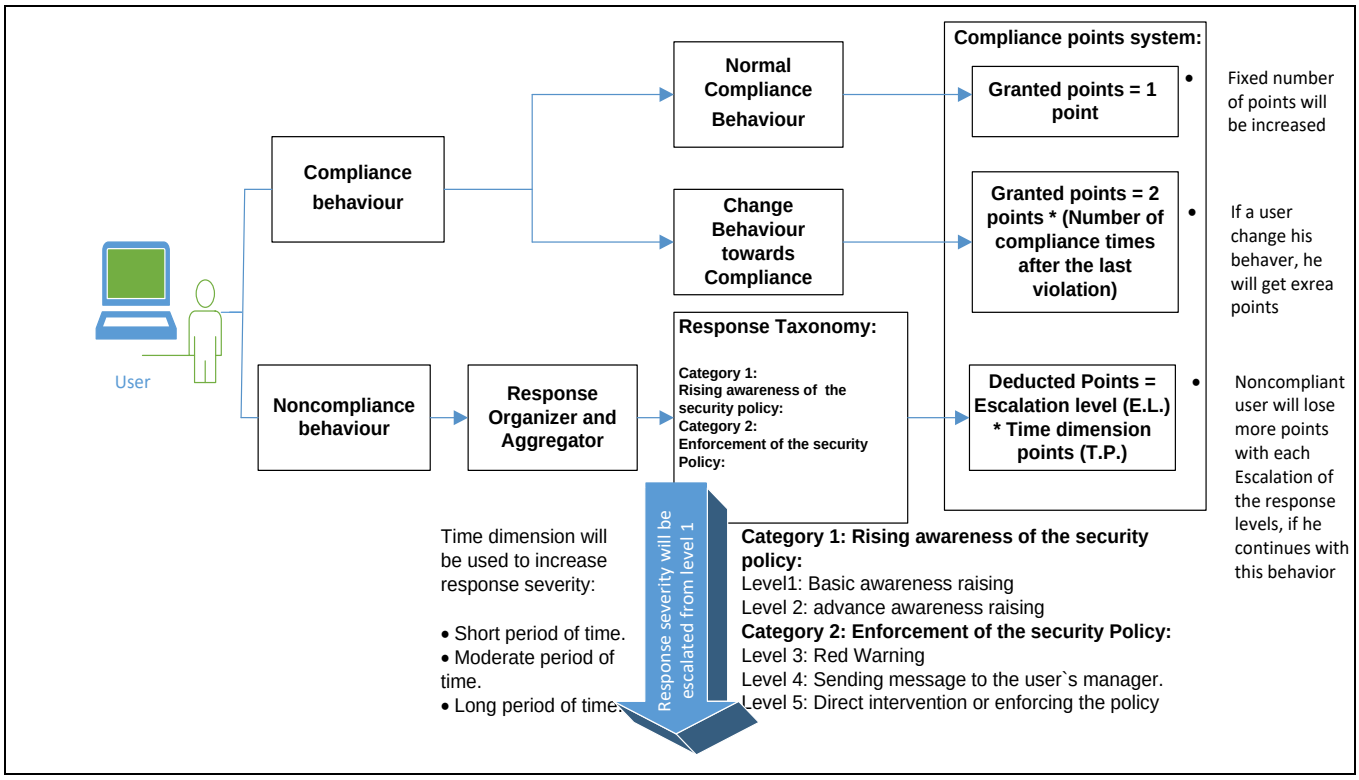


Figure 5.2: A model for monitoring end-user security policy compliance

As mentioned previously, there are two kinds of user behaviour with regards to the information security policy: compliant behaviour and non-compliant behaviour. The proposed framework, detailed in Figure 5.2, aims to dynamically monitor user behaviour in relation to such information security policies. In addition to that, the compliance points system is used to track levels of the compliance of users. The following sections explain the model in more detail.

5.4.1 Compliance behaviour

A user is considered to be compliant when they show the desired behaviour regarding the information security policies and rules. To measure compliance, two methods of evaluating users' behaviour are suggested:

1- Based on the explicit action, for when a user performs certain actions of compliance, for example, they have changed their password after six months in response to the policy requiring this specific action (the changing password policy);

2- Based on the elapsed period of time (the compliance period), considers a user as compliant if they do not violate a security policy during a set period of time, for example, if a user has not browsed non-work related websites for a period of three months.

A user that adheres to the information security policies earns compliance points for behaviour in relation to each element, and each element of the information security policy has a separate tracker of points for each user. There are two mechanisms for granting points: points awarded for normal compliance behaviour, and points awarded for changing behaviour towards compliance (see Figure 5.3).

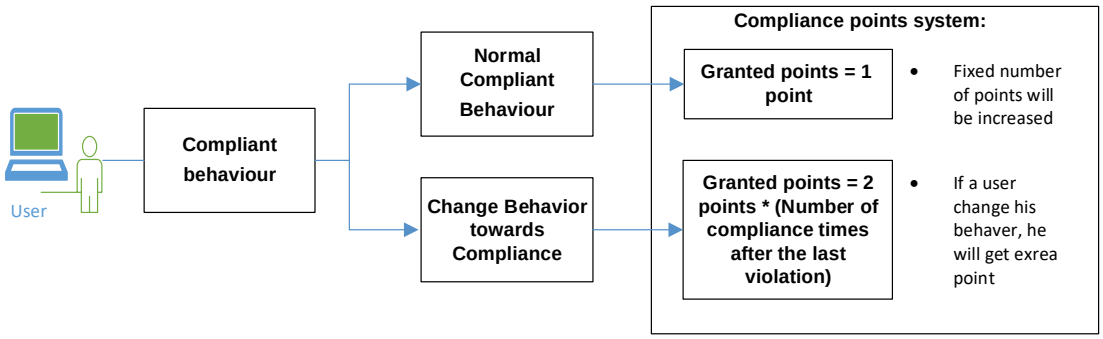


Figure 5.3: Dealing with compliance behaviour

5.4.1.1 Normal compliance behaviour

It is desired behaviour that users adhere to the information security policy that is a part of their culture. This behaviour is granted 1 point as a reward for each commitment to each separate security policy element (Granted points = 1 point).

To demonstrate, the following scenario in Table 5.3 assumes that User A has performed compliant actions in relation to two different elements of a security policy - changing password security policy and non-browsing of non-work-related websites policy:

Table 5.3: Example of normal compliance behaviour: User A

#	Actions and date	Policy description
Action 1	User A changed his password - 01-01-2016	Passwords must be changed every six months.
Action 2	User A changed his password - 01-06-2016	
Action 3	User A did not browse non-work-related websites - 01-01-2016 to 01-03-2016	Browsing non-work-related websites is prohibited.
Action 4	User A did not browse any non-work-related websites - 01-03-2016 to 01-06-2016	

According to Table 5.3, User A earns four points for his security compliant behaviour regarding the two elements of the policy. The first action earned 1 point when they changed their password in compliance with the changing password security policy, with total points for this policy at 1 point. The second action also earned 1 point when User A changed their password for a second time, bringing their total for the password changing policy to 2 points. The third action earned 1 point when User A was compliant for three months, and as a result the total points for non-browsing non-work-related websites will be 1 point. Likewise, in the fourth and last action, User A will earn another point for being compliant with the non-browsing of non-work-related websites security policy, and as a result the total of these particular security policy elements will be 2 points.

5.4.1.2 Changing behaviour towards compliance

The second mechanism is for users who change their behaviour from non-compliance towards compliance. The aim of this mechanism is to encourage users to continue complying with the security policy in order to earn extra points, gradually recovering the lost points from

previous non-compliant behaviour. It assists in replenishing what has been lost in points in a quick and gradual manner. The proposed equation for this mechanism would be:

*Points of changing behaviour = 2 points * (No. of compliance actions after the last Violation of the same policy element)*

The following Figure 5.4 shows how the points are granted for the two mechanisms of compliance (normal compliance behaviour and changing behaviour towards compliance):

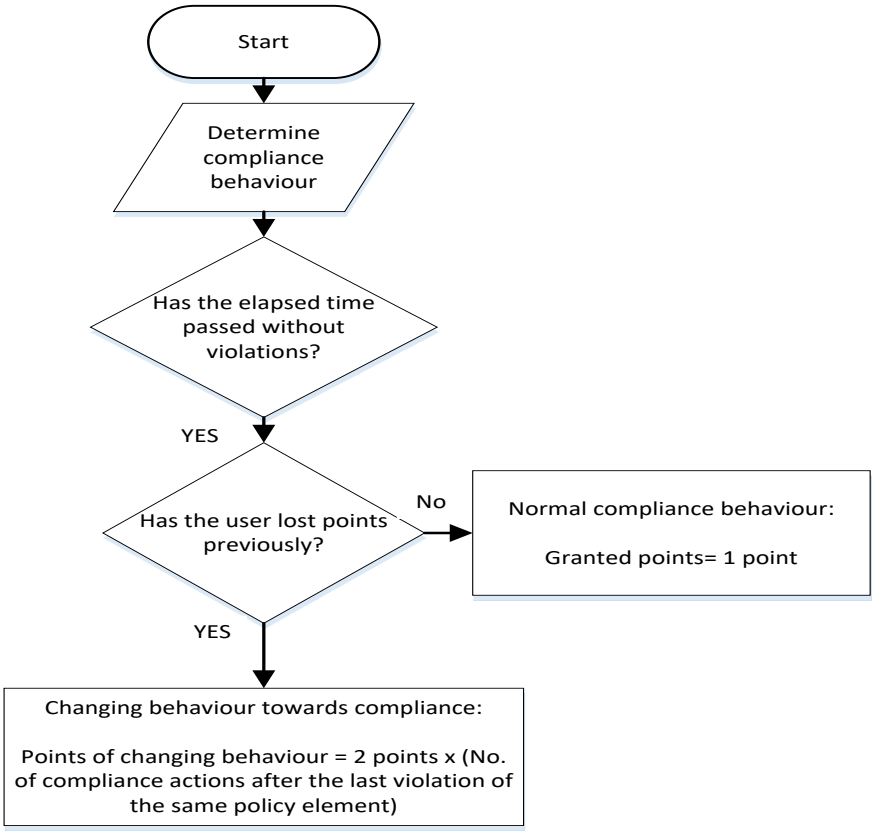


Figure 5.4: Granting points for compliance behaviour

The following scenario is illustrated using Table 5.4. User B has not changed their password for 24 months, and this policy requires it to be changed every six months. Due to this non-compliance behaviour, user B lost points four times (24/6 = 4). Following this, they changed their behaviour to be in line with the changing password policy. As a result, User B earns

more points each time they comply with the policy until they have recovered the lost points for that element. These three actions are shown in the table below.

Table 5.4: Example of changing behaviour towards compliance: User B

#	Action and date	Points earned
Action 1	User B changed his password - 01-01-2016	*Points earned = 2 x (No. of compliance actions after last violation)* Points earned = 2 x 1 = 2 points
Action 2	User B changed his password - 01-06-2016	Points earned = 2 x 2 = 4 points
Action 3	User B changed his password - 01-12-2016	Points earned = 2 x 3 = 6 points

In Action 1, User B earned 2 points for being compliant with this element of the policy, and because this action was the first compliance after the last violation. In Action 2, the points earned by User B have increased to 4 points because it was the second compliance, so the total points for this policy element are now 6 points. In Action 3, the third compliance of the user changing their password earned 6 points, with the total for the policy becoming 12 points. User B has gradually gained points by changing their behaviour towards compliance, however, this mechanism is stopped when the user recovers their lost points and they are switched back to the normal compliance mechanism.

There may be a circumstance where an organisation wishes to grant more than 1 point for a particular element of the security policy if it believes an element is more important than the others. If an organisation wishes to promote certain behaviours due to higher importance or difficulty, then more points could be granted for specific behaviour. For example, if an organisation has a concern about users accessing social networks, it can award more points for users who comply with the internet usage policy. Table 5.5 illustrates the potential ways to grant points for compliant behaviour.

Table 5.5: Compliance points for compliance behaviour

Behaviour	Points earned
Normal compliant behaviour.	1 point earned for each instance of compliance.
Changing and maintaining behaviour towards compliance.	2 points x (No.of compliance actions after last violation) will be earned by the user each time until they recover any lost points. The extra points are a reward for positively changing behaviour.
Compliance to elements with higher difficulty or importance.	More points earned as a reward for particular elements, totals determined by the organisation.

5.4.2 Non-compliance behaviour

Non-compliance behaviour of users is evaluated on an explicit action that leads to the violation of the security policy, such as downloading unauthorised software. Non-compliance behaviour is subjected to various levels of response, in conjunction with the points system (see Figure 5.5).

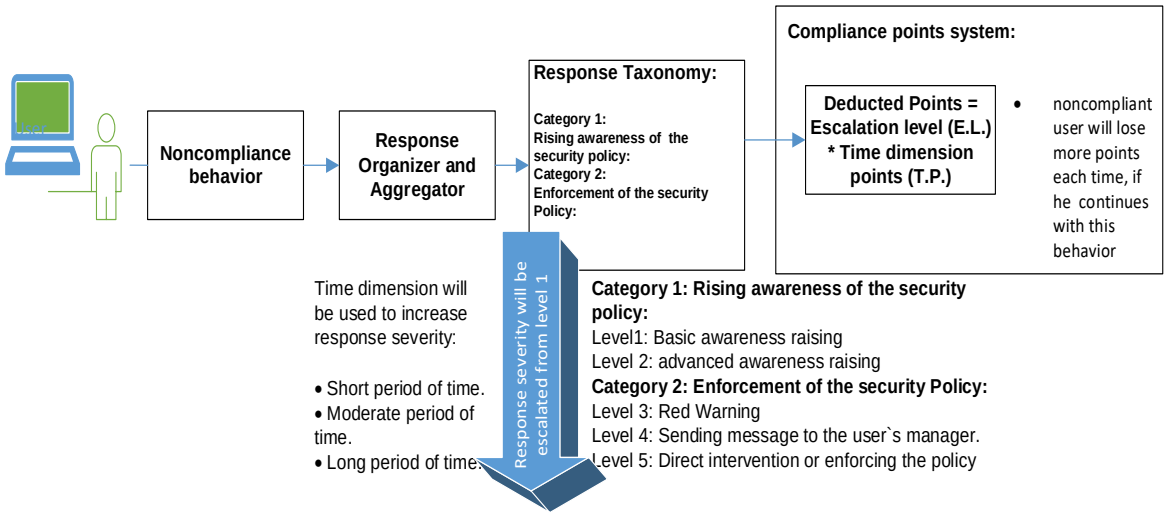


Figure 5.5: Dealing with non-compliance behaviour

5.4.2.1 Response organiser and aggregator

The aim of this component is to organise the process of responding to non-compliant behaviour. The level of response is determined by this component, as is the number of points to be deducted. The aggregation concept is used to determine the method of the response. For

example, if the response is an email to the user's manager, then the response aggregator considers other violations from other users, to be aggregated in one email.

5.4.2.2 Response taxonomy

There will be a response strategy for non-compliance behaviour to raise awareness or enforce the information security policy. Thus, the framework has two potential categories of response to the non-compliance behaviour: (1) Raising awareness of the security policy, (2) Enforcement of the security policy. Moreover, each category is composed of a variety of sub-responses, which have been designed for increasing the severity levels in a gradual manner.

Category 1: Raising awareness of the security policy (Two levels of escalation)

Level 1: Yellow Warning &Written security policy reminder (Basic awareness raising)

Level 2: Orange Warning &Web-based awareness training program or video-based awareness reminder (Advance awareness raising).

Category 2: Enforcement of the security Policy (Three levels of escalation)

Level 3: Red Warning

Level 4: Sending message to the user's manager

Level 5: Direct intervention or enforcing the security policy e.g. reducing privileges of accessing resources or blocking access to some IT resources

Time dimension is used as an indicator for increasing response severity up to the next level. Time dimension refers to the period of time between violations of the same security policy element. In other words, over what period of time the non-compliance behaviour has happened since the last violation in relation to a particular element of the policy. There are three types of time dimension:

(1) Short period of time

(2) Moderate period of time

(3) Long period of time

Table 5.6 clarifies the three types of time dimensions.

Table 5.6: Time dimension types

Time dimension	Duration	Expected behaviour	Escalation to the next level
Short time	Set as a short time, e.g. less than 1 day (24 hours).	Users may be unaware of the information security policy and repeat the same violation, perhaps four times within ten minutes.	There will not be enough time for any significant intervention, the sequence of events occurring in a very short period of time. All repeated events in this time duration will be considered as a single event, and there will be no escalation in this type of time duration.
Moderate time	Set as a Moderate time, e.g. From 1 day up to 6 months.	Users may be aware of the information security policy and frequent violations occur in a moderate period of time, perhaps over four days. This implies a user is not learning from known mistakes.	Intervention is required, escalating the response severity to the next level.
Long time	Set as a Long time, e.g. 7 months or longer.	Users may forget details of the information security policy, due to long period of time.	In this instance, users will require an awareness reminder from Category 1: raising awareness of the information security policy.

The three types of time dimensions (Short time, moderate time and long time) would be configurable by the organisation itself, but the author has set the recommended defaults values of the three types as shown below.

1- Short time dimension = less than 24 hours as a default value. Because, there will be not enough time for any significant intervention, so the time should be short.

2- Moderate time dimension = from 24 hours up to 6 months as a default value. Because, there will be enough time since the last violation and the user should be received a response for the last violation.

3- Long time dimension = more than 6 months as a default value. Because, the period between the new violation and the last violation should be long period of time because the user is considered as a forgotten user.

To demonstrate the time dimension effect on the response strategy for non-compliance behaviour, Table 7 describes the following scenario. User C has violated a particular information security policy, policy 1, many times over a two-year time period. The time dimensions, used in the response strategy for these violations have been assigned the following time values:

1- Short time dimension = less than 24 hours

2- Moderate time dimension = from 24 hours up to 6 months

3- Long-time dimension = more than 6 months

Table 5.7: User C violations

Violation No.#	Description	Date
Violation 1	User C violated policy 1 for the first time	01-01-2015
Violation 2	User C violated policy 1 for the second time	05-01-2015
Violation 3	User C violated policy 1 for the third time	07-02-2015
Violation 4	User C violated policy 1 for the fourth time	07-02-2015
Violation 5	User C violated policy 1 for the fifth time	07-05-2015
Violation 6	User C violated policy 1 for the sixth time	01-05-2016

User C has violated this policy six times over two years. The first violation was on 01-01-2015, and the response level was set to Level 1, basic raising of awareness. As such, because it was the first violation, there is no time dimension between the current violation and the past violation, therefore in this case the response level is considered as level 1.

The second violation occurred on 05-01-2015, four days after the first, so the time duration was considered as moderate. User C was considered to be intentionally violating the security policy for the second time, therefore the response level was escalated from Level 1 to Level 2, advanced raising of awareness.

The third violation on 07-02-2015 came nearly a month after the second violation. The time dimension was considered as moderate time dimension and the response escalated to Level 3, Red warning.

The fourth violation occurred the same day as the third, so the time duration was considered a short time dimension. There was no escalation of response because both violations occurred in a short period of time, so response severity remained at Level 3.

The fifth violation was on 01-05-2015, two months after the fourth violation, and was considered a moderate time dimension. The response escalated to the next level, Level 4, informing the user's manager.

The sixth violation happened on 01-05-2016, 1 year after the previous violation, which was now considered as long-term dimension. As a result, there is no response escalation to the next level, and the required response is only Level 1, basic raising of awareness.

As described in this scenario with User C, the escalation of response for non-compliance behaviour is determined by the time dimension type. The response strategy consists of five levels, in which the escalation process is based on the time dimension type. The next step is to integrate the compliance points system with the response strategy.

5.4.2.3 Compliance points system for non-compliance behaviour

For any non-compliance behaviour, the user loses points from their compliance rate, with different procedures applied each time the level of response severity is increased against that

behaviour. The amount of points deducted increases gradually after each escalation of response severity for the same violation. The number of deducted points relies on two factors:

1) Escalation level

2) Time dimension points

The escalation process of response from one level to the next is based on the time dimension type, short time, moderate time or long time, and is used in the points' deduction equation. Each type of time dimension has a points value: short time = 1, moderate time = 2 and long-time = 1. Table 5.8 demonstrates how time dimension is used.

Table 5.8: Time dimension points

Time dimension	Duration parameters	Expected behaviour	Escalating to the next level	Time dimension points (T.P.)
Short time dimension	Short period of time, e.g. from 1 second up to 1 day (24 hours).	User may be unaware	No escalation to next level.	1
Moderate time dimension	Moderate period of time, e.g. from 1 day up to 6 months.	User is aware	Escalation to the next level required.	2
Long time dimension	Long period of time, e.g. from 7 months or longer.	User may have forgotten	No escalation to the next level. Only a reminder from category 1	1

A user loses points for continually violating the same security policy element and ignoring each escalation level of response. The escalation level of a user and the time dimension type affects how many points the framework deducts. An equation of the proposed technique is as follows:

*Deducted Points = Escalation level (E.L.) * Time dimension points (T.P.).*

The E.L. value is based on the escalation level the user already has, and is used together with the time dimension points outlined in Table 8.

The second variable in the equation would be the time dimension. There are three types of time dimension, which are short period of time, moderate period of time and long period of

time, and each type is assigned a particular point: short period of time =1, moderate period of time = 2 and long period of time =1.

Table 5.9: Deducted compliance points for non-compliance behaviour

Response taxonomy	Escalation level	Deducted point(s)
Category 1: Raising awareness of the security policy	Level 1: Yellow warning and security policy reminder issued in writing (basic raising of awareness)	Deducted points = E.L. x T.P. If Time dimension is short, T. P.= 1: Deducted points = 1 x 1 = 1 point If Time dimension is moderate, T.P.= 2: Deducted points = 1 x 2 = 2 points If Time dimension is long, T.P.= 1: Deducted points = 1 x 1 = 1 point
	Level 2: Orange warning and web-based awareness training or video-based awareness reminder (advanced raising of awareness)	Deducted points = E.L. x T.P. If Time dimension is short, T.P.= 1: Deducted points = 2 x 1 = 2 points If Time dimension is moderate, T.P.= 2: Deducted points = 2 x 2 = 4 points If Time dimension is long, T.P.= 1: Deducted points. = 2 x 1 = 2 points
Category 2: Enforcement of the security policy	Level 3: Red warning	Deducted points = E.L. x T.P. If Time dimension is short, T.P.= 1: Deducted points = 3 x 1 = 3 points If Time dimension is moderate, T.P.= 2: Deducted points = 3 x 2 = 6 points If Time dimension is long, T.P.= 1: Deducted points = 3 x 1 = 3 points
	Level 4: Informing the user's manager	Deducted points = E.L. x T.P. If Time dimension is short, T.P.= 1: Deducted points = 4 x 1 = 4 points If Time dimension is moderate, T.P.= 2: Deducted points = 4 x 2 = 8 points If Time dimension is long, T.P.= 1: Deducted points = 4 x 1 = 4 points
	Level 5: Direct intervention or enforcing the security policy e.g. reducing privileges of accessing resources or blocking access to some IT resources	Deducted points = E.L. x T.P. If Time dimension is short, T.P.= 1: Deducted points = 5 x 1 = 5 points If Time dimension is moderate, T.P.= 2: Deducted points = 5 x 2 = 10 points If Time dimension is long, T.P.= 1: Deducted points = 5 x 1 = 5 points

The following diagram (Figure 5.6) explains how compliance points system is working and integrated with the response taxonomy for the non-compliance behaviour.

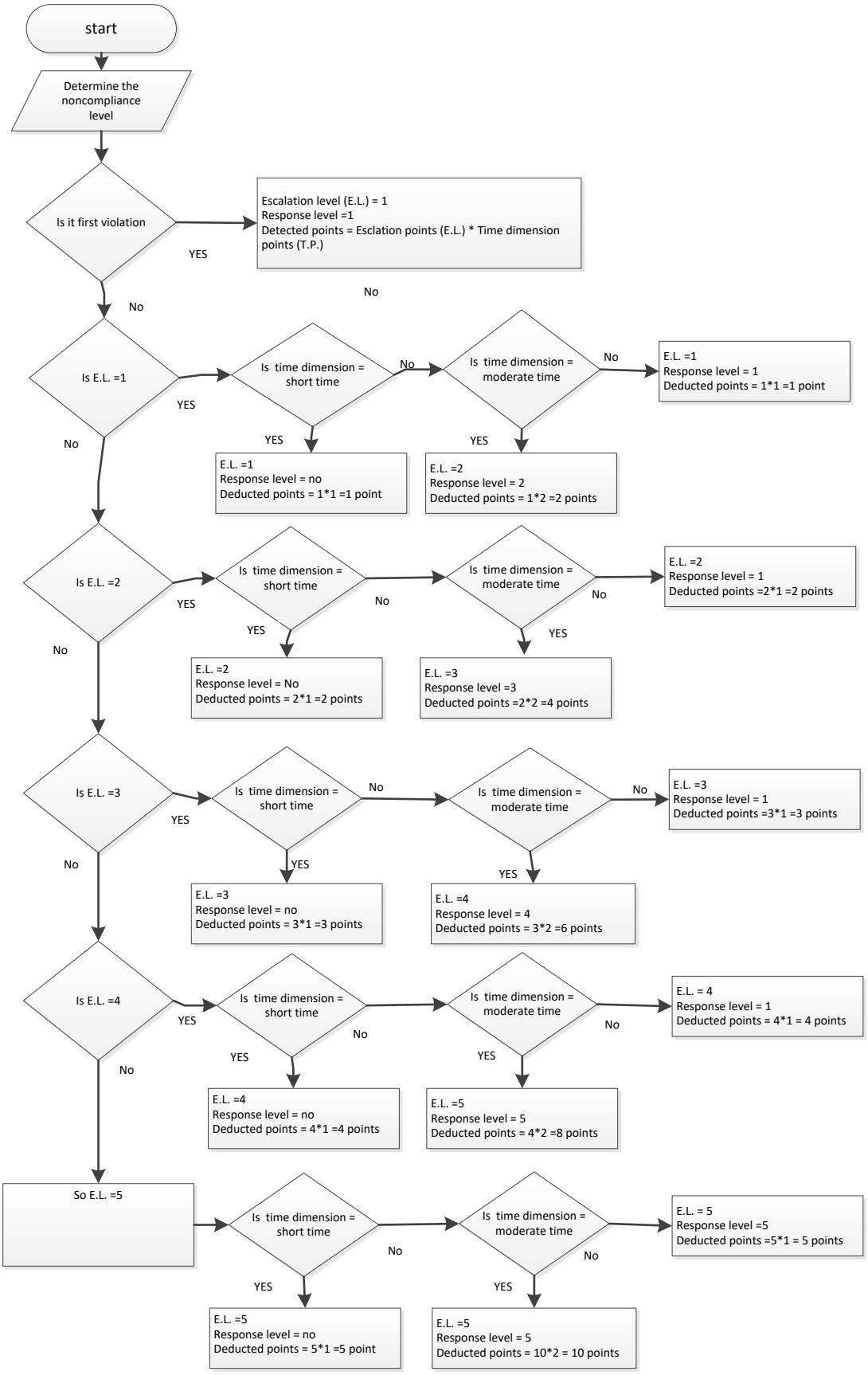


Figure 5.6: Compliance points for non-compliance behaviour

To clarify the concept of the compliance points system in conjunction with the response strategy to non-compliance behaviour, User C's violations will be used. It is assumed that User C has frequently ignored the escalation levels, which were in response to their non-compliant behaviour with this policy. Consequently, the compliance points of User C for this particular policy will be decreased after each violation.

Violation 1: User C violated policy 1 on 01-01-2015.

User C violated the policy for the first time, so E.L. is Level 1 and the time dimension type is considered as long because it is the first violation:

Deducted Points = E.L. x T.P.
Deducted Points = 1 x 1 = 1 point, with -1 total for policy 1.

Violation 2: User C violated policy 1 on 05-01-2015

User C violated the policy for the second time, the E.L. will be Level 2 and the time dimension is moderate period.
(moderate period points T.P. =2). So,

Deducted Points = E.L. x T.P.
Deducted Points = 2 x 2 = 4 points, with -5 points total for policy 1.

Violation 3: User C violated policy 1 on 07-02-2015

User C violated the policy for the third time, the E.L. will be Level 3 and the time duration is moderate period.
(moderate period points T.P. =2). So,

Deducted Points = E.L. x T.P.
Deducted Points = 2 x 3 = 6 points, with -11 points total for policy 1.

Violation 4: User C violated policy 1 on 07-02-2015

User C violated the policy for the fourth time and in the same day of the second violation, so the E.L. is Level 3 and the time duration is short.
Because this violation occurred quickly after the previous one, there was no escalation to the next level.

Deducted Points = E.L. x T.P.
Deducted Points = 3 x 1 = 3 points, with -14 points total for policy 1.

Violation 5: User C violated policy 1 on 07-05-2015

User C violated the policy for the fifth time, the E.L. will be Level 4 and the time duration is moderate.

Deducted Points = E.L. x T.P.
Deducted Points = 4 x 2 = 8 points, with -22 points total for policy 1.

Violation 6: User C violated policy 1 on 01-05-2016

User C violated the policy for the fifth time, one year after the previous violation, the E.L. will remain at Level 4 and the time duration is long.
(long period points = 1). Because this violation occurred a long time after the previous one, the deducted points are:

Deducted Points = E.L. x T.P.

Deducted Points = 4 x 1 = 4 points, with -26 points total for policy 1.

5.5 Significance of the proposed framework

It is important to investigate the ability to encourage users to comply with their information security policy by implementing some important factors, such as monitoring, persuasion, awareness and enforcement, together in one framework. As such, a dynamic response to users' behaviour may be an effective solution towards raising compliance levels. The main objectives of the proposed framework are the individualisation and personalisation of raising awareness. There are targeted responses for each employee when non-compliance behaviour has occurred. Each user is given a targeted response, such as raising security awareness, based on their behaviour events and the response type focuses on the element of the policy that they have violated.

The use of persuasive technology in motivating behavioural change has recently gained the attention of many researchers as a useful approach to promoting change. It is now being applied in many domains, such as marketing, health and psychology (Busch et al. 2016). Motivation and deterrents are examples of persuasive techniques, such as rewards and sanctions as motivation and deterrence, respectively. As such, a scoring points system (or compliance points system) is used to reward or punish users to motivate or deter them.

Persuasion is an integral part of our lives and of human interaction. Fogg (2009)] described persuasive technology (PT) as "interactive computing systems designed to change people's attitudes and behaviours". Persuasive computing technology can affect people's attitudes and bring about some constructive changes in many domains, for example, marketing, health,

safety and the environment. Marketing is perhaps the most significant domain in which persuasive technologies are used to encourage customers to buy products and services. With regard to information security, the results of an empirical study by Yeo et al. (2008) suggest the significance of persuasive technology in changing end-users' behaviour. Furthermore, Qudaih et al. (2014) indicate that using persuasive technology to disseminate policies and procedures can lead to effective information security awareness programmes.

There are two main reasons why the proposed work is deemed necessary and worthwhile. Firstly, no studies have been known to address targeted and on-going compliance with regard to security policy. Secondly, while theoretical research has investigated factors affecting employee behaviour in relation to compliance with information security, none has employed these factors in an integrated framework.

From the perspective of the author, the proposed framework can assist an organisation to gain insight into two different aspects regarding the security policy itself and user behaviour. The following section illustrates how an organization may benefit from the proposed framework.

5.5.1 Gaining insight on the implemented security policy

It is important for any organisation to know the extent of success of the implementation of its security policy. In many organisations, the information security policy is only ink on paper and there is no dynamic way to measure user's behaviour with each element of the policy separately. However, decision makers in an organisation need to have a clear vision about their information security policy and this is difficult without measuring each element of the policy. As such, the proposed framework attempts to fulfil this aim. Figure 5.7 demonstrates some examples of how an organisation might gain insight on its security policy.

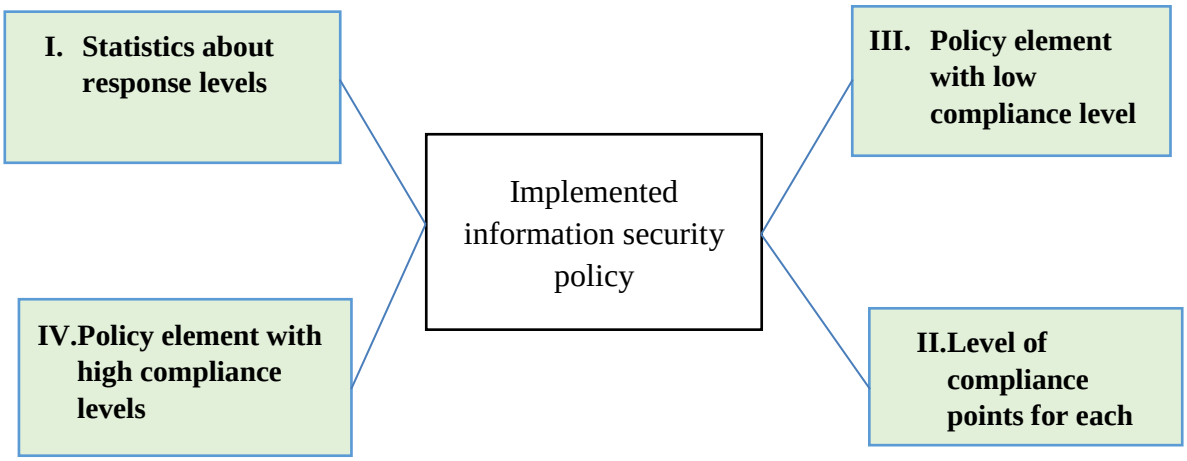


Figure 5.7: Gaining insight on the implemented security policy

I. Policy element with low compliance levels:

Any element of the security policy with large volumes of user violations need urgent investigation regarding the effectiveness of countermeasures related to this element of the policy

II. Statistics about response levels:

There are five levels of response to non-compliance behaviour. The framework records all responses to any non-compliance behaviour, providing an organisation with some useful information regarding each element of the policy. For example, an organisation can see how many times a policy has received the response Level 3 for all users, or even a particular user.

III. Policy element with high compliance levels:

By measuring the compliance of users regarding each element of an information security policy, an organisation can constantly update and review its policy. If any

element of the security policy has a high level of user compliance, this indicates that all efforts to encourage compliance with this element have succeeded in achieving its goals.

IV. Level of compliance points for each policy element:

The compliance points system is designed as a response to users' behaviour, whether granting points as a reward or deducting points for non-compliance. The cumulative points from all users regarding each element of the policy facilitates the measurement process of compliance. And thus, the level of compliance points of each element of the policy can be used to measure the extent of users' compliance.

5.5.2 Gaining an insight into users' behaviour

The proposed framework assists organisations in monitoring and measuring users' behaviour with each element of the security policy in a dynamic way. Figure 5.8 shows examples of how an organisation could gain insight on its users' behaviour.

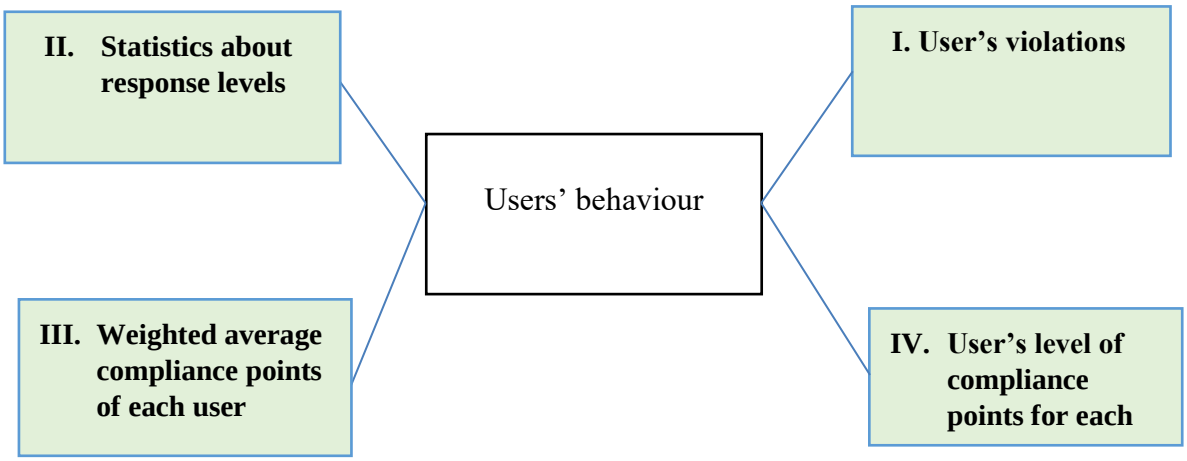


Figure 5.8: Gaining insight on the users' behaviour

I. User violations:

All user violations of any element of the security policy can be monitored by the proposed framework. Information about user violations can be useful for an organisation, for example in statistical analysis or risk assessment.

II. Statistics about response levels:

For non-compliance behaviour, there are five levels of response, and the proposed framework keeps records of all response levels a user has received. An organisation will be able to have a good perception of its employees' behaviour.

III. Weighted average compliance points of each user:

An organisation can weight each element of its security policy by giving more value to the important elements of that policy. For example, a scale of 10 to 1, which means a security policy element that is assigned with 10 is most important and 1 is less important. The weighted values are used in the compliance points system to calculate user's compliance points in relation to every element of the policy. As such, each user within an organisation has a weighted average of points with regard to all elements of the policy, which describes the overall behaviour of a user.

IV. User's level of compliance points for each element of the policy:

A user has a score of compliance points for each element of the security policy, in which the points increase with compliance behaviour or decrease with user violations. Therefore, it will be feasible for an organisation to evaluate user behaviour with each element of the security policy by looking at the user's level of compliance points.

5.6 Conclusion

This chapter has proposed a novel model that aims to increase the compliance levels of users regarding each element of a security policy. This model has been designed to accommodate organisations' needs for raising users' compliance with security policies, and the components and functionalities of the model are described in detail. By providing users with a dynamic response to their behaviour, it can generate a new dimension on how compliance with security policies can be improved.

The model aims at enhancing the compliance level of users based on two main concepts: taxonomy of the response strategy to non-compliance behaviour, and utilising a compliance points system. The response taxonomy of non-compliance behaviour is comprised of two categories: raising awareness and enforcement of the security policy. The compliance points system is used to grant points for compliant behaviour, and deduct points from non-compliant behaviour.

In the next chapter, a simulation based approach is carried out on the proposed model to gain insight into its functionalities.

Chapter Six

A Prototype System for Simulating the Model for Monitoring End-User Security Policy Compliance

6. A Prototype System for Simulating the Model for Monitoring End-User Security Policy Compliance

6.1 Introduction

Having offered a theoretical explanation of the model used for monitoring users' security policy compliance in the previous chapter, the next phase of the research concentrates upon developing a prototype system that simulates the proposed model in order to provide a clear image of its functionalities and how it is meant to work. Therefore, a prototype system was developed to work as a system that responds to the behaviour of users (whether violation or compliance behaviour) in relation to the information security policies of their organisations.

In general, the model for monitoring users' security policy compliance was proposed to improve the compliance level of users. In order for such a model to be understandable and operational, the implementation of a prototype system that simulates the proposed model is important. Thus, a prototype system was developed in order to visualise the real system for monitoring users' security policy compliance.

With the purpose of operating the prototype system, some scenarios of the potential behaviour of users in relation to the information security policies of their organisations need to be assumed and simulated. Therefore, several scenarios were created and used during the simulation process, thus helping to explain the prototype system and how it works. The prototype system acts as a simulation of the real system in a real environment, integrating all the related entities together. As such, the scenarios of the potential behaviour of the users in relation to security policy were used to feed the prototype system (as an input for the prototype) in order to obtain a result and understand how it would work in a real environment. The proposed model, which was explained in the previous chapter, is

demonstrated practically in this chapter. Moreover, the compliance points mechanism used within the proposed model was clarified practically by utilising the assumed scenarios.

This chapter begins by introducing the platform or the environment used to design and program the prototype system. Then some scenarios of potential user behaviour in relation to the information security policies used in the simulation process are explained. Lastly, the prototype system, the simulation process and the results of the simulation, data and charts are illustrated and discussed in more detail.

6.2 Prototype development platform

A practical implementation of the prototype system was designed based upon the model proposed for monitoring users' security policy compliance. The MATLAB environment was selected to develop the prototype system.

According to the MATLAB website (MathWorks 2016), millions of engineers and scientists worldwide use MATLAB to analyse and design systems and products. The MATLAB platform is considered to be optimised to solve scientific problems (Door & Valentine 2016). The matrix-based MATLAB language represents a natural method of expressing computational mathematics, and this feature may be difficult to find in other programming languages. In addition, its built-in graphics make it easy for researchers and programmers to visualise and gain insights into data. Furthermore, other programming languages can be integrated into the MATLAB environment, enabling researchers and programmers to deploy applications or algorithms within production systems, the Web and enterprise. Therefore, due to all the benefits of using the MATLAB environment, it was chosen as a platform to develop and implement the prototype system.

6.3 Simulation Methodology

The proposed model has been designed to be implemented within a real environment and on real users. However, the reality of doing that hits certain challenges, which are

a- This research is conducted by one researcher within certain time frame.

b- The need to develop appropriate controls to do the monitoring process

c- Having an organisation willing to integrate this technology within their operational business, it would not be achievable and acceptable.

And therefore, a different approach, which is simulation methodology, had been sort. A simulation based approach is used to imagine the operation of a real-world process or system over time, and it is considered to be one of the common academic research approaches (Cheng et al. 2014; Dooley 2002). Thus, to test the design and validation of the proposed model, its efficiency and functionality were investigated and validated with the appropriate input data. Hence, a simulation-based approach was used as input data in order to run and demonstrate the prototype functionalities.

Thus, prior to running the prototype system and demonstrating its functionality it was necessary to prepare and set the following input data and parameters:

- Information security policies used
- Scenarios of some potential behaviour of users
- Simulation settings

Therefore, the following sections detail the above inputs in order to understand how the simulation process for the proposed model was designed and approached.

6.3.1 Information security policies used

It was necessary to enter the information security policy settings into the prototype system prior to starting the simulation process. As such, a variety of information security policies were selected from different types of policies, such as password security policy, Internet usage policy, clean desk policy and email usage policy, to be used during the simulation process. Thus, twenty elements of the information security policies were selected for use within the simulation process and each of which has a policy number, policy description, weighted average and elapsed time.

- **Policy number**: This is a unique number to be used within the prototype.
- **Policy description**: This is a clear explanation of each policy element.
- **Weighted average**: This is based on the policy's importance from the organisation's perspective. A scale of the policy elements indicating their importance incorporates 0, 0.1, 0.2, 0.3,…...1, with policies ranked 1 being very important (100%), 0.2 less important (20%) and 0 not important (0%). The main aim of identifying the weighted average of each policy element is that it can be used later in calculating the overall compliance points for each user for all the policies.
- **Elapsed time**: This is used to determine the users' period of compliance with each policy element in order to grant points to the compliant users.

Table 6.1 below presents the twenty different elements of the information security policies along with their settings (These elements of security policies were selected as an example but organisations can do their rules, their selves). Here, the values of weighted average and elapsed time are assumed in order to run the simulation and explaining the model, however an organisation can set any values that suite it.

Table 6.1: The twenty different elements of security policies

Policy #	Policy Description (Policy Element)	Weighted Average	Elapsed Time
1	Computer Workstations must be locked when workspace is unoccupied.	0.5	90 days
2	Computer Workstations must be shut down completely at the end of the workday.	0.2	90 days
3	Electronic storage devices, such as USB and DVDs, that contain restricted information should be kept secure.	0.9	90 days
4	Employees are not allowed to remove or disable anti-virus software.	1	90 days
5	Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.	0.7	90 days
6	User level passwords, such as those used for application, web, email and desktop accounts, must be changed every six months.	0.2	90 days
7	All passwords should meet or exceed the following guidelines: contain at least 12 alphanumeric characters; contain both upper and lower case letter; contain at least one number and one special character.	0.7	90 days
8	Passwords must not be added to or written in an email message, transmitted in any electronic form or revealed to anyone over the phone, via a questionnaire or in a security form.	0.4	90 days
9	Users are not allowed to utilise password memorisation, which is available in some applications as an additional feature, such as the web browser ‘remember password’ feature.	0.8	90 days
10	Users should not undertake deliberate activities that waste staff effort or networked resources.	1	90 days
11	The organisation's email account should be fundamentally utilised for business that is related to the organisation.	0.8	90 days
12	The organisation’s email system must not be utilised to create or distribute any offensive or disruptive messages. For example, offensive comments about age, disabilities, sexual orientation and religious beliefs.	0.9	90 days
13	Users should not send unprotected sensitive or confidential information externally.	1	90 days
14	Users should not use the email system in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.	0.5	90 days
15	Forwarding of company confidential messages to external locations is not allowed.	1	90 days
16	Employees must not download, visit or view any illegal materials on the Internet.	0.8	90 days
17	Personal use of the Internet must not cause a significant increase in resource demand.	0.1	90 days

18	Employees must not download any software from the Internet without prior approval of the IT Department.	1	90 days
19	Employees must not download copyrighted material, such as music media (MP3) files, film and video files (not an exhaustive list), without appropriate approval.	0.3	90 days
20	Employees are not allowed to play any games on the Internet.	0.7	90 days

6.3.2 Scenarios of some potential behaviour of users

In the literature, many researchers have recognised and elaborated upon the potential behaviour of users in relation to information security policy. For instance, Furnell and Thomson (2009) named eight factors that may affect user behaviour in relation to information security policy: culture, commitment, obedience, awareness, ignorance, apathy, resistance and disobedience. Additionally, Alfawaz et al. (2010) proposed a model that categorises user security behaviour, as follows: not knowing-not doing, not knowing-doing, knowing-not doing and knowing-doing. Moreover, misusing, being unaware of and ignoring policy are well-known forms of user behaviour that are considered to represent a challenge to information security policy.

There are two major behaviours of users with an information security policy: fully compliant and fully non-compliant. Moreover, many behaviours can be identified in between those two behaviours, such as unaware, changeful and forgetful. Therefore, based on using the criteria of Alfawaz et al. (2010), and Furnell and Thomson (2009), further three behaviours of users have been identified, which are unaware, changeful and forgetful. This, then led to the design of five scenarios of users, and incorporate all different types.

Based on the above, five different types of user behaviour were chosen in order to create the following scenarios, which were used during the simulation process.

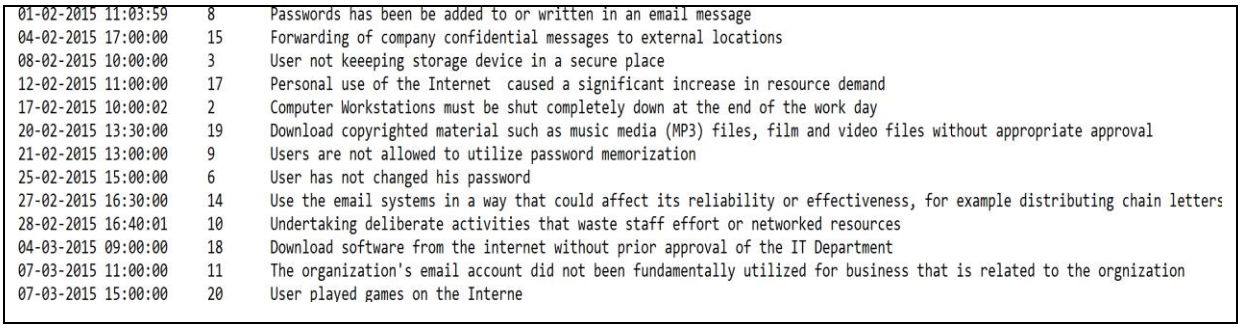
1- **Scenario 1:** Compliant behaviour (Optimal behaviour). A user is aware of security policies and fully complying and showing the required behaviour, compliance is a natural party of users' daily behaviour.
2- **Scenario 2:** Unaware behaviour. A user has no idea about the information security of an organization and does not understand the security requirements.
3- **Scenario 3:** Changeful behaviour. A user behaviour with an information security policy is inconsistent, so their behaviour is fluctuating between compliance and non-compliance.
4- **Scenario 4:** Forgetful behaviour. A user unintentionally break the policy and fail to comply with it, after long period of time the user may forget to comply that policy.
5- **Scenario 5:** Very non-compliant behaviour. A user knows the necessary information about the security policy of his or her organization and has the required skills and knowledge; however, the user deliberately neglects to perform the right behaviour or violates the security policy.

Table 6.2: Scenarios of potential user behaviour

# Scenarios	Description	Behaviour with each policy element
Scenario 1: User A Compliant behaviour (Optimal behaviour)	User A is very compliant with all the security policies.	No violations during the simulation period
Scenario 2: User B Unaware behaviour	User B is not compliant with all the elements of the security policies (20 policies) during the first six months of the simulation period.	Only one violation during the simulation period
Scenario 3: User C Changeful behaviour	In this scenario, User C is non-compliant, then becomes compliant, and then becomes noncompliant again.	5 or 6 violations during the simulation period
Scenario 4: User D Forgetful behaviour	User D is forgetful in regard to complying with the information security policies of his/her organisation.	2 violations during the simulation period
Scenario 5: User E Very noncompliant behaviour	User E is very noncompliant with all the elements of the security policies. User E has not gained any compliance points on any of the elements of the policies because User E never passed the elapsed time of each element without a violation.	13 or more violations during the simulation period

Each scenario represents a specific type of user behaviour, which were all assumed to apply to each of the twenty security policy elements. Each possible scenario arising from a

combination of the user security events with all the policies over a period of time was created in the form of a log file (as shown in Figure 6.1). All the created scenarios represent the actual behaviours of users with information security policies as reported in the literature. Thus, it was anticipated that by creating those scenarios the actual behaviour of some users could be simulated in order to run the prototype system.



01-02-2015 11:03:59	8	Passwords has been be added to or written in an email message
04-02-2015 17:00:00	15	Forwarding of company confidential messages to external locations
08-02-2015 10:00:00	3	User not keeeping storage device in a secure place
12-02-2015 11:00:00	17	Personal use of the Internet caused a significant increase in resource demand
17-02-2015 10:00:02	2	Computer Workstations must be shut completely down at the end of the work day
20-02-2015 13:30:00	19	Download copyrighted material such as music media (MP3) files, film and video files without appropriate approval
21-02-2015 13:00:00	9	Users are not allowed to utilize password memorization
25-02-2015 15:00:00	6	User has not changed his password
27-02-2015 16:30:00	14	Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters
28-02-2015 16:40:01	10	Undertaking deliberate activities that waste staff effort or networked resources
04-03-2015 09:00:00	18	Download software from the internet without prior approval of the IT Department
07-03-2015 11:00:00	11	The organization's email account did not been fundamentally utilized for business that is related to the orgnization
07-03-2015 15:00:00	20	User played games on the Interne

Figure 6.1: Screenshot for a user log file of violations

6.3.2.1 Scenario 1: Compliant behaviour (optimal behaviour)

In this scenario, User A, who was created to simulate complaint behaviour, was very compliant with all twenty elements of the security policies. Indeed, during the three year simulation period, starting on 01-01-2015 and ending on 01-01-2018, User A did not violate any of the elements of the security policies. In other words, the log file of User A is empty since no violations were recorded within this time period. The behaviour of User A was used to explain the proposed model practically and how the model deals with this sort of behaviour. Moreover, User A behaviour, which represents compliant behaviour, was used during the simulation as a benchmark for other behaviour to offer a clearer idea about the proposed model and how it processes different types of behaviour.

6.3.2.2 Scenario 2: Unaware behaviour

In this scenario, User B was created to simulate unaware behaviour. User B was not compliant with all twenty elements of the security policies during the first six months of the

three-year simulation period, committed one violation of each element of the policies because they were unaware of each of those elements. However, thereafter User B changed his/her behaviour and became compliant with all the elements of the policies because they had become aware of those policies. Thus, the violations log file of User B contains one violation of each policy element during the simulation period, as illustrated in the following Table 6.3 (for all User B's violations of the elements of the security policies, see User B's original log file in appendix A):

Table 6.3: User B violations

Policy element #	Violation date &time	Policy element #	Violation date &time
1	01-01-2015 09:00:00	11	29-06-2015 16:00:00
2	02-01-2015 09:30:02	12	30-06-2015 09:30:00
3	03-01-2015 10:00:00	13	21-07-2015 17:00:00
4	04-01-2015 11:30:40	14	29-06-2015 16:30:00
5	20-01-2015 12:00:00	15	03-04-2015 17:00:41
6	28-03-2015 14:00:00	16	01-07-2015 12:00:00
7	01-04-2015 13:00:00	17	03-04-2015 17:00:00
8	01-04-2015 14:03:05	18	01-07-2015 11:00:00
9	02-04-2015 13:00:00	19	30-06-2015 08:30:00
10	01-04-2015 16:40:01	20	02-04-2015 30:00:00

6.3.2.3 Scenario 3: Changeful behaviour

In this scenario, User C was created to simulate changeful behaviour. User C's behaviour is inconsistent in relation to information security policy. User C's behaviour was non-compliant, then became compliant, and then became non-compliant again. User C was not compliant with the security policies for the first six months of the simulation period; however, after this period, User C changed his/her behaviour and became compliant with those policies for a period of time. However, once again User C changed his/her behaviour and returned to non-compliant behaviour.

Table 6.4 shows User C's violations of four elements of the security policies, policy element no.1, policy element no.2, policy element no.3 and policy element no.4, during the simulation

period (for all User C's violations of the elements of the policies, see User C's original log file in appendix D).

Table 6.4: User C violations

Policy #	Violations date &time	Policy #	Violations date &time
1	First violation on 24-03-2015 10:30:00 Second violation on 10-05-2015 15:00:00 Third violation on 30-06-2015 08:30:00 Fourth violation on 01-07-2017 15:00:00 Fifth violation on 27-09-2017 15:00:00 Sixth violation on 17-11-2017 09:00:00	3	First violation on 01-01-2015 10:00:00 Second violation on 20-03-2015 11:00:00 Third violation on 01-04-2015 15:00:00 Fourth violation on 24-06-2017 15:00:00 Fifth violation on 20-09-2017 15:00:00 Sixth violation on 11-11-2017 12:00:00
2	First violation on 01-01-2015 09:00:02 Second violation on 09-02-2015 13:00:00 Third violation on 01-04-2015 16:00:00 Fourth violation on 23-06-2017 09:00:02 Fifth violation on 18-09-2017 09:00:02 Sixth violation on 10-11-2017 16:00:02	4	First violation on 01-01-2015 11:30:40 Second violation on 23-01-2015 13:00:00 Third violation on 07-02-2015 15:00:00 Fourth violation on 09-02-2015 11:00:00 Fifth violation on 16-03-2015 11:00:00 Sixth violation on 01-04-2015 13:00:00 Seventh violation on 20-06-2017 11:30:40 Eighth violation on 15-09-2017 13:30:40 Ninth violation on 05-11-2017 13:30:40

6.3.2.4 Scenario 4: Forgetful behaviour

When users forget security policy information, possibly after not having used the system for a long period of time, this may affect their behaviour. In this scenario, the author assumes that User D is forgetful in terms of complying with the information security policies of his/her organisation.

During the simulation period, which was three years, User D violated each element twice, and the time period between the two violations was six months or more. Table 6.5 shows User D's violations of each element of the policies during the three year simulation period (for all User D's violations of the elements of the security policies, see User D's original log file in appendix C).

Table 6.5: User D violations

Policy #	Violation date &time	Policy #	Violation date &time
1	First violation on 24-06-2016 14:30:00 Second violation on 19-06-2017 16:30:00	11	First violation on 26-03-2016 12:00:00 Second violation on 21-03-2017 17:00:00
2	First violation on 26-03-2016 15:00:00 Second violation on 21-03-2017 18:00:00	12	First violation on 24-06-2016 15:30:00 Second violation on 19-06-2017 17:30:00
3	First violation on 28-09-2015 10:00:00 Second violation on 22-09-2016 10:00:00	13	First violation on 24-06-2016 12:00:00 Second violation on 19-06-2017 15:00:00
4	First violation on 28-09-2015 11:30:40 Second violation on 22-09-2016 11:30:40	14	First violation on 26-03-2016 16:00:00 Second violation on 21-03-2017 18:10:00
5	First violation on 27-12-2015 12:00:00 Second violation on 21-12-2016 12:00:00	15	First violation on 26-03-2016 11:00:00 Second violation on 21-03-2017 16:50:00
6	First violation on 27-12-2015 14:00:00 Second violation on 21-12-2016 15:00:00	16	First violation on 26-03-2016 13:00:00 Second violation on 21-03-2017 17:30:00
7	First violation on 27-12-2015 15:00:00 Second violation on 21-12-2016 14:00:00	17	First violation on 26-03-2016 10:00:00 Second violation on 21-03-2017 16:20:11
8	First violation on 27-12-2015 16:03:59 Second violation on 21-12-2016 15:03:59	18	First violation on 26-03-2016 14:00:00 Second violation on 21-03-2017 17:40:00
9	First violation on 26-03-2016 09:00:00 Second violation on 21-03-2017 16:00:00	19	First violation on 26-03-2016 17:00:00 Second violation on 21-03-2017 18:30:00
10	First violation on 26-03-2016 08:40:01 Second violation on 21-03-2017 15:40:01	20	First violation on 24-06-2016 11:00:00 Second violation on 19-06-2017 11:00:00

6.3.2.5 Scenario 5: Very noncompliant behaviour

In this scenario, User E was noncompliant with all the elements of the security policies. During the simulation period, which was three years, starting from 01-01-2015 and ending on 01-01-2018, User E violated each element of the policies many times. In fact, there were nearly 13 violations per element. User E did not gain any compliance points on any of the elements of the policies because User E never got past the elapsed time of each policy element without violating the policies. Hence, this user lost many points for each security policy element and he/she reached the minimum level of compliance points for each element of the policies. As an example, User E's violations of four elements of the security policies, which are policy element no.1, policy element no.2, policy element no.3 and policy element no.4, are illustrated in the following Table 6.6 (for all User E's violations of the elements of the security policies, see User E's original log file in appendix D):

Table 6.6: User E violations

Policy #	Violation date &time	Policy #	Violation date &time
1	First violation on 25-01-2015 09:00:00 Second violation on 19-04-2015 16:00:00 Third violation on 12-07-2015 16:00:00 Fourth violation on 07-10-2015 16:00:00 Fifth violation on 05-01-2016 09:00:00 Sixth violation on 01-04-2016 16:00:00 Seventh violation on 28-06-2016 16:00:00 Eighth violation on 24-09-2016 16:00:00 Ninth violation on 20-12-2016 09:00:00 Tenth violation on 15-03-2017 12:00:00 Eleventh violation on 10-06-2017 12:00:00 Twelfth violation on 05-09-2017 13:00:00 Thirteenth violation on 25-11-2017 16:00:00	3	First violation on 08-02-2015 10:00:00 Second violation on 02-05-2015 10:00:00 Third violation on 25-07-2015 10:00:00 Fourth violation on 20-10-2015 10:00:00 Fifth violation on 15-01-2016 10:00:00 Sixth violation on 11-04-2016 10:00:00 Seventh violation on 06-07-2016 10:00:00 Eighth violation on 01-10-2016 10:00:00 Ninth violation on 28-12-2016 10:00:00 Tenth violation on 24-03-2017 10:00:00 Eleventh violation on 20-06-2017 10:00:00 Twelfth violation on 15-09-2017 10:00:00 Thirteenth violation on 05-12-2017 10:00:00
2	First violation on 17-02-2015 10:00:02 Second violation on 10-05-2015 10:00:02 Third violation on 03-08-2015 10:00:02 Fourth violation on 28-10-2015 10:00:02 Fifth violation on 23-01-2016 10:00:02 Sixth violation on 19-04-2016 10:00:02 Seventh violation on 15-07-2016 10:00:02 Eighth violation on 10-10-2016 10:00:02 Ninth violation on 05-01-2017 10:00:02 Tenth violation on 28-06-2017 10:00:02 Eleventh violation on 24-09-2017 10:00:02 Twelfth violation on 17-12-2017 10:00:02	4	First violation on 22-01-2015 11:30:40 Second violation on 17-04-2015 15:30:40 Third violation on 10-07-2015 15:30:40 Fourth violation on 05-10-2015 15:30:40 Fifth violation on 02-01-2016 11:30:40 Sixth violation on 28-03-2016 15:30:40 Seventh violation on 24-06-2016 15:30:40 Eighth violation on 20-09-2016 15:30:40 Ninth violation on 15-12-2016 11:30:40 Tenth violation on 10-03-2017 15:30:40 Eleventh violation on 05-06-2017 15:30:40 Twelfth violation on 01-09-2017 15:30:40 Thirteenth violation on 20-11-2017 15:30:40

6.3.3 The simulation settings and parameters

Before starting the simulation process, it was necessary to create some settings with appropriate values, as follows.

- **The simulation period.** This refers to the period of time that the simulation process ran for. Therefore, there are two variables in this regard, start date (from) and end date (to). In this simulation, the simulation period ran from 01-01-2015 to 01-01-2018. This period, which is three years, was selected to explain the proposed model during a reasonable long period of time
- **Time dimensions**. As explained previously, three time dimensions (long, moderate and short) were used as an indicator for the response taxonomy of non-compliance

behaviour. Each time dimension type had its own settings: duration and points. In this simulation, the settings were as follows:

1- Long-time dimension: Duration > 6 months, as a default value. Because, the period between the new violation and the last violation should be long period of time because the user is considered as a forgotten user. Points =1.

2- Moderate time dimension: 1 day < Duration < 6 months, as a default value. Because, there will be enough time since the last violation and the user should be received a response for the last violation. Points =2.

3- Short time dimension. Duration < 1 day. as a default value. Because, there will be not enough time for any significant intervention, so the time should be short. Points =1

The author has set the recommended defaults values of the three types as shown above, However, an organisation can choose any values for the above stings.

- **Compliance points level.** As explained previously, the compliance point system was used within the model to grant or deduct points based on user behaviour with information security policy. However, granting or deducting points was time restricted and there was a limit on the number of points awarded, with a maximum level for granting and a minimum level for deducting. Therefore, if a user reached the maximum or the minimum level of points, he/she stayed at that level in spite of his/her behaviour. For the purpose of this simulation, the following values were assigned to the compliance points levels.

  - Maximum = 12 points. This value was suggested based on one point every three months (elapsed time= 3 months) for a period of 3 years.
  - Minimum = -31. This value was suggested based on a total of 6 violations (violations occurring in the moderate time).

6.4 Input interface

An input screen within the prototype facilitated the input of settings prior to running the simulation, as shown below in Figure 6.2.

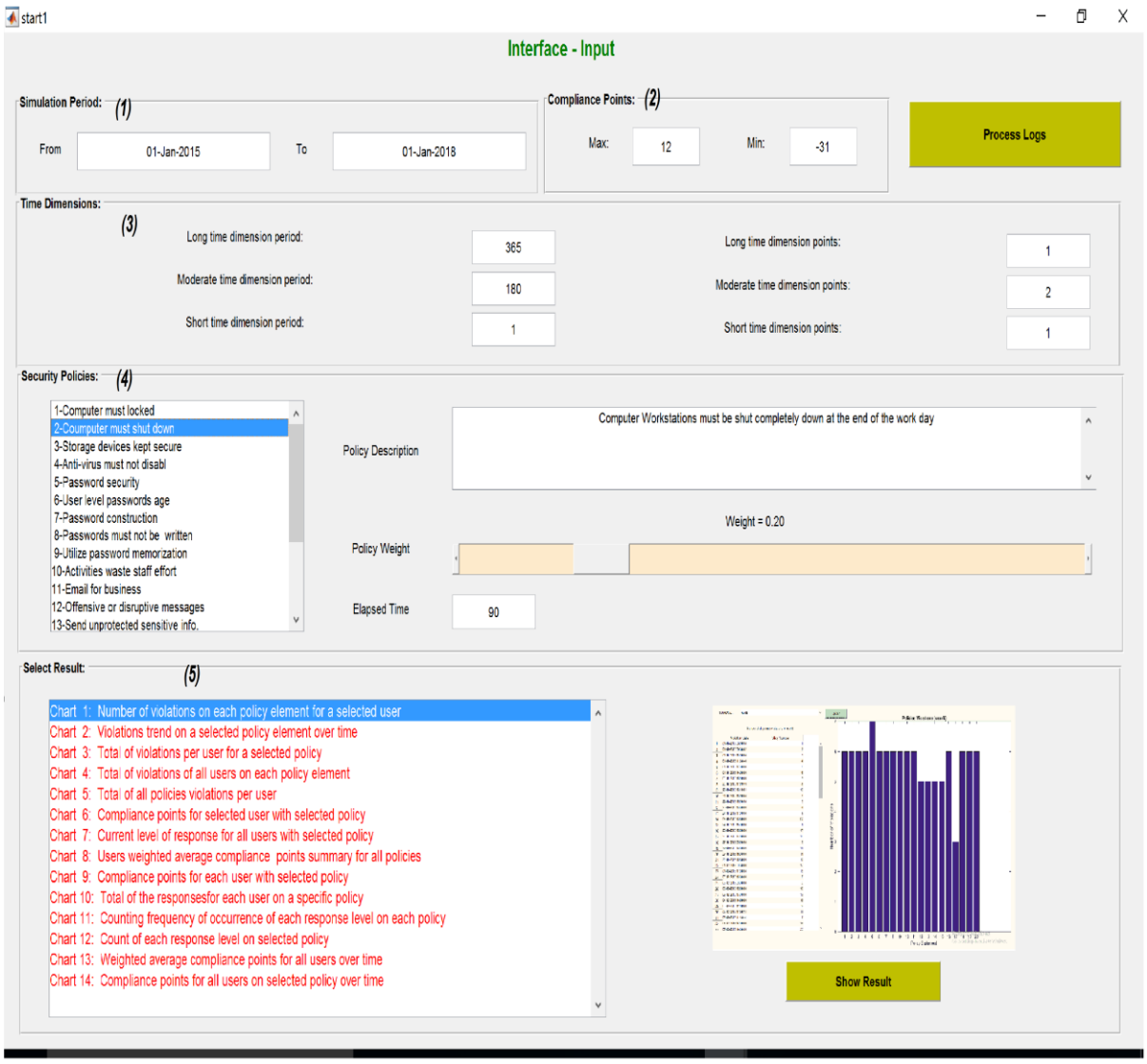


Figure 6.2: Screenshot for the interface input of the prototype system

The input interface was comprised of five main parts:

1) Simulation period. The simulation duration could be entered through this part. The simulation period had two values: start date (From) and end date (To).
2) Compliance points level: The maximum and minimum level of compliance points could be set via this part.

3) Time dimensions: Each time dimension type has two values for settings: duration, meaning the time period between violations; and points, which is used in the compliance points system. The default value of the duration was set in days but it could have been set in seconds, minutes or hours. As seen in Figure 2, each time dimension type had a specific duration value, as follows:
    - Short time dimension = 1 - This means the duration between violations is considered short if it is less than 1 day.
    - Moderate time dimension = 180 - This means the duration between violations is considered moderate if it is greater than 1 day and less than 180 days.
    - Long-time dimension = 365 - This mean the duration between violations is considered long if it is greater than 180 days.
4) Security policies: It is possible to enter and manage the settings of each element of the security policies via this part of the interface. These settings are as follows:
    - Policy weight: Each element of the policies has a weighted average number based on its importance. Therefore, there is a GUI slider within the interface that displays a range of values (from 0, 0.1, 0.2, 0.3, ……..., 0.9 till 1) and has an indicator, or knob, which shows the current setting.
    - Elapsed time: It is possible to set and change the value of the elapsed time for each policy element via this part of the interface.
5) Results selection: From this part of the interface, it is possible to select the desired type of results and present many of the results or charts of the simulation with their data and graphs. Therefore, a scrolling list of the results titles facilitated the selection of the desired results title. A scroll list contains fourteen different results titles obtained from the simulation process, as shown in Figure 6.3. Moreover, there is a preview for each results title among the list, which helped the interface's user to select

an appropriate results title to be displayed. Once a desired results title is selected, double clicking on it will open another interface, and from that interface, the selected users or policies could be changed to gain more specific results.

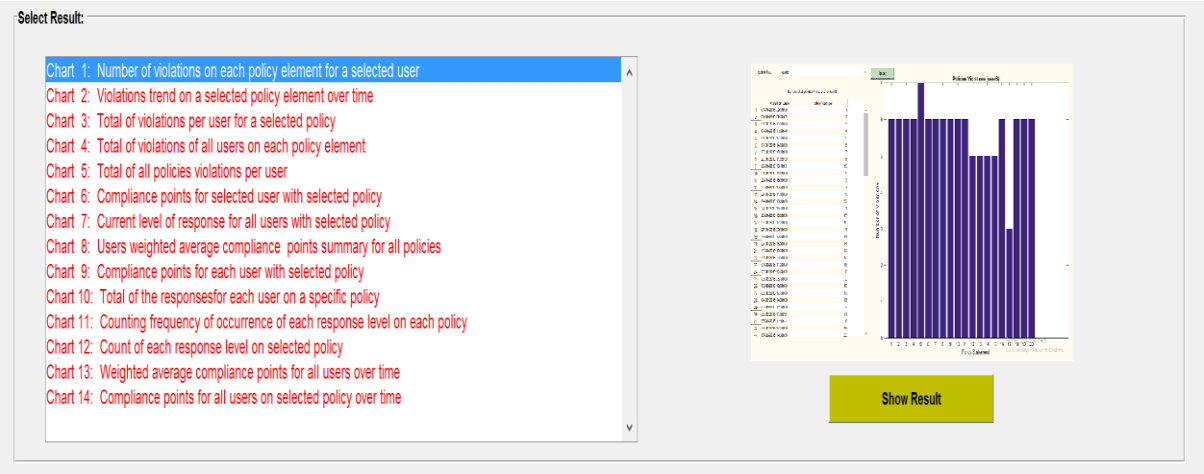


Figure 6.3: Screenshot for the selection of results

6.5 Output interface

The output of the simulation is presented in the form of data and charts. However, in order to run the prototype and the simulation, it is necessary to feed the users' violations or behaviour in relation to the information security policies into the prototype system. Therefore, the scenarios created of user behaviour in relation to security policy in the previous section (1.3.2) were processed by the prototype system in order to simulate the real system of the proposed model (By pressing on the process users' logs button within the interface input of the prototype system will start the simulation process).

In this section, the manner in which the prototype system responded to those scenarios of users' behaviour is explained, taking each scenario separately. In addition, the output of the simulation process regarding user behaviour and policies was assigned to two groups:

- Gaining insight into the implemented security policies.
- Gaining insight into user behaviour.

6.5.1 Simulation results of scenario 1: Compliant behaviour (optimal behaviour)

Scenario 1 was created to simulate very compliant behaviour (optimal behaviour), with User A playing the role of a compliant user. User A was very compliant with all the policies during the simulation period and did not violate any of the elements of the security policies.

To explain how the behaviour of User A was processed by the prototype system, policy element no.1 was selected as an example because whatever applied to it would also apply to the other policies. As suggested from the beginning, the simulation period was three years, starting on 01-01-2015 and ending on 01-01-2018, and the elapsed time period for policy statement 1 was set at 90 days, meaning that if the user did not violate policy 1 for a period of 90 days, he/she would be granted one security point. Consequently, User A did not violate policy element no.1 during the simulation period and, as a result, was granted 12 compliance points for that policy element as a reward for their compliance. Figure 6.4 shows User A's compliance points pattern for policy element no.1 over the simulation period.

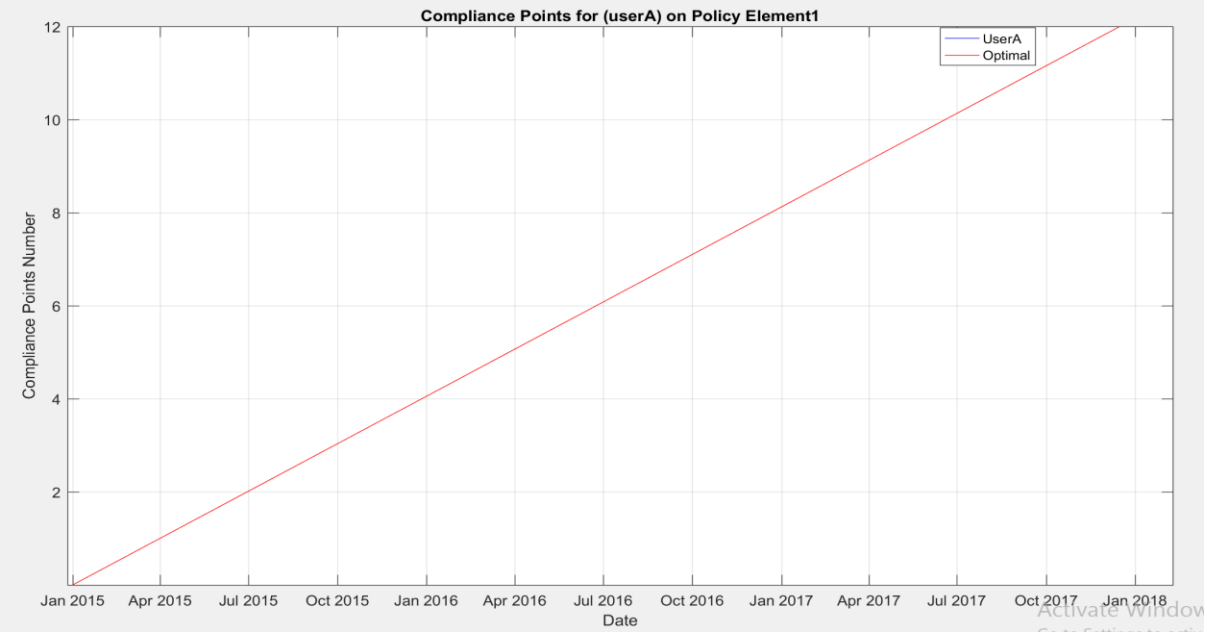


Figure 6.4: User A compliance points in relation to policy element no.1 over 3 years

The above chart, which shows User A's compliance points for policy element no.1 over the simulation period, was copied from the prototype system. The chart presents an optimal behaviour line and User A's behaviour line. The optimal behaviour line indicates the optimal compliance points for policy element no.1 based on an elapsed time period of 90 days. Therefore, the optimal compliance points increase by one point every 90 days, and thus there are 12 accumulative compliance points at the end of the simulation period (3 years). The second line in the chart indicates User A's compliance points in relation to policy element no.1, and this line matches the optimal line exactly (because User A was a very compliant user and there were no violations during the simulation period). Hence, the two lines appear as one line on the graph. Thus, the number of User A's compliance points rose gradually and steadily by 1 point every 90 days between 01-01-2015 and 01-01-2018, and therefore, the total points at the end of the simulation period was 12.

1 currentUser	2 PolicyNumber	3 Date	4 diff	5 EL	6 RL	7 ARL	8 Current_points	9 Total_points
'userA'	1	01-Apr-2015	2160:00:00	0	0	0	1	1
'userA'	1	30-Jun-2015	2160:00:00	0	0	0	1	2
'userA'	1	28-Sep-2015	2160:00:00	0	0	0	1	3
'userA'	1	27-Dec-2015	2160:00:00	0	0	0	1	4
'userA'	1	26-Mar-2016	2160:00:00	0	0	0	1	5
'userA'	1	24-Jun-2016	2160:00:00	0	0	0	1	6
'userA'	1	22-Sep-2016	2160:00:00	0	0	0	1	7
'userA'	1	21-Dec-2016	2160:00:00	0	0	0	1	8
'userA'	1	21-Mar-2017	2160:00:00	0	0	0	1	9
'userA'	1	19-Jun-2017	2160:00:00	0	0	0	1	10
'userA'	1	17-Sep-2017	2160:00:00	0	0	0	1	11
'userA'	1	16-Dec-2017	2160:00:00	0	0	0	1	12

Table 6.7: Screenshot for the User A simulation result on policy element 1

As shown in Table 6.7, the prototype system responded to User A's behaviour. Due to no violations of policy element no.1 being committed by User A, there was no response

taxonomy for the non-compliance behaviour. Thus, the values of escalation level (EL), response level (RL) and actual response level (ARL) were all zero.

The first action taken by the system occurred on 01-Apr-2015, meaning that 90 days (2160 hours) after the start of the simulation, the user acquired one point. The second action was on 30-Jun-2015, 90 days after the first action, for which the user was given another point, meaning that User A had 2 total points for policy element no.1. In such a way, User A's total points increased by one point every 90 days until the end of the simulation period. Therefore, by 16-Dec-2017 User A had 12 compliance points for policy element no.1 (the User A was increased 1 points every 90 days during the 3 years = 12 points).

6.5.2 Simulation results of scenario 2: Unaware behaviour

This scenario was created to simulate an employee who is unaware of the existence of an information security policy. User B was created to simulate this kind of user behaviours. In this scenario, User B was unaware of all the security policies (each with twenty elements), and therefore, he/she committed one violation of each policy element during the simulation period, which started on 01-01-2015 and ended on 01-01-2018. Consequently, with each violation, User B received a response to his/her non-compliance behaviour from the system (response taxonomy for non-compliance), which was in this case level 1: basic awareness raising. However, after that, User B was aware of that policy element and was then compliant with it since he/she had received the system response for his/her first violation. To explain how the proposed model dealt with this scenario, User B's behaviour in relation to policy element no.2 was selected, as is explained below.

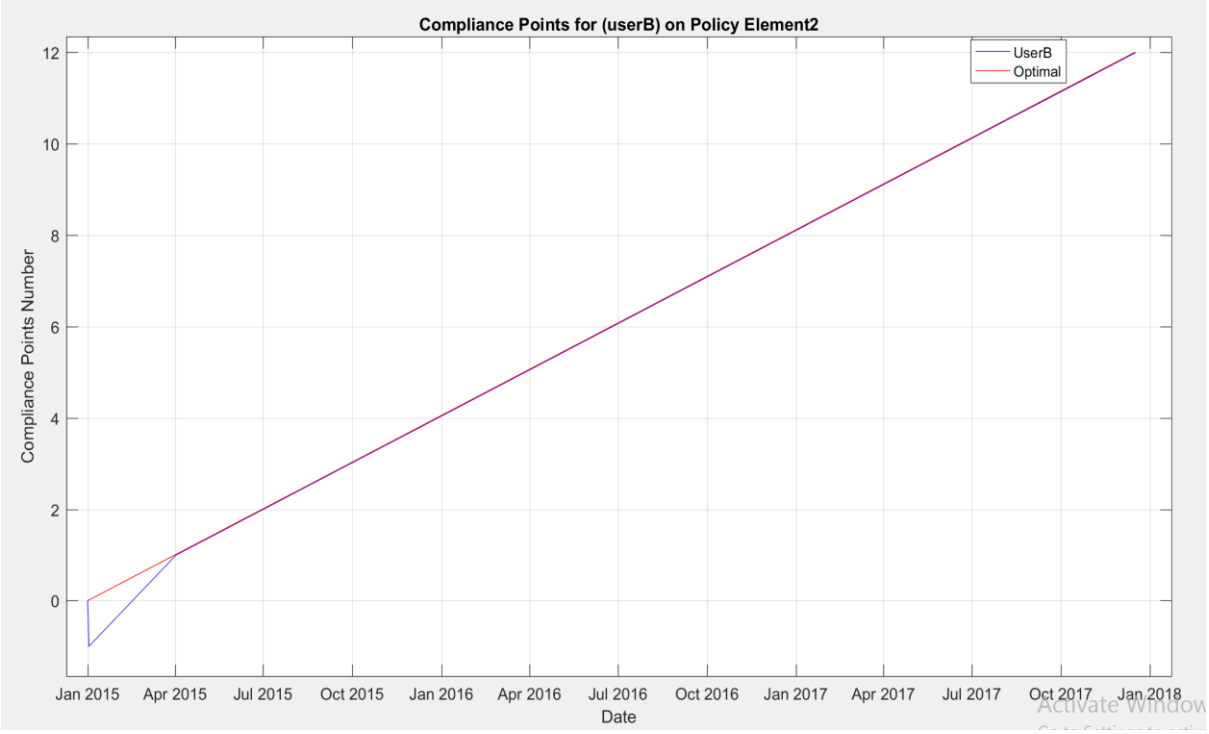


Figure 6.5: User B compliance points for policy element no.2 over 3 years

As demonstrated in Figure 6.5, User B's compliance points for policy element no.2 were compared with the optimal compliance points for the same policy element over the simulation period. In this scenario, during the simulation period, User B violated policy element no.2 only once on 02-01-2015. Therefore, the system responded to this violation and deducted points. As can be seen in the graph, on Jan 2015, User B had 1 point deducted, and thus was in credit for policy element no.1, with -1 points. However, since Apr 2015, User B's compliance points for policy element 2 matched the optimal points, meaning that User B was compliant with that policy for 3 months (the elapsed time period for policy element no.2). User B had become aware of policy element no.2, and therefore, he/she carried on complying with that policy element till the end of the simulation period. Table 6.8 demonstrates step by step how User B's behaviour was processed by the system.

1 currentUser	2 PolicyNumber	3 Date	4 diff	5 EL	6 RL	7 ARL	8 Current_point	9 Total_points
'userB'	2	02-Jan-2015	33:30:02	1	1	1	-1	-1
'userB'	2	02-Apr-2015	2160:00:00	1	1	0	2	1
'userB'	2	01-Jul-2015	2160:00:00	1	1	0	1	2
'userB'	2	29-Sep-2015	2160:00:00	1	1	0	1	3
'userB'	2	28-Dec-2015	2160:00:00	1	1	0	1	4
'userB'	2	27-Mar-2016	2160:00:00	1	1	0	1	5
'userB'	2	25-Jun-2016	2160:00:00	1	1	0	1	6
'userB'	2	23-Sep-2016	2160:00:00	1	1	0	1	7
'userB'	2	22-Dec-2016	2160:00:00	1	1	0	1	8
'userB'	2	22-Mar-2017	2160:00:00	1	1	0	1	9
'userB'	2	20-Jun-2017	2160:00:00	1	1	0	1	10
'userB'	2	18-Sep-2017	2160:00:00	1	1	0	1	11
'userB'	2	17-Dec-2017	2160:00:00	1	1	0	1	12

Table 6.8: Screenshot for the simulation result of User B on policy element no.2

On 02-Jan-2015:	User B violated the policy for the first time. The time dimension type was considered to be long (T.P.=1) because it was the first violation, so: Escalation level (EL) = level 1 Actual response level (ARL) = level 1 (Basic awareness) Deducted Points = Escalation level (E.L.) * Time dimension points (T.P.) Deducted Points = 1 * 1 = 1 point, Total points for User B for policy element no.2 = -1 point
On 02-Apr-2015:	This action was taken by the system because the user had been compliant for 90 days following the last violation, which was the elapsed time period for policy element no.2. User B's points increased based on changing behaviour in relation to compliance. *Points of changing behaviour = 2 points * (No. of compliance times after the last violation of the same policy).* Compliance points= 2 * 1 (first compliance after the last violation) = 2 points. Total points for User B for policy statement 2 = 1 point
On 01-Jul-2015:	Another 90 days passed without any violation of policy element no.2, and therefore, the system granted User B one point based on normal compliance behaviour. The user recovered the lost points and was then in line with the optimal points for policy element no.2.
From 01-Jul-2015 until the simulation end:	User B's score increased by one security point every 90 days until the end of the simulation period because the system viewed him/her as having normal compliance behaviour.

6.5.3 Simulation results of scenario 3: Changeful behaviour

Scenario 3 was created to simulate the changeful or inconsistent behaviour of some users. User C played the role of a user with changeful behaviour in relation to information security policies. In this scenario, User C was assumed to be noncompliant for a period of time, then complaint for a period of time, and then noncompliant again. User C committed 5 or 6 violations of each element of the twenty policies during the simulation period, which started on 01-01-2015 and ended on 01-01-2018. To explain how the system responded to User C's behaviour, policy element no. 2 was selected as an example. Figure 6.6 shows how User C's compliance points for the policy element no.2 appear over the three year simulation period.

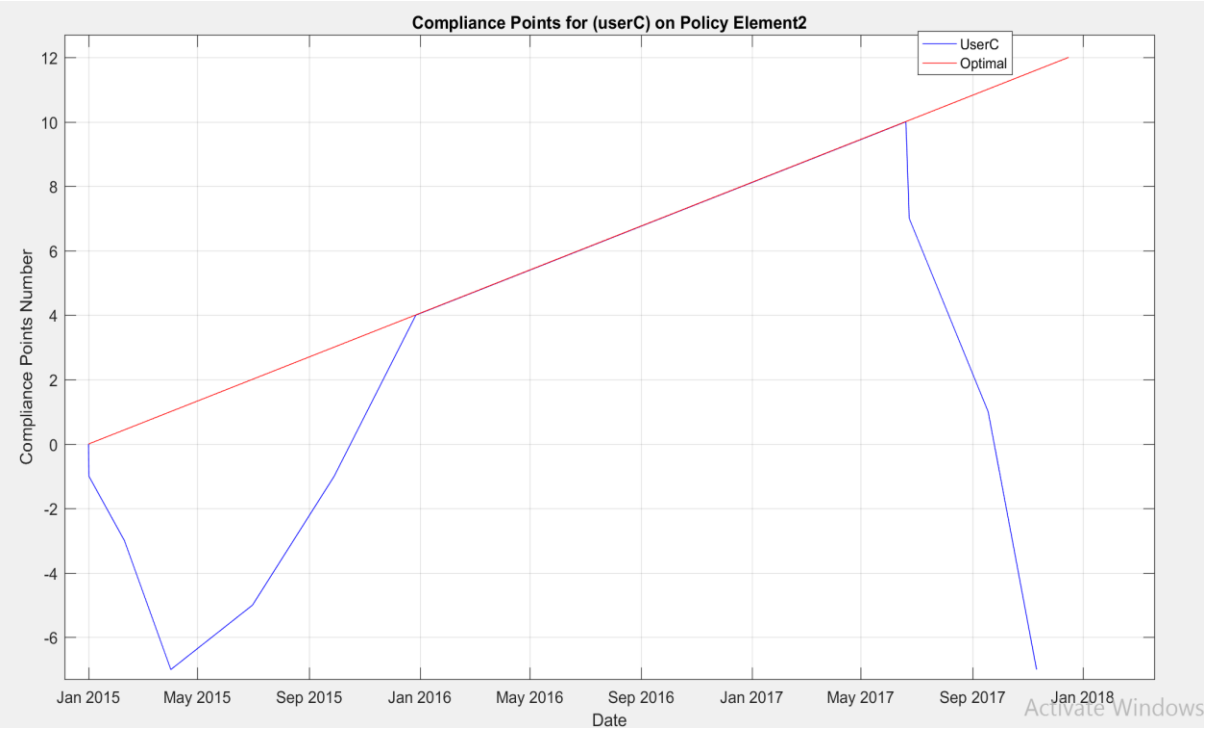


Figure 6.6: Screenshot for the simulation result of User C for policy element no.2

As demonstrated above in Figure 6.8, User C's compliance points for his/her behaviour in relation to policy element no.2 (blue line) were compared with the optimal compliance points for the same policy (green line). Between 1-Jan-2015 and 1-Apr-2015, User C's compliance points decreased to -7 points because he/she committed three violations during that period.

However, after that period, between 1-Apr-2015 and 23-Jun-2017, User C became compliant with that policy, and so the system granted points based on two mechanisms: 1) points for changing behaviour towards compliance; and 2) points for normal compliance. The first mechanism was applied from 1-Apr-2015 until 27-Dec-2015, with the user being granted compliance points based on the changing behaviour toward compliance equation, which is:
*Points of changing behaviour = 2 points * (No. of compliance times after the last violation of the same policy).*

The aim of using this mechanism was to assist the user in recovering lost points in a quick and gradual manner. Thus, from 1-Apr-2015 until 27-Dec-2015, the User C was granted more points each three months of compliance (elapsed time), and the compliance points of User C for policy element no.2 went up more sharply from -7 to 4 points on 27-Dec-2015, matching the optimal points on that date. After that, between 27-Dec-2015 and 23-Jun-2017, the system made granting the compliance points the responsibility of the second mechanism, which awarded points for normal compliance, because User C was compliant during that period and his/her compliance points for policy element no.2 matched the optimal compliance points for the same policy. Therefore, User C's compliance points were exactly in line with the optimal points and increased by one point every three months (because the elapsed time of policy element no.2 = 3 months), the compliance points climbing to 10 points by 23-Jun-2017.

However, it can be clearly seen that from 23-Jun-2017 until the end of the simulation period, User C's compliance points dropped rapidly to -7 points because he/she committed three violations during that period. There was a heavy loss of compliance points because the escalation level (E.L.) that the User C already had was level 3, which affected the number of

points detected. To explain how the system responded to User C's behaviour, Table 6.9 demonstrates User C's history in relation to policy element no.2:

1 currentUser	2 PolicyNumber	3 Date	4 diff	5 EL	6 RL	7 ARL	8 Current_points	9 Total_points
'userC'	2	01-Jan-2015	09:00:02	1	1	1	-1	-1
'userC'	2	09-Feb-2015	939:59:58	2	2	2	-2	-3
'userC'	2	01-Apr-2015	1227:00:00	3	3	3	-4	-7
'userC'	2	30-Jun-2015	2160:00:00	3	3	0	2	-5
'userC'	2	28-Sep-2015	2160:00:00	3	3	0	4	-1
'userC'	2	27-Dec-2015	2160:00:00	3	3	0	5	4
'userC'	2	26-Mar-2016	2160:00:00	3	3	0	1	5
'userC'	2	24-Jun-2016	2160:00:00	3	3	0	1	6
'userC'	2	22-Sep-2016	2160:00:00	3	3	0	1	7
'userC'	2	21-Dec-2016	2160:00:00	3	3	0	1	8
'userC'	2	21-Mar-2017	2160:00:00	3	3	0	1	9
'userC'	2	19-Jun-2017	2160:00:00	3	3	0	1	10
'userC'	2	23-Jun-2017	19529:00:02	3	1	1	-3	7
'userC'	2	18-Sep-2017	2088:00:00	4	2	2	-6	1
'userC'	2	10-Nov-2017	1279:00:00	5	3	3	-8	-7

Table 6.9: Screenshot for the simulation result of User C on policy element no.2

On 01-Jan-2015:	User C violated the policy for the first time, so the time dimension type is considered to be long (T.P.=1) because it was the first violation, so: Escalation level (EL) = level 1 Actual response level (ARL) = level 1 (Basic awareness) Deducted Points = Escalation level (E.L.) * Time dimension points (T.P.) Deducted Points = 1 * 1 = -1 point, Total points for User C for policy element no.2 = -1 point
On 09-Feb-2015:	User C violated the policy for the second time, around a month after the first violation, so the time duration was considered to be moderate (T.P. =2). User C was considered to be intentionally violating the security policy for the second time, and therefore the response level was escalated from Level 1 to Level 2, advanced raising of awareness. Deducted Points = Escalation level (E.L.) * Time dimension points (T.P.) Deducted Points = 1 * 2 = -2 points, Total points for User C for policy element no.2 = -3 points
On 01-Apr-2015:	The third violation was on 07-02-2015, nearly two months after the second violation. Therefore, the time dimension was considered to be moderate, and the response escalated to Level 3, red warning. Deducted Points = Escalation level (E.L.) * Time dimension points (T.P.) Deducted Points = 2 * 2 = -4 point, Total points for User C for policy element no.2 = -7 points

On 30-Jun-2015:	This action was taken by the system because the elapsed time had passed without any violation, so User C increased 2 points for being compliant with this element of the policy. Due to this action being the first compliance after the last violation and User C's compliance points being less than the optimal points, the second mechanism was applied, which is changing behaviour towards compliance. *Points of changing behaviour = 2 points * (No. of compliance times after the last violation of the same policy) = 2*1= 2 points* Total points for User C for policy element no.2 = -5 points
On 28-Sep-2015:	This action was taken by the system because User C was compliant and the elapsed time had passed without any violation. This was the second compliance after the last violation and the user was under the optimal points, so the second mechanism for granting points was applied. *Points of changing behaviour = 2 points * (No. of compliance times after the last violation of the same policy) = 2*2= 4 points* Total points for User C for policy element no.2 = -1 points
On 27-Dec-2015:	This action was taken by the system. The elapsed time had passed without any violation for the third time after the last violation and the user points were still under the optimal points, so the second mechanism for granting points was applied. *Points of changing behaviour = 2 points * (No. of compliance times after the last violation of the same policy) = 2*3= 6 points, but the user was increased just 5 points because 5 points was enough to reach the optimal points for that date* Total points for User C for policy element no.2 = 4 points.
From 26-Mar-2016 until 19-Jun-2017:	In this period, User C was still complying and his/her compliance points had come in line with the optimal points, and therefore the system converted to the first mechanism for granting points (normal compliance behaviour). Based on that, User C was increased one point every three months during that period of compliance. Total points for User C for policy element no.2 = 10 points
On 23-Jun-2017:	User C violated the policy for the fourth time and changed his/her behaviour towards non-compliance. Because this violation occurred a long time after the last violation (around 2 years), the user may have forgotten the policy. Therefore, in this case, the user received level 1 as a response (basic awareness raising) and the time dimension type was considered to be long (T.P.=1). However, the escalation level (E.L.) was the same at Level 3. *Deducted Points = Escalation level (E.L.) * Time dimension points (T.P.)* *Deducted Points = 3 * 1 = -3 points,* Total points for User C for policy element no.2 = 7 points
On 18-Sep-2017:	User C violated the policy for the fifth time, around three months after the fourth violation, so the time duration was considered to be moderate (T.P. =2). The response level was escalated from Level 1 to Level 2, advanced raising of awareness. Deducted Points = Escalation level (E.L.) * Time dimension points (T.P.)

	Deducted Points = 3 * 2 = -6 point, Total points for User C for policy element no.2 = 1 points
On 10-Nov-2017:	User C violated the policy for the sixth time, around three months after the fifth violation, so the time duration was considered to be moderate (T.P. =2). The response level was escalated from Level 2 to Level 3, advanced raising of awareness. Deducted Points = Escalation level (E.L.) * Time dimension points (T.P.) Deducted Points = 4 * 2 = -8 point, Total points for User C for policy element no.2 = -7 points

6.5.4 Simulation result of scenario 4: Forgetful behaviour

The User D scenario was created to simulate forgetful behaviour of users. Therefore, during the simulation period, which was three years, starting from 01-01-2015 and ending on 01-01-2018, User D violated each element twice, and the duration between the two violations was long (seven months or longer). Therefore, User D's compliance points were decreased twice over the simulation period as well as receiving level 1 of the response taxonomy for non-compliance. To demonstrate how the system responded to the behaviour of User D, policy element no.18 was selected as an example. Figure 6.7 shows User D's compliance points for policy element no. 18 over the simulation period.

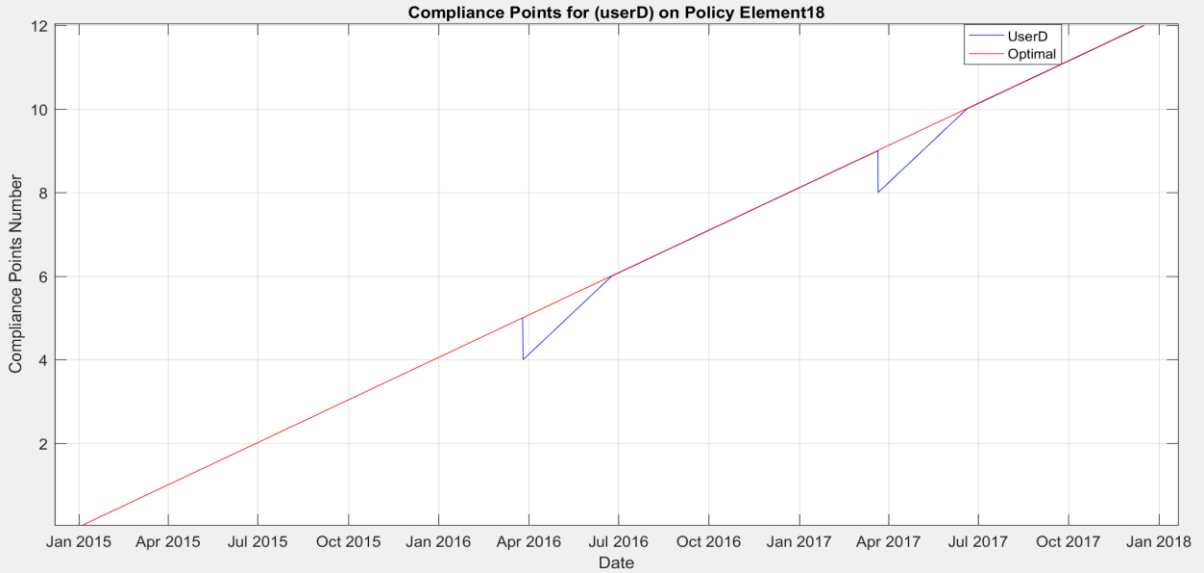


Figure 6.7: Screenshot for the simulation result of User D for policy element 18

As seen in the above figure, User D's compliance points for policy element 18 almost matched the optimal compliance points for that policy element except for the two times User D lost compliance points due to two different violations during the simulation period. The first violation was in March 2016, and therefore, the user received the level 1 response taxonomy for non-compliance behaviour, which is basic awareness raising, as well as having 1 point deducted from his/her compliance points rate for that policy. After the first violation, the user was compliant for approximately one year until the occurrence of the second violation, which was in March, 2017. The system responded to that violation by sending the level 1 response to User D again because the time dimension between those two violations was long (1 year). Therefore, it was considered that the user had forgotten to comply with that policy and only needed a reminder from category 1, which is level 1 (basic awareness raising). To demonstrate how the prototype system responded to User D behaviour, Table 6.10 shows User D's history for policy element no.18:

1 currentUser	2 PolicyNumber	3 Date	4 diff	5 EL	6 RL	7 ARL	8 Current_points	9 Total_points
'userD'	18	01-Apr-2015	2160:00:00	0	0	0	1	1
'userD'	18	30-Jun-2015	2160:00:00	0	0	0	1	2
'userD'	18	28-Sep-2015	2160:00:00	0	0	0	1	3
'userD'	18	27-Dec-2015	2160:00:00	0	0	0	1	4
'userD'	18	26-Mar-2016	2160:00:00	0	0	0	1	5
'userD'	18	26-Mar-2016	10814:00:...	1	1	1	-1	4
'userD'	18	24-Jun-2016	2160:00:00	1	1	0	2	6
'userD'	18	22-Sep-2016	2160:00:00	1	1	0	1	7
'userD'	18	21-Dec-2016	2160:00:00	1	1	0	1	8
'userD'	18	21-Mar-2017	2160:00:00	1	1	0	1	9
'userD'	18	21-Mar-2017	8643:40:00	1	1	1	-1	8
'userD'	18	19-Jun-2017	2160:00:00	1	1	0	2	10
'userD'	18	17-Sep-2017	2160:00:00	1	1	0	1	11
'userD'	18	16-Dec-2017	2160:00:00	1	1	0	1	12

Table 6.10: Screenshot for the simulation result of User D on policy element no.18

From 01-Apr-2015 until 26-Mar-2016:	User D was compliant during this period, so he was increased by 1 point every three months, which was the elapsed period of compliance for policy element no. 18. Total points for User D for policy element no. 18 = 5 points.

On 26-Mar-2016:	User D violated the policy for the first time, so the time dimension type was considered to be long (T.P.=1) because it was the first violation, so: Escalation level (EL) = level 1 Actual response level (ARL) = level 1 (Basic awareness) Deducted Points = Escalation level (E.L.) * Time dimension points (T.P.) Deducted Points = 1 * 1 = -1 point, Total points for User D for policy element no. 18 = 4 points
From 24-Jun-2016 until 21-Mar-2017:	User D was compliant during this specific period, so his points were increased using the two mechanisms for increasing points. The first mechanism, granting points for changing behaviour, was applied on the user because of his changing behaviour towards compliance and his compliance points on that policy were less than optimal, and therefore Use D was given 2 points. However, from 22-Sep-2016 until 21-Mar-2017, the user was switched to the second mechanism, granting points for normal behaviour, and his points increased by 1 point every month. Total points for User D for policy element no. 18 = 9 points
On 21-Mar-2017:	User D violated the policy for the second time. The time dimension type was long (T.P.=1) because the time between the two violations was 1 year, so: Escalation level (EL) = level 1 Actual response level (ARL) = level 1 (Basic awareness) Deducted Points = Escalation level (E.L.) * Time dimension points (T.P.) Deducted Points = 1 * 1 = -1 point, Total points for User D for policy element no. 18 = 8 points
From 19-Jun-2017 until simulation end:	User D was compliant, and therefore his/her points were increased during that period. Total points for User D for policy element no. 18 = 12 points

6.5.5 Simulation result of scenario 5: very noncompliant behaviour

The User E scenario was created to simulate very noncompliant behaviour. In this scenario User E violated each element of the security policies many times, with nearly 13 violations per policy element (nearly one violation every 90 days). Hence, during the simulation period, which was three years, User E did not gain any compliance points for any of the elements of the policies because he/she never passed the elapsed time of each element without any violation. To explain how the prototype system treated this scenario, the behaviour of User E with policy element no. 7 was selected. Figure 6.8 shows the compliance points trend for User E over the three years.

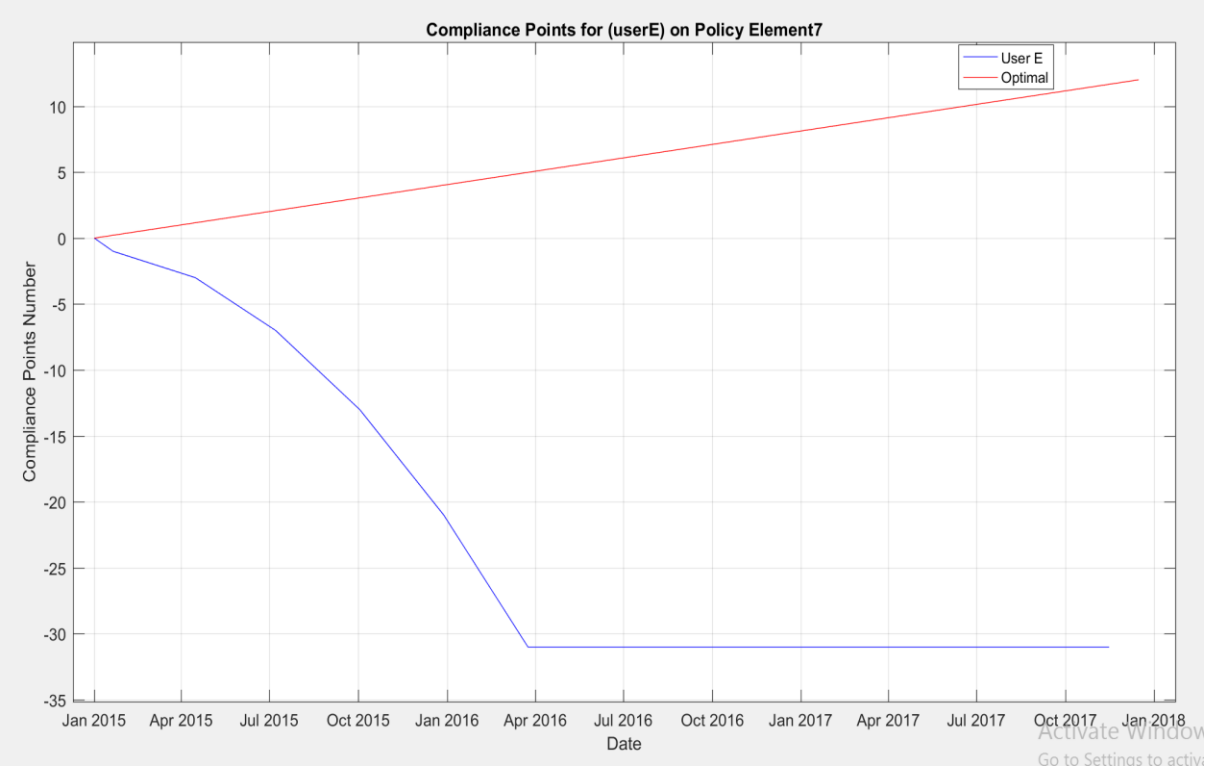


Figure 6.8: Screenshot for the simulation result of User E for policy element no. 7

It can be clearly seen that over the three years, User E's compliance points for policy element no. 7 dropped rapidly and no compliance points were gained. Apparently, the compliance points decreased gradually from the beginning of the simulation until reaching the minimum level of compliance points at -31 in Mar 2016. Here, the minimum level of compliance points means that with any new violations or losing of points the user will stay at that level of points. Therefore, since User E had reached the minimum level of points in Mar 2016, he/she continued to have the same level of points (-31points) until the simulation end, which means that the user maintained the same behaviour of non-compliance with that policy element during that period.

Furthermore, User E received all the five levels of responses as a countermeasure to his violations of this element of the policy, with the response severity escalating from level 1 to level 5. Table 6.11 demonstrates how User E's behaviour was processed by the prototype system.

1 currentUser	2 PolicyNumber	3 ViolationDate	4 diff	5 EL	6 RL	7 ARL	8 Current_points	9 Total_points
'userE'	7	20-Jan-2015	467:00:00	1	1	1	-1	-1
'userE'	7	15-Apr-2015	2041:00:00	2	2	2	-2	-3
'userE'	7	07-Jul-2015	1992:00:00	3	3	3	-4	-7
'userE'	7	02-Oct-2015	2088:00:00	4	4	4	-6	-13
'userE'	7	28-Dec-2015	2087:00:00	5	5	5	-8	-21
'userE'	7	24-Mar-2016	2089:00:00	5	5	5	-10	-31
'userE'	7	20-Jun-2016	2112:00:00	5	5	5	-10	-31
'userE'	7	15-Sep-2016	2088:00:00	5	5	5	-10	-31
'userE'	7	10-Dec-2016	2063:00:00	5	5	5	-10	-31
'userE'	7	05-Mar-2017	2041:00:00	5	5	5	-10	-31
'userE'	7	01-Jun-2017	2112:00:00	5	5	5	-10	-31
'userE'	7	27-Aug-2017	2088:00:00	5	5	5	-10	-31
'userE'	7	15-Nov-2017	1920:00:00	5	5	5	-10	-31

Table 6.11: Screenshot for the simulation result of User E on policy element no.7

on 01-Jan-2015:	User E violated the policy for the first time, so the time dimension type was considered to be long (T.P.=1) because it was the first violation, so: Escalation level (EL) = level 1 Actual response level (ARL) = level 1 (Basic awareness) Deducted Points = Escalation level (E.L.) * Time dimension points (T.P.) Deducted Points = 1 * 1 = -1 point, Total points for User E for policy element no.7 = -1 point
On 15-Apr-2015:	User E violated the policy for the second time, less than three months after the previous violation, so the time dimension was considered to be moderate (T.P.=2). The response level was escalated from Level 1 to Level 2, advanced raising of awareness. Deducted Points = Escalation level (E.L.) * Time dimension points (T.P.) Deducted Points = 1 * 2 = -2 point, Total points for User E for policy element no.7 = -3 points
On 07-Jul-2015:	User E violated the policy for the third time, less than three months after the previous violation, so the time dimension was considered moderate (T.P.=2). The response level was escalated from Level 2 to Level 3, Deducted Points = Escalation level (E.L.) * Time dimension points (T.P.) Deducted Points = 2 * 2 = -4 points, Total points for User E for policy element no.7 = -7 points
On 02-Oct-2015:	User E violated the policy for the fourth time, less than three months after the previous violation, so the time dimension was considered moderate (T.P =2). The response level was escalated from Level 3 to Level 4, Deducted Points = Escalation level (E.L.) * Time dimension points (T.P.) Deducted Points = 3 * 2 = -6 points, Total points for User E for policy element no.7 = -13 points

On 28-Sec-2015:	User E violated the policy for the fifth time, less than three months after the previous violation, so the time dimension was considered moderate (T.P. =2). The response level was escalated from Level 4 to Level 5, Deducted Points = Escalation level (E.L.) * Time dimension points (T.P.) Deducted Points = 4 * 2 = -8 points, Total points for User E for policy element no.7 = -21 points
On 24-Mar-2016:	User E violated the policy for the sixth time, less than three months after the previous violation, so the time dimension was considered moderate (T.P. =2). The response level was the same at level 5, Deducted Points = Escalation level (E.L.) * Time dimension points (T.P.) Deducted Points = 5 * 2 = -10 points, Total points for User E for policy element no.7 = -31 points
From 20-Jun-2016 until simulation end:	During this period User E committed at least one violation on this policy element, nearly one violation every 90 days. Therefore, the user stayed at the same level of points, at -31 points, over this period. Thus, despite losing more points, the user stayed at that level of points because the minimum level of points was set at -31.

6.5.6 Gaining insight on the implemented security policies.

As mentioned in the previous chapter (the theoretical chapter), the proposed model can help an organisation to understand and gain insight into each element of its security policies. In the following sections, and by using the five created scenarios, some results from the prototype system are explained. These results can be selected from the main input screen within the system from the results selection section.

6.5.6.1 Violations trend on a selected policy element over time

The violations trend over time for each policy element is offered by the prototype system. This report or chart can help an organisation to gain some useful information on each policy element, such as the peak number of violations of a specific policy element in a certain period of time. In the following example, policy element no. 16 is selected, as shown in Figure 6.9.

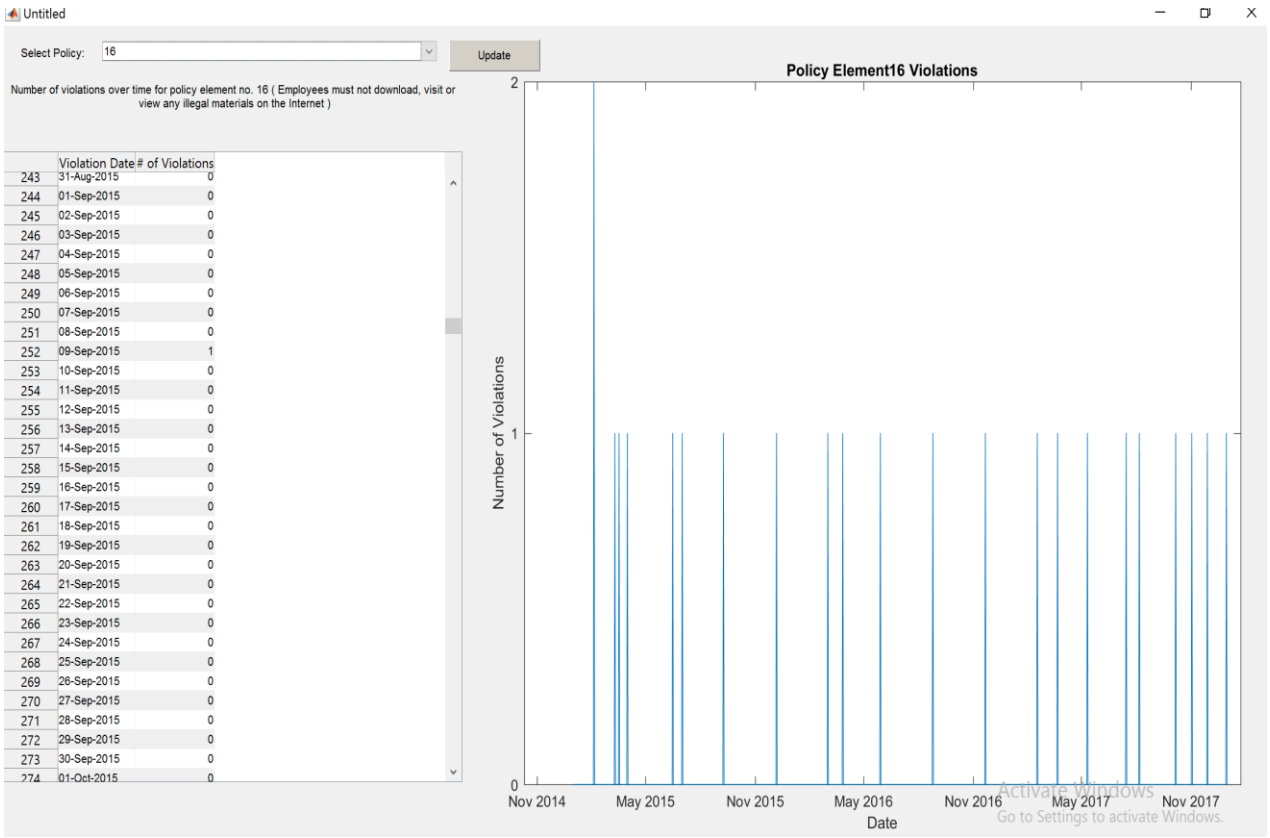


Figure 6.9: Screenshot of violations trend for policy element no.16

As demonstrated above, all the users' violations (User A, User B, User C, User D, User E) of policy element no.16 over the 3 years of the simulation are presented in the form of a graph and data. By using this graph, it is easy to identify which particular period has a maximum or minimum number of violations.

6.5.6.2 Total number of violations of all users of each policy element

Each policy element can count of all the users' violations, which can help an organisation to have a clear vision about its security policies. Thus, an organisation will have the ability to determine the total number of violations of each policy element, identifying which policy element has the most or least number of violations. In addition, this may help top management or the decision makers to evaluate the current state of such policies or even compare levels of compliance among them.

Thus, all the users' violations of each policy element during the simulation period are presented below in Figure 6.10.

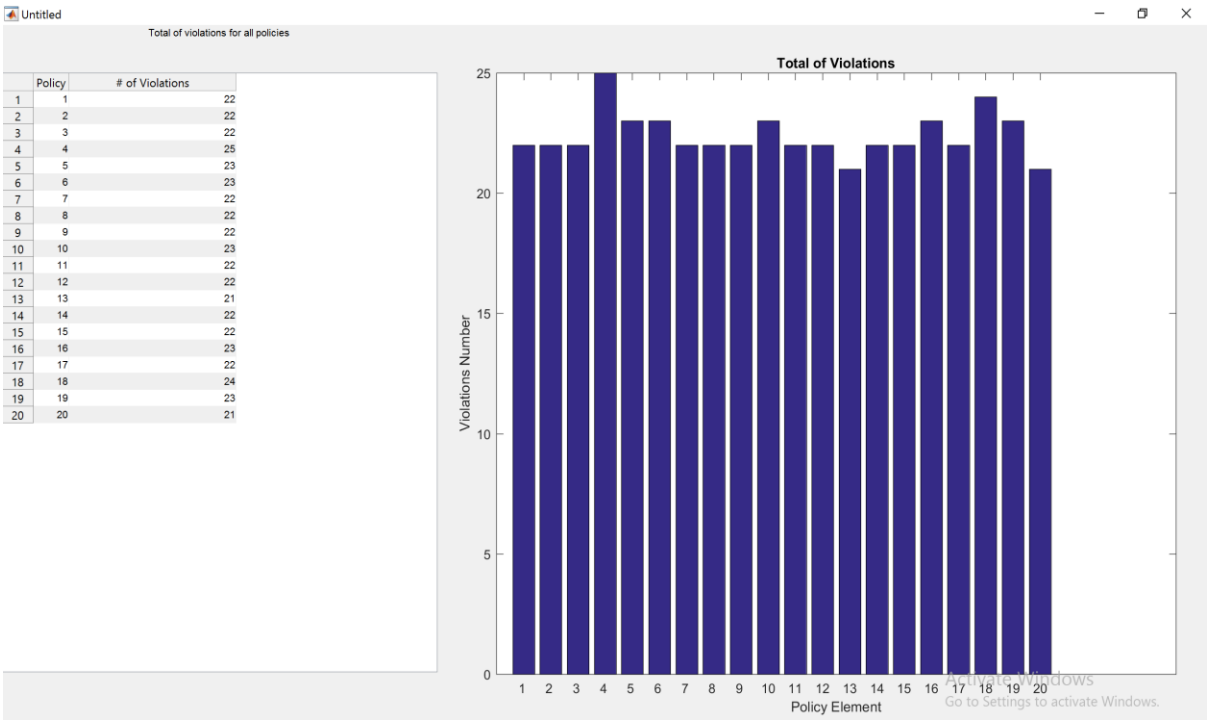


Figure 6.10: Screenshot of the total number of violations of all users for each policy element

The above screen demonstrates the total number of violations of the twenty elements of the policies. Thus, it can be seen that policy element no. 4 had the highest number of user violations at 25 violations during the 3 years. However, policy element no.13 had the lowest number of user violations at 21 violations.

6.5.6.3 Current level of the response taxonomy for all users with a selected policy

Whenever users are noncompliant, they will receive a certain level of the response taxonomy from the system. As such, it would be beneficial for an organisation to know the current level of each user's responses for each policy element. Therefore, within the prototype system, there is a screen that can generate a report on the current level of responses. For example, by selecting policy element no.2 from the dropdown menu, as in Figure 6.11, the current level of responses of all users is presented.

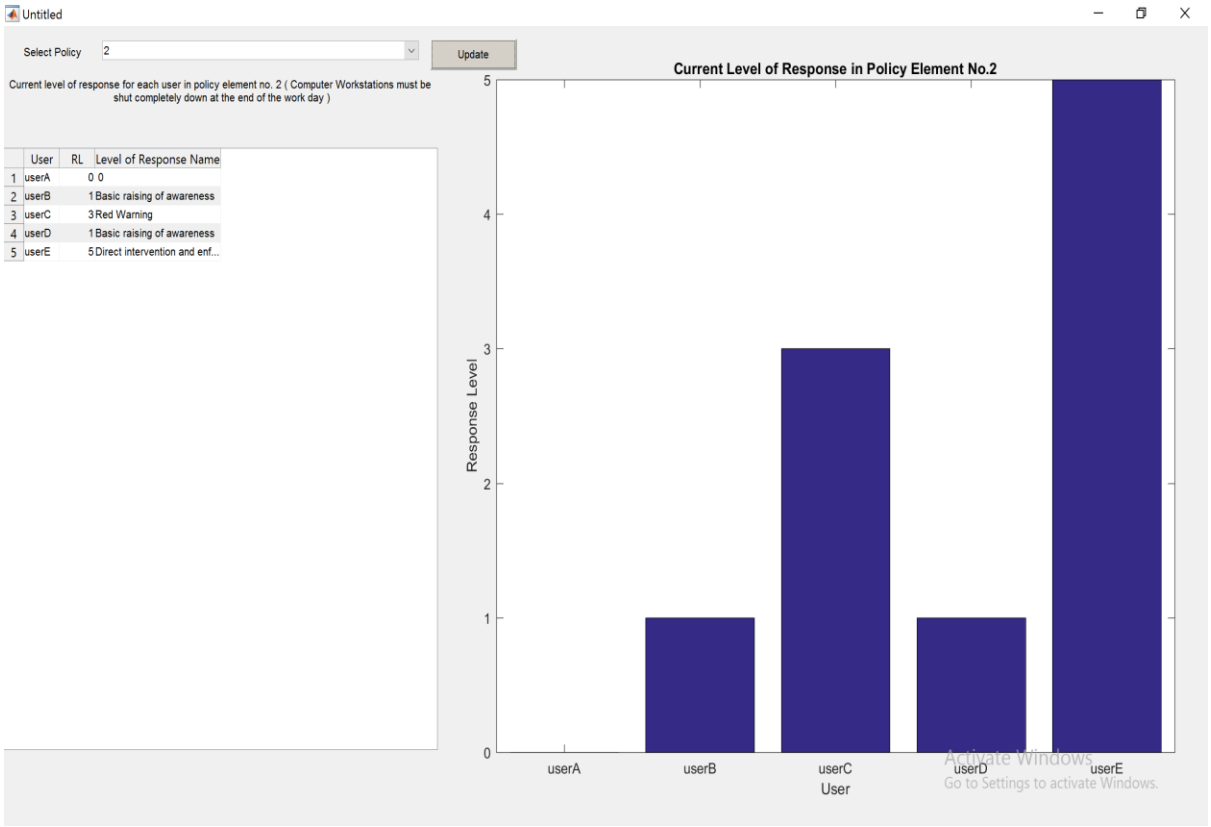


Figure 6.11: Current level of response for all users with policy element no. 2

As demonstrated above, the five users are displayed with their current level of responses for policy element no.2, as in the following:

- User A has not received any response level because no violations were committed during the simulation period.
- User B had response level 1 (Basic awareness raising).
- User C had response level 3 (Red warning).
- User D had response level 1 (Basic awareness raising).
- User E had response level 5 (Direct intervention).

6.5.6.4 Total number of responses for each user for a specific policy element

The prototype system provides a chart that displays the total number of responses for each user for any policy element. In other words, the total number of responses from all the response levels launched by the system for each user for a specific policy element. To

demonstrate this, the following figure 6.12 shows the total number of responses for policy element no 9.

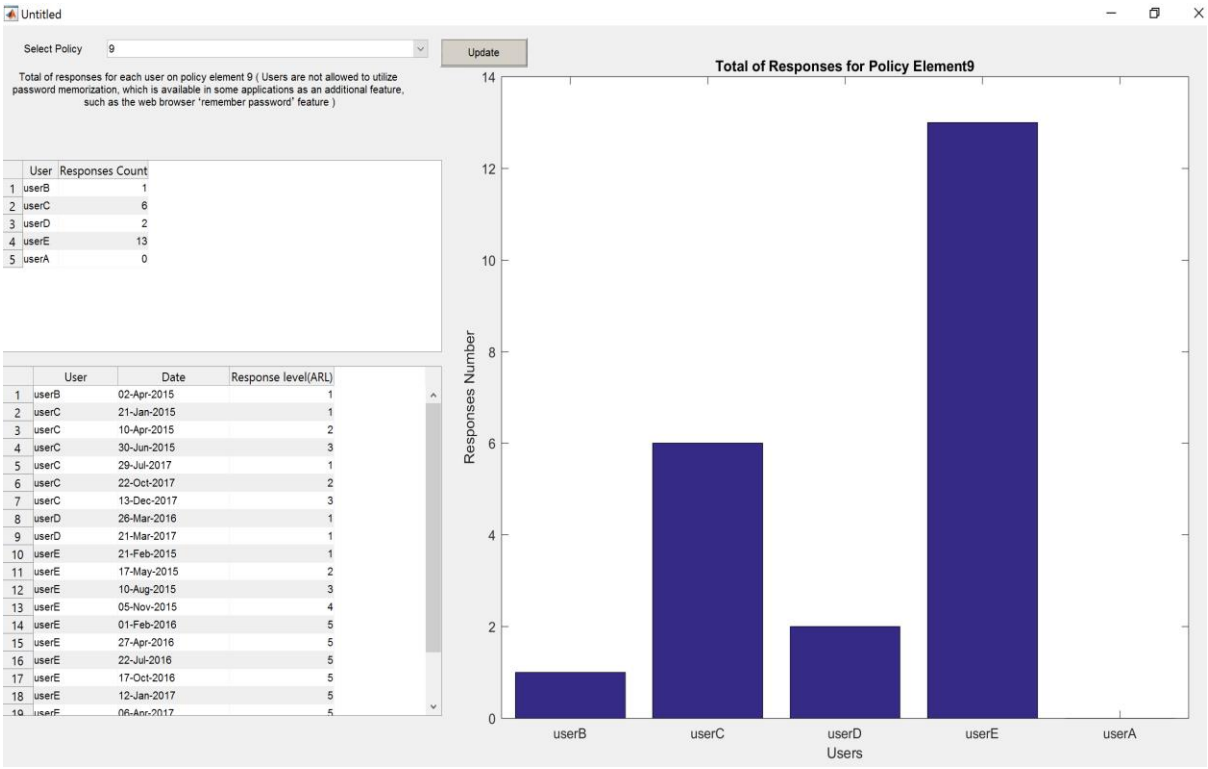


Figure 6.12: Screenshot for total of the responses for each user on the policy element no. 9

As demonstrated above, the total number of responses for each user for policy element no.9 is displayed, and each user had the following number of responses:

- User A did not receive any responses.
- User B had 1 response in total.
- User C had 6 responses in total.
- User D had 2 responses in total.
- User E had 13 responses in total.

Furthermore, the right side of the above chart (the screen) provides some useful information regarding each response, specifically the user's name, the date of the response and the level of response.

6.5.6.5 Counting the frequency of occurrence of each response level for each policy element

It is vital to monitor each policy element in terms of non-compliance behaviour and to know the frequency of the occurrence of each response level for each policy element. As explained previously, the response taxonomy for noncompliant behaviour is composed of five levels of responses, and therefore, the number of response for each response level for a particular policy element would be an indication of the success or failure of that response level. For example, if a policy element has the maximum number of responses at response level 1, that means level 1 was an effective response level because there were no escalations to the next levels of the responses to noncompliant behaviour. Figure 6.13 demonstrates how the prototype system visualises this concept.

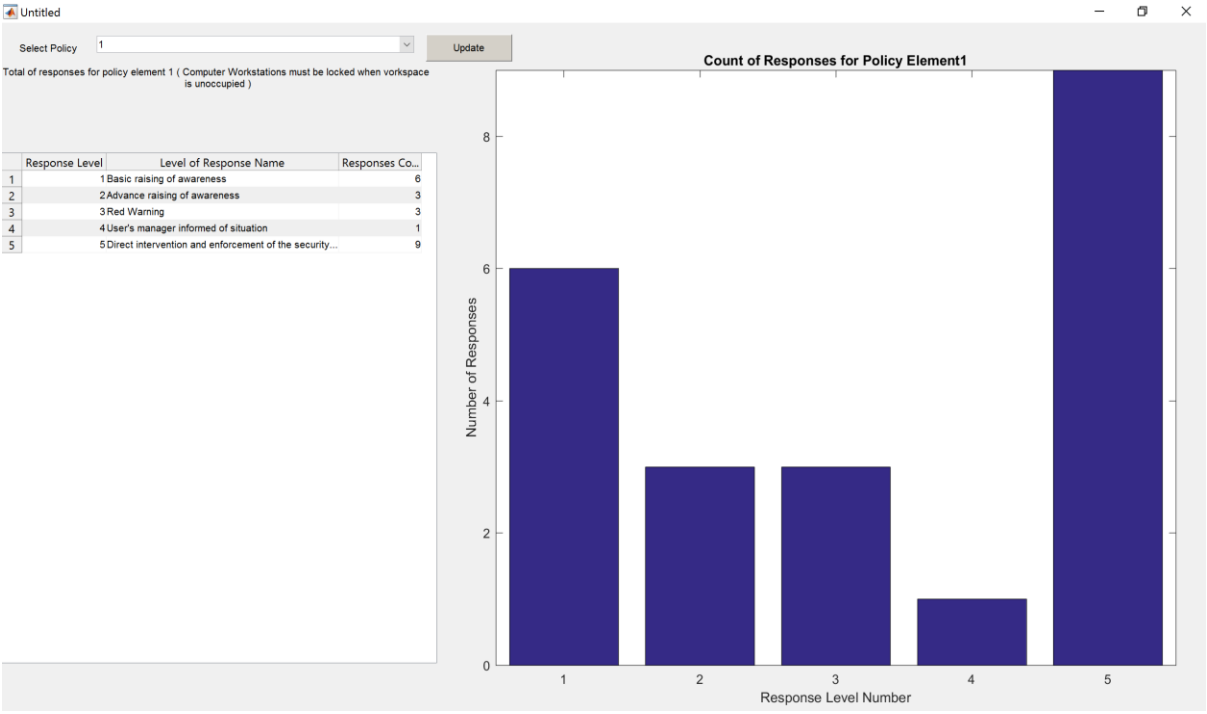


Figure 6.13: Screenshot for number of occurrence times of each response level on the policy element no. 1

As shown above, counting the number of times each response level occurred for policy element no. 1 is presented. Therefore, policy element 1 received a number of responses for each response level, as follows:

- Response level 1 occurred 6 times for policy element no. 1
- Response level 2 occurred 3 times for policy element no. 1
- Response level 3 occurred 3 times for policy element no. 1
- Response level 4 occurred 1 times for policy element no. 1
- Response level 5 occurred 9 times for policy element no. 1

6.5.7 Gaining insight into users' behaviours.

In the following sections, the simulation results of the five users are used to explain how the prototype system can provide some useful information and charts regarding the behaviour of those users.

6.5.7.1 Number of violations of each policy element for a selected user

The prototype system provides a screen that queries the total number of violations for each policy element for any users. Thus, a comprehensive report about a user's violations of each policy element is provided by the system, which can assist an organisation in measuring users' behaviour. For example, in Figure 6.14, User A is selected in order to present his violations of each element of the policies.

Figure 6.14: Screenshot for number of violations of each policy element for User A

Thus, User A did not commit any violations of any of the elements of the policies during the simulation period, and thus User A exhibited very compliant behaviour and his log of violations was empty. However, if a different user is selected, for example the User C, a different number of violations of each policy element is displayed, as in Figure 6.15.

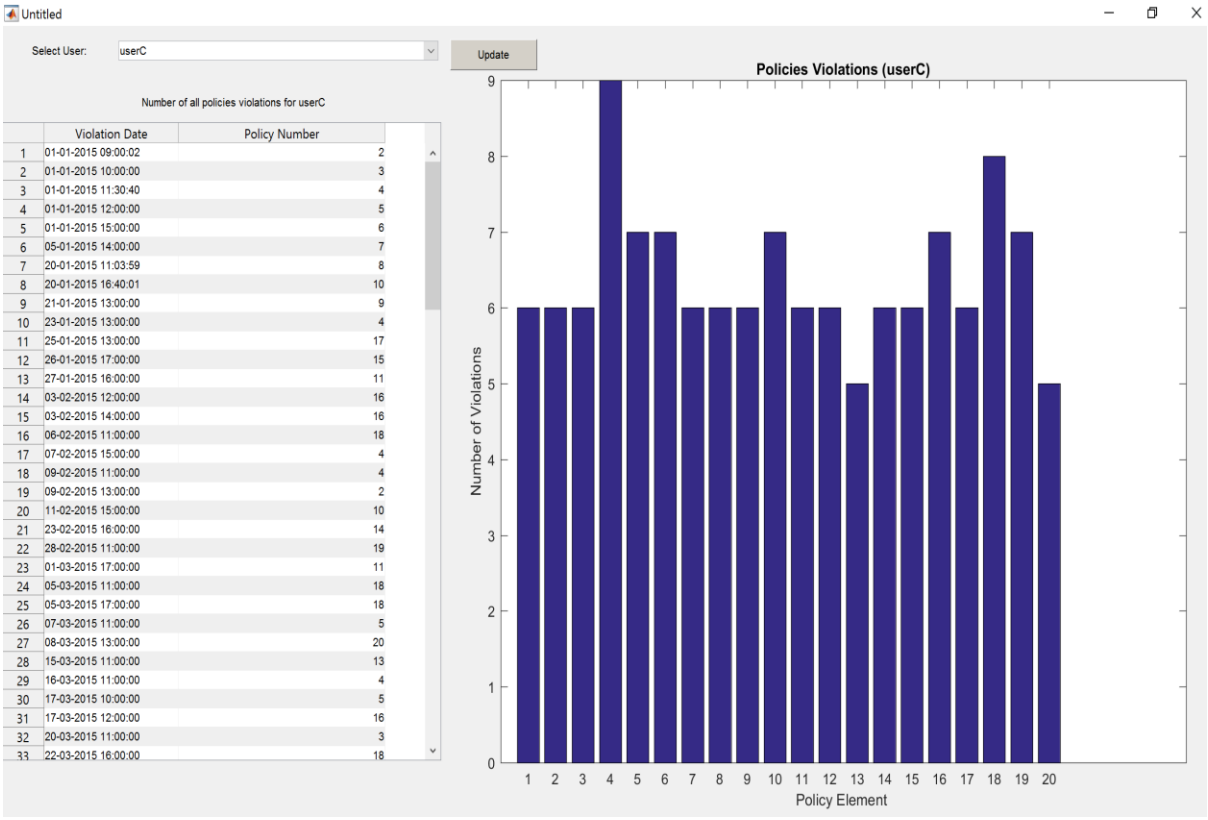


Figure 6.15: Screenshot for number of violations on each policy element for the User C

6.5.7.2 Total number of violations per user for a selected policy element

This chart enables organisations to gain insight into the total number of violations of a specific policy element by each user (or even department). Figure 6.16 shows the total of violations committed by each of the five users for policy element no 12.

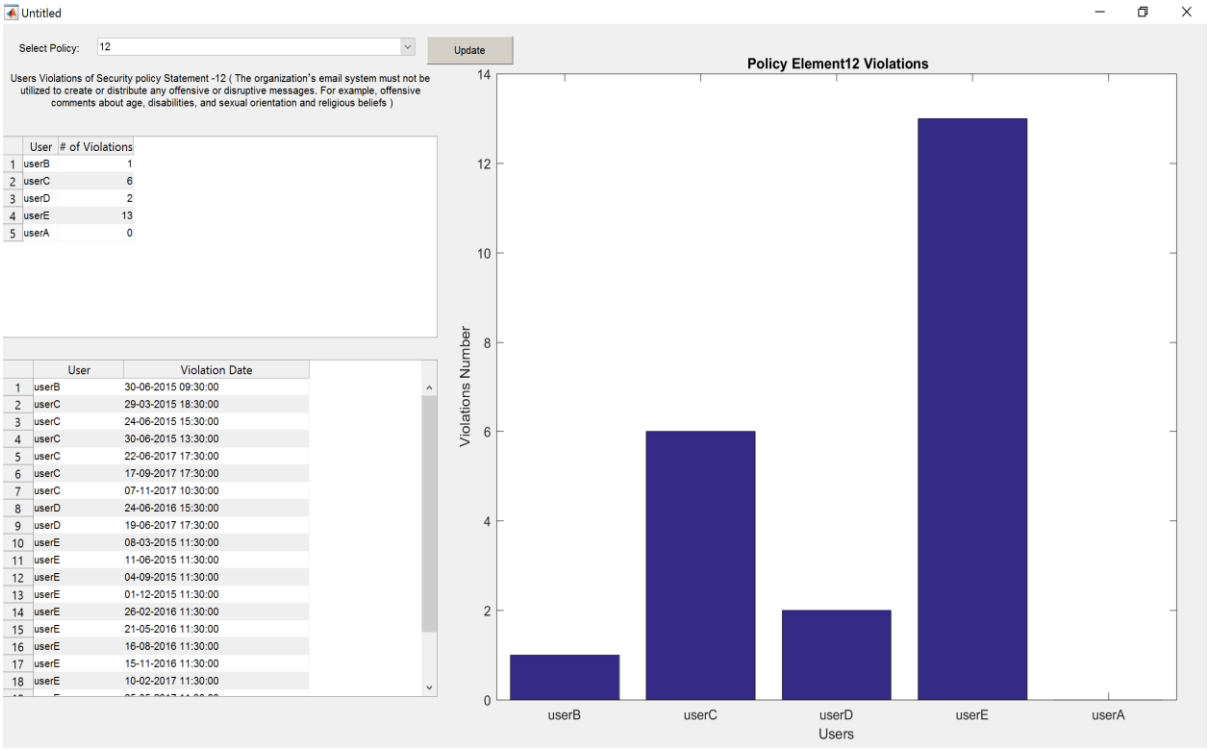


Figure 6.16: Screenshot of the total number of violations of all users of each policy element no. 12

As demonstrated above, all the users' violations of policy element no.12 are presented in the chart, each user separately. It can be seen that the most violations were committed by User E at 13 violations and, by contrast, the least violations were assigned to User A, with zero violations.

6.5.7.3 All policies violations per user

Another useful chart provided by the prototype system shows all the policy violations of each user. In this chart, a user is presented with his/her total number of violations of all the elements of the policies as one number. Figure 6.17 shows each user with all his/her violations of all the elements of the policies.

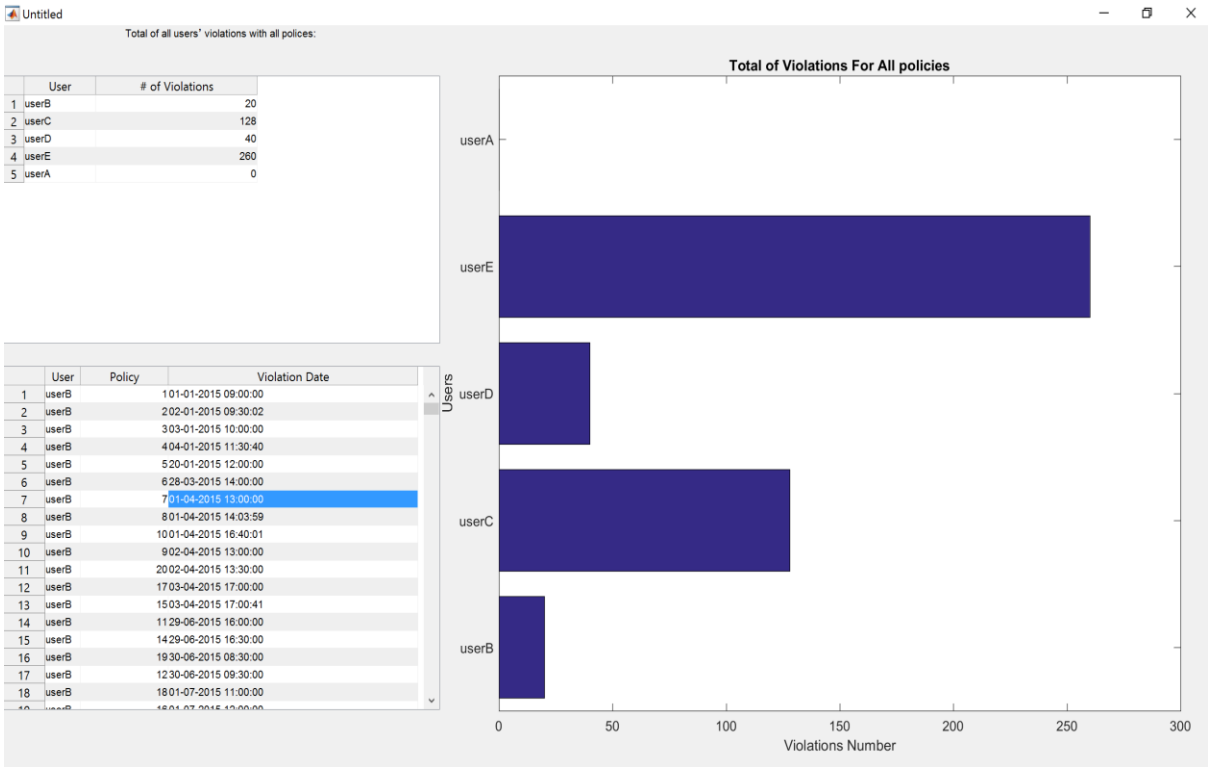


Figure 6.17: Screenshot of all the policy violations per user

In the above chart, each user has a total number of violations of all the elements of the policies, as listed below:

- User A had no violations (the optimal user)
- User E had 260 violations (the worst user)
- User D had 40 violations
- User C had 126 violations
- User B had 20 violations

6.5.7.4 Compliance points for a selected user with a selected policy

The trend of the compliance points of a user with any security policy element over time is presented in a chart by the prototype system. For example, the trend of User A compliance points with element no. 6 of the security policy over the simulation period is presented in Figure 6.18.

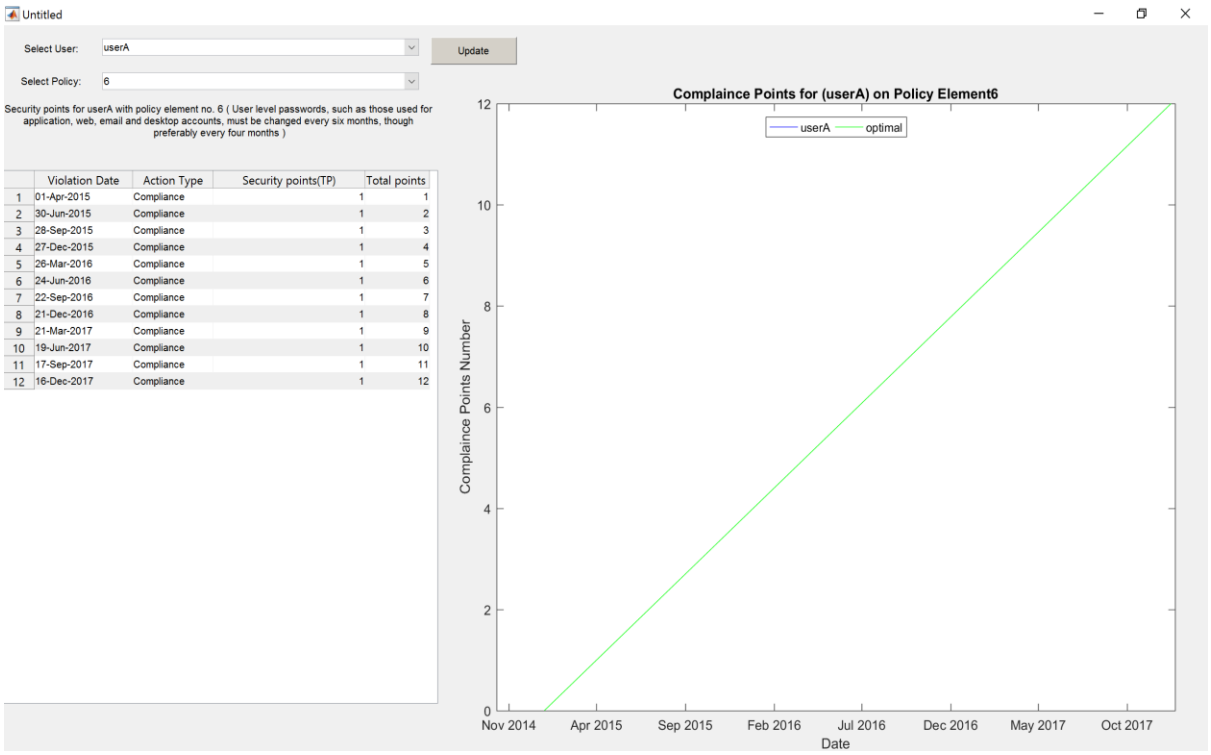


Figure 6.18: Screenshot for the compliance points for the User A with the policy element no. 6

As demonstrated in the above chart, there are two lines; one is for User A compliance points and the other is for the optimal points that the user is supposed to have. User A is a very compliant user because no violations occurred during the three-year simulation period, and therefore, the User A compliance line exactly matches the optimal line. Thus, from the beginning, User A increased 1 point for every 90 days of compliance, which is the elapsed time of policy element no. 6, as appears on the right side of the chart.

Another user was selected to further explain this concept. Figure 6.19 shows the compliance points of User D with policy element no.2 over the simulation period.

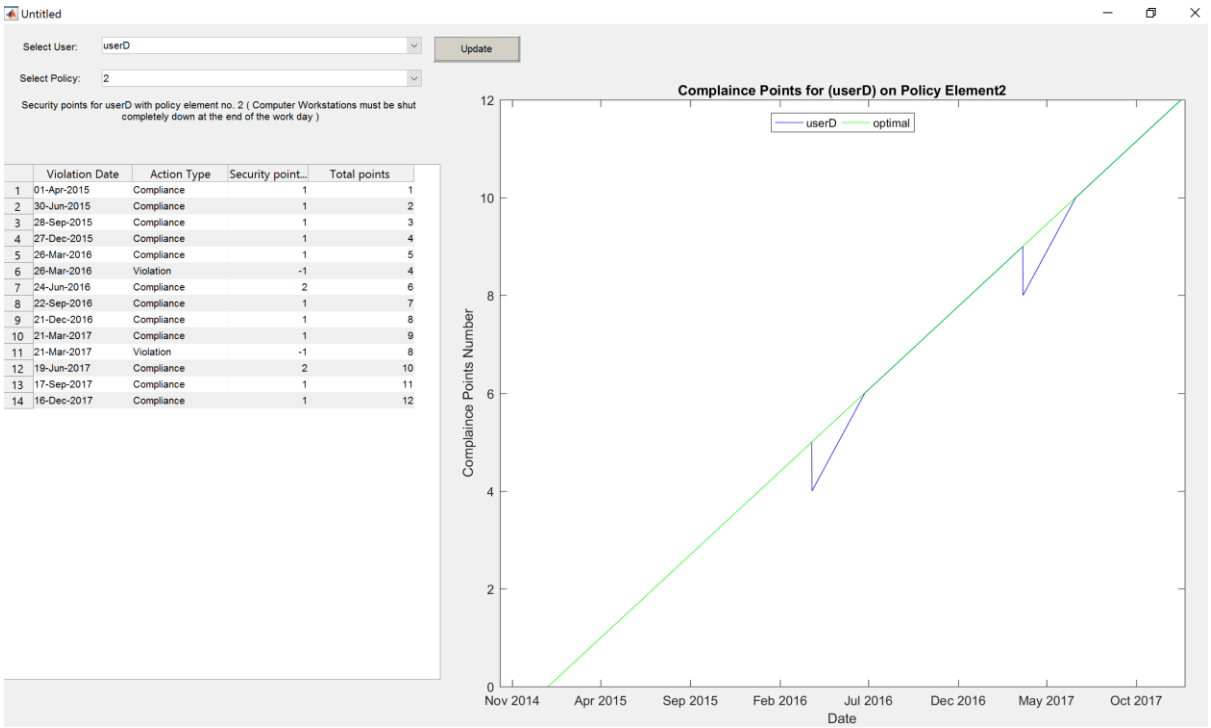


Figure 6.19: Screenshot of the compliance points of User D for policy element no. 2

As seen in the chart, User D compliance points for policy element no. 2 is compared with the optimal points, and points were lost twice during the three years. For more details, on the left side of the chart is a log or history of all actions taken by the prototype system in terms of increasing or deducting points from the user compliance points rate for that policy element.

6.5.7.5 Users weighted average compliance points summary for all policies

Each policy element has a weighted value according to its importance from an organisation's perspective. The weighted average formula is used to calculate the average value of user compliance points with the all the elements of the policies. Therefore, the weighted average compliance points for a user would be:

*Weighted average = w1 *x1 + w2 *x2 + w3 *x3…….. wn *xn / n*

W= relative weight for a policy element (0, 0.1, 0.2, 0.3……..1)

X= compliance points value of a policy element

In this simulation, the optimal compliance points for each policy element are 12 points (x) because the elapsed time of each policy element is 90 days, and therefore, 1 point every 90 days during 3 years will be equal to 12 points in total. Moreover, each policy element in this simulation was assigned a particular weight value (w). Hence, the optimal weighted average is calculated as follows:

*Weighted average = (12*0.5) + (12*0.2) + (12*0.9) + (12*1) + (12*0.7) + (12*0.2) + (12*0.7) + (12*0.4) + (12*0.8) + (12*1) + (12*0.8) + (12*0.9) + (12*1) + (12*0.5) + (12*1) + (12*0.8) + (12*0.1) + (12*1) + (12*0.3) + (12*0.7) / 20 = 8.1 points (at the end of the 3 years)*

Figure 6.20 shows all the users weighted average compliance points with all the policy elements at the end of the three years. Thus, using the chart, it is easy to compare each user's weighted average compliance points against the optimal weighted average, which can help organisations understand their employees' behaviour.

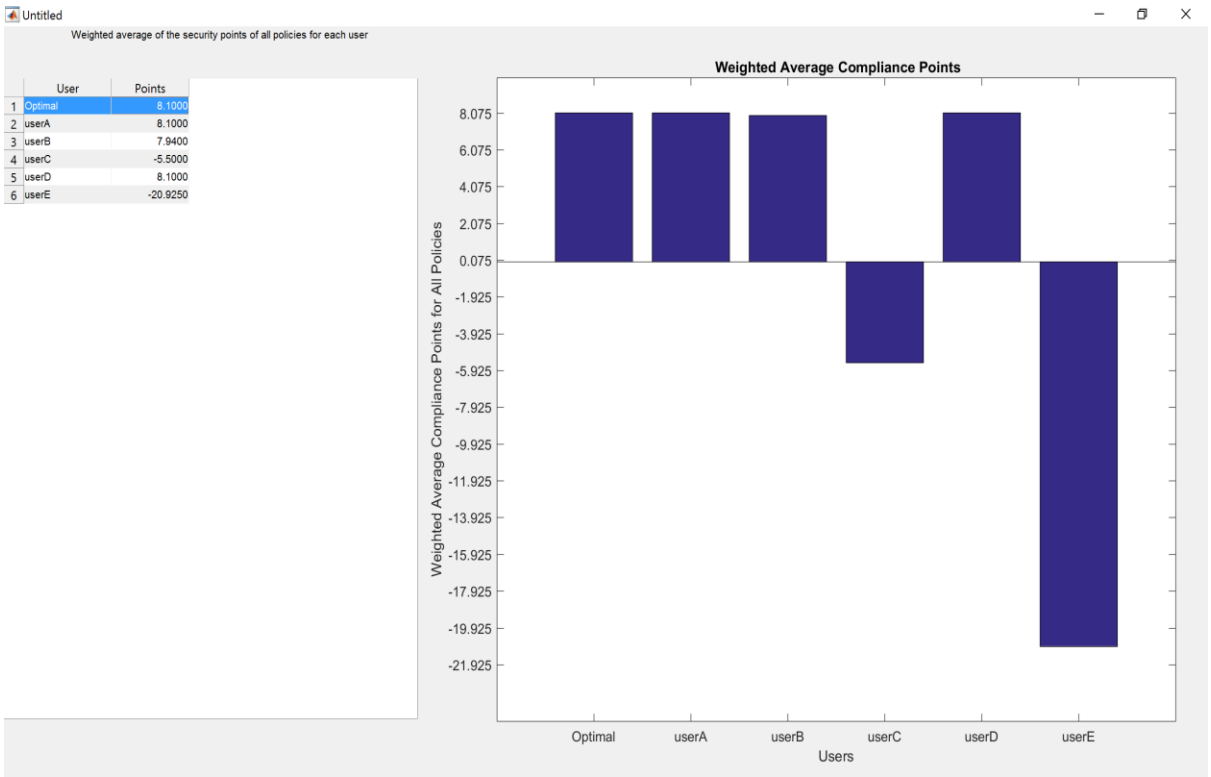


Figure 6.20: Screenshot of users weighted average compliance points summary for all policies

6.5.7.6 Compliance points for each user with selected policy

The current situation of the users' compliance points with any selected policy element is another feature that is provided by the prototype system. For example, from the simulation result, all the users current level of compliance points for policy element no.1 is demonstrated in Figure 6.21.

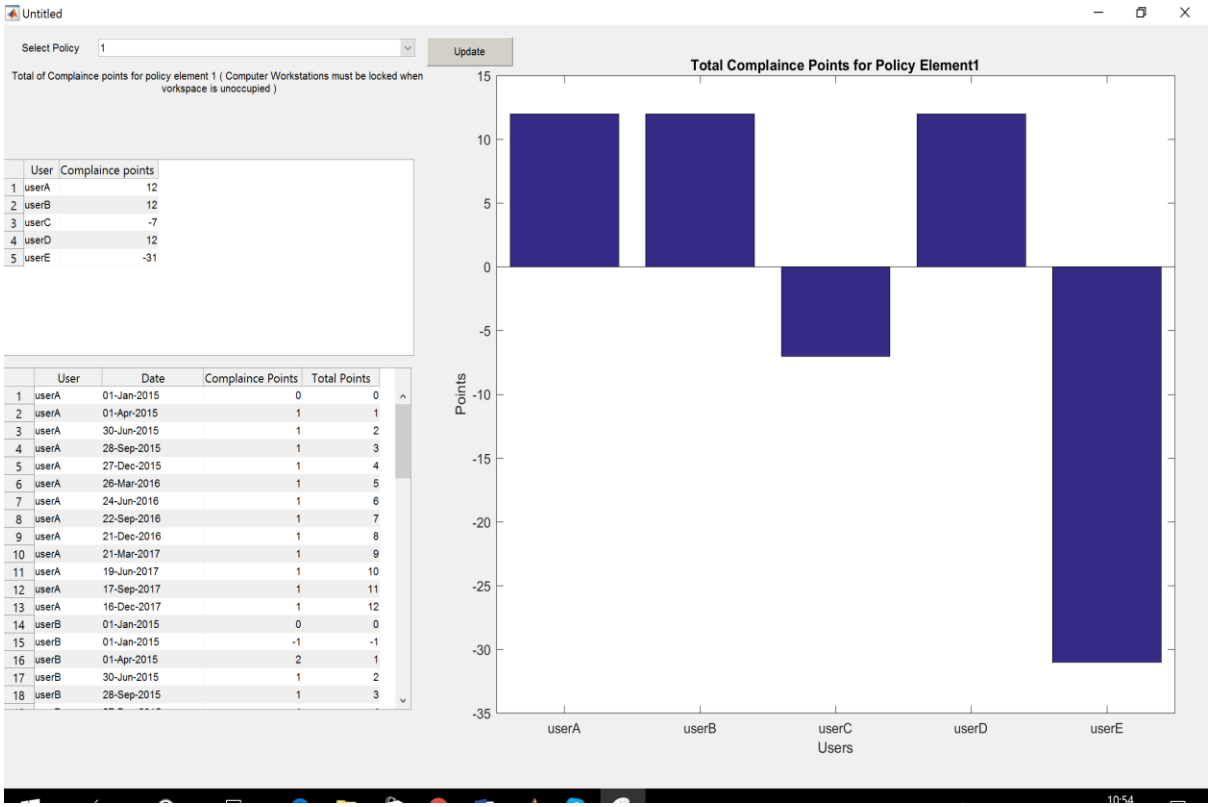
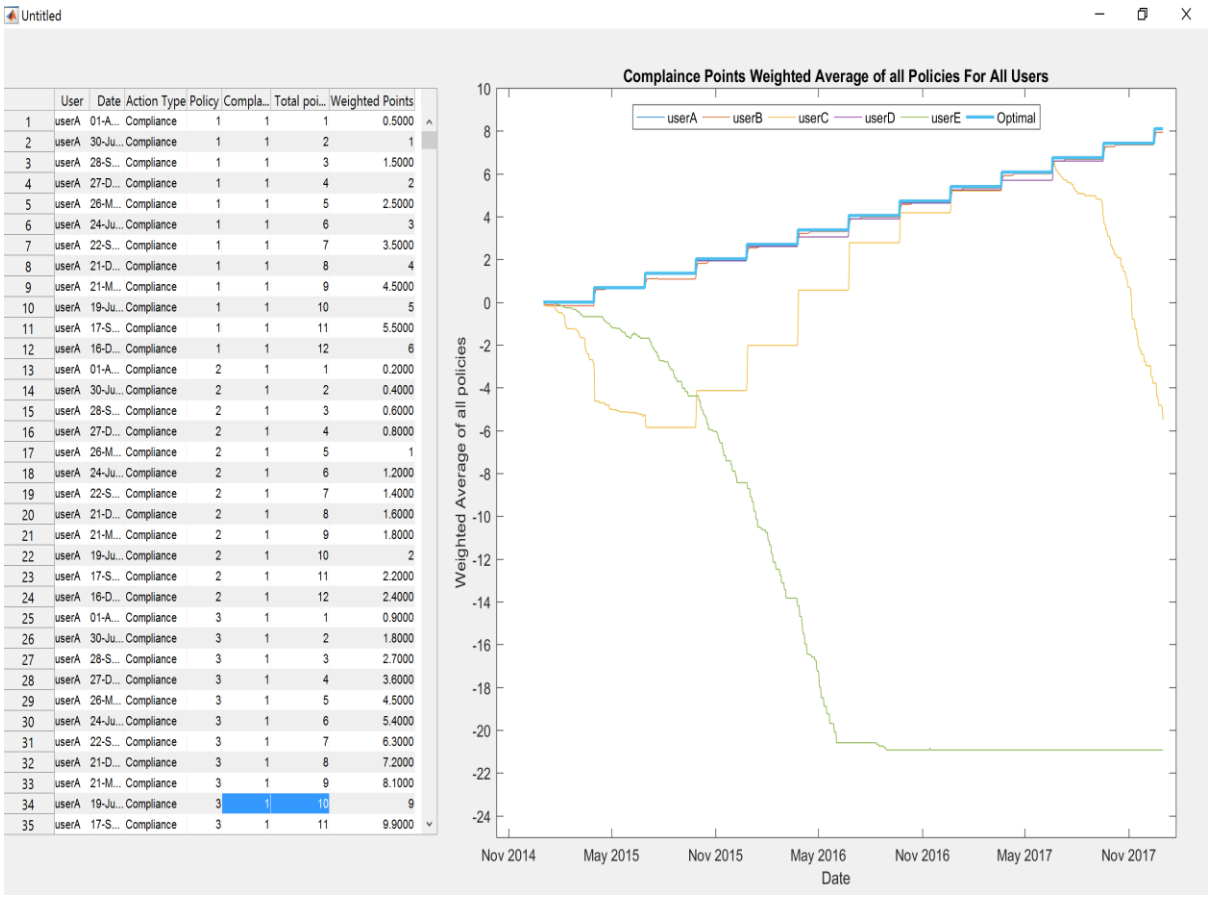


Figure 6.21: Screenshot for the current level of compliance points for each user with policy element no.1

6.5.7.7 Weighted average compliance points for all users over time

The trend of the weighted average compliance points of all users with all elements of the policies over a time is presented in this chart. Therefore, an organisation will be able to keep track of each user's behaviour with the whole policy. Figure 6.22 shows the trend of the weighted average compliance points of all the users over the simulation period of three years.



	User	Date	Action Type	Policy	Compla...	Total poi...	Weighted Points
1	userA	01-A...	Compliance	1	1	1	0.5000
2	userA	30-Ju...	Compliance	1	1	2	1
3	userA	28-S...	Compliance	1	1	3	1.5000
4	userA	27-D...	Compliance	1	1	4	2
5	userA	26-M...	Compliance	1	1	5	2.5000
6	userA	24-Ju...	Compliance	1	1	6	3
7	userA	22-S...	Compliance	1	1	7	3.5000
8	userA	21-D...	Compliance	1	1	8	4
9	userA	21-M...	Compliance	1	1	9	4.5000
10	userA	19-Ju...	Compliance	1	1	10	5
11	userA	17-S...	Compliance	1	1	11	5.5000
12	userA	16-D...	Compliance	1	1	12	6
13	userA	01-A...	Compliance	2	1	1	0.2000
14	userA	30-Ju...	Compliance	2	1	2	0.4000
15	userA	28-S...	Compliance	2	1	3	0.6000
16	userA	27-D...	Compliance	2	1	4	0.8000
17	userA	26-M...	Compliance	2	1	5	1
18	userA	24-Ju...	Compliance	2	1	6	1.2000
19	userA	22-S...	Compliance	2	1	7	1.4000
20	userA	21-D...	Compliance	2	1	8	1.6000
21	userA	21-M...	Compliance	2	1	9	1.8000
22	userA	19-Ju...	Compliance	2	1	10	2
23	userA	17-S...	Compliance	2	1	11	2.2000
24	userA	16-D...	Compliance	2	1	12	2.4000
25	userA	01-A...	Compliance	3	1	1	0.9000
26	userA	30-Ju...	Compliance	3	1	2	1.8000
27	userA	28-S...	Compliance	3	1	3	2.7000
28	userA	27-D...	Compliance	3	1	4	3.6000
29	userA	26-M...	Compliance	3	1	5	4.5000
30	userA	24-Ju...	Compliance	3	1	6	5.4000
31	userA	22-S...	Compliance	3	1	7	6.3000
32	userA	21-D...	Compliance	3	1	8	7.2000
33	userA	21-M...	Compliance	3	1	9	8.1000
34	userA	19-Ju...	Compliance	3	1	10	9
35	userA	17-S...	Compliance	3	1	11	9.9000

Figure 6.22: Screenshot of weighted average compliance points for all users over time

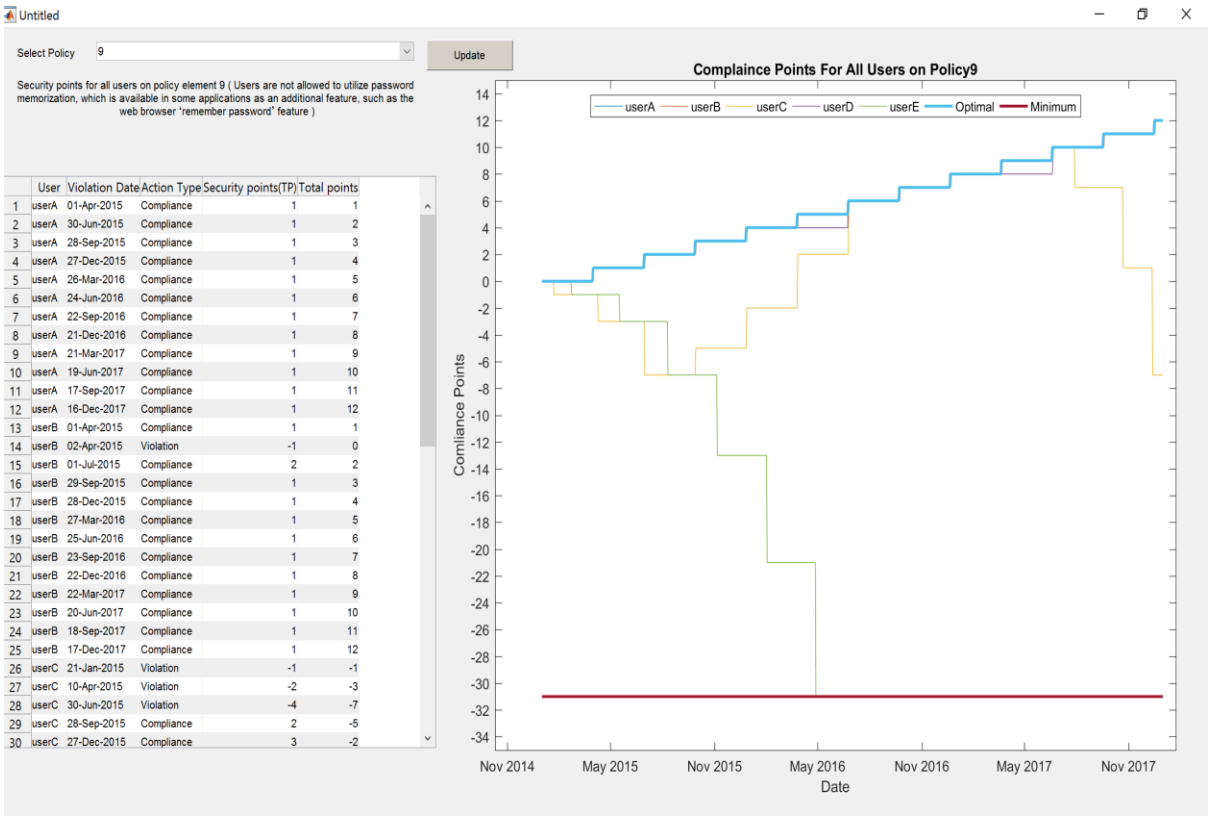
As seen in the chart, the optimal weighted average compliance points trend over the three years is presented. As such, any user's weighted average compliance points can be compared against the optimal, which gives an insight into user behaviour over a certain period of time.

As an example, User C weighted average compliance points give a clear image of his/her behaviour during the three years of the simulation, during which time User C had three main changes of behaviour. Firstly, he/she lost compliance points due to his/her non-compliance behaviour in the period from the beginning of the simulation almost until November 2015. Secondly, after that date, the user changed his/her behaviour towards compliance, matching the optimal points in November 2016. User C continued with compliance behaviour in line with the optimal level almost until July 2017. However, the third change of User C's

weighted average compliance points was from almost July 2017 until the end of the simulation when User C lost points due to his/her non-compliance behaviour.

6.5.7.8 Compliance points for users on selected policy over time

The trend of the users' compliance points with a selected policy element, the minimum level of the compliance points and the optimal points for that policy element are all presented in this chart of the simulation period. To explain this output of the prototype system, the users' behaviour in relation to policy element no. 9 is selected as an example. Figure 6.23 shows the trend of compliance points of all users for policy element no. 9.



	User	Violation Date	Action Type	Security points(TP)	Total points
1	userA	01-Apr-2015	Compliance	1	1
2	userA	30-Jun-2015	Compliance	1	2
3	userA	28-Sep-2015	Compliance	1	3
4	userA	27-Dec-2015	Compliance	1	4
5	userA	26-Mar-2016	Compliance	1	5
6	userA	24-Jun-2016	Compliance	1	6
7	userA	22-Sep-2016	Compliance	1	7
8	userA	21-Dec-2016	Compliance	1	8
9	userA	21-Mar-2017	Compliance	1	9
10	userA	19-Jun-2017	Compliance	1	10
11	userA	17-Sep-2017	Compliance	1	11
12	userA	16-Dec-2017	Compliance	1	12
13	userB	01-Apr-2015	Compliance	1	1
14	userB	02-Apr-2015	Violation	-1	0
15	userB	01-Jul-2015	Compliance	2	2
16	userB	29-Sep-2015	Compliance	1	3
17	userB	28-Dec-2015	Compliance	1	4
18	userB	27-Mar-2016	Compliance	1	5
19	userB	25-Jun-2016	Compliance	1	6
20	userB	23-Sep-2016	Compliance	1	7
21	userB	22-Dec-2016	Compliance	1	8
22	userB	22-Mar-2017	Compliance	1	9
23	userB	20-Jun-2017	Compliance	1	10
24	userB	18-Sep-2017	Compliance	1	11
25	userB	17-Dec-2017	Compliance	1	12
26	userC	21-Jan-2015	Violation	-1	-1
27	userC	10-Apr-2015	Violation	-2	-3
28	userC	30-Jun-2015	Violation	-4	-7
29	userC	28-Sep-2015	Compliance	2	-5
30	userC	27-Dec-2015	Compliance	3	-2

Figure 6.23: Screenshot for Compliance points for users on policy element no. 9 over the simulation period

As can be seen in the chart, all the users' compliance points plus the optimal compliance points and the minimum points are presented over the three years. The trend of the optimal points increases 1 point every three months during the three years because the elapsed time setting of policy element no. 9 is 90 days. User A compliance points for policy element no.9

exactly match the optimal level for that policy during the three years. However, if we look at the worst user, which is User E, we find that his/her compliance points dropped from the beginning until the end of the simulation, which means this user exhibited security noncompliant behaviour with this policy element during the 3 years.

6.6 Conclusion

During this chapter, the simulation process for the model proposed for monitoring information security policy compliance has been discussed. The prototype system was developed in order to simulate this model and facilitate understanding of its functionalities. Therefore, five users with different compliance behaviour profiles, and scenarios of some of the potential behaviour of those users, were created and then used to run the prototype system. Moreover, how the prototype dealt with each scenario or user type was explained in detail according to each action taken by the system as a response to the user's behaviour.

The prototype system was built based upon two main concepts; response taxonomy for non-compliance behaviour, and the compliance points system. According to the response taxonomy, a targeted response to a user's non-compliance behaviour or a policy violation may be an effective way of changing behaviour towards compliance. For example, if a user violates an information security policy for the first time, then he will need targeted awareness raising as a response because he may not be aware of that policy, and if he commits any further violations, there will be an escalation of the response taxonomy. In addition, the compliance points system is a supportive tool for organisations or security administrators, who can gain insight into users' behaviours and the effectiveness of their security policies.

A wide variety of results and charts were obtained from the prototype system regarding the five scenarios. The screenshots presented in the previous sections are the proposed system to

give an idea of how the processes for the model might be in the future or the real environment. The prototype represents the realisation of the proposed system based on the model for monitoring security policy compliance.

Having established an operational version of the system, it was necessary to determine whether it would be seen to be of value to the intended target audience, and whether the framework that it illustrates would be considered to be a relevant contribution to those working in the discipline. As such, an expert-based evaluation of the proposed model and its prototype system was necessary. The opinion of experts from both sectors, academic and industry, would provide important feedback on the usefulness of the proposed model, its limitations and any improvements that may need to be undertaken. Therefore, the next chapter addresses the experts' evaluation of the proposed model process.

Chapter Seven

Evaluation of the Model for Monitoring End-User Security Policy Compliance

7. Evaluation of the Model for Monitoring End-User Security Policy Compliance

7.1 Introduction

In addition to the practical simulation of the proposed model, a further qualitative evaluation method is deemed necessary. The main objective behind this evaluation is to gain quantitative feedback received from experts from different sectors including industry and academic, which helps to evaluate the proposed model and the associated development work. It is also significant to fulfil the academic requirements by following a well-known research methodology, which is experts based evaluation.

With the aim of cover experts point of views, 14 academics and practitioners have taken part in this evaluation. The participants, who were all experts on the subject matter, were carefully selected and a set of questions was accurately designed and presented to the experts. There was a detailed interview with the participants and different aspects regarding the proposed model were discussed, using the open-ended questions. Thus, it is vital for this project to be judged about its effectiveness and the actual implementation of it in the real world of the information security policies. In other words, it is important to assess the usefulness and value of the approach developed in this research from the domain experts' point of view.

The chapter begins with an explanation of the evaluation method used and its scope in general as well as the justification of the selected method. A further section gives more details about the experts who participated in this evaluation and basis of selection them as experts in the field. Finally, the findings of the evaluation process alongside with the experts' feedback are discussed by this chapter.

7.2 The Evaluation Method

The main aim of any research in any field is to contribute and add a new piece of knowledge to the already existing knowledge body of that field. Therefore, selecting the most suitable evaluation methodology will play significant role towards measuring the outcome of any conducted research. Thus, the expert surveys assist in gaining information from the specialists in the research field, by asking them certain questions on the subjects being researched. Usually, in the expert surveys methodology, open-ended questions are designed in order to receive a large amount of information regarding the researched matter and giving the participants the freedom of demonstrating their knowledge (Johnson & Turner 2003). Moreover, the open-ended questions can indicate a significant aspect, trend or opinion about the researched issue that the researcher may have not thought of it before. According to the adequate number of experts that needed to conduct an expert based evaluation, the research literature stated that the suitable range of experts should be up to 10 persons: 6 experts (Creswell 2007), 6-8 experts (Kuzel 1992) and 6-10 experts (Morse 2000).

And such, an expert-based evaluation (expert survey methodology) was selected with the aim of seeking the experts' feedback on the proposed model of monitoring security policy compliance. The selected participants, who are involved in this evaluation, were all experts in the research domain, since not everyone is eligible to take part in the evaluation process. In total, 14 experts with an academic and industry background were selected. The contribution of the experts with an academic background in this evaluation is important, since the educational context of the research and the need for a feedback that is adequate for the academic research. Likewise, the viewpoint of practitioners and professionals from the industrial sector is also important to be undertaken in the evaluation due to the natural of this kind of research and its practical requirements. Therefore, different opinions and perspectives

coming from experts with different knowledge backgrounds and experiences assist in investigating and evaluating the effectiveness and usefulness of the proposed model.

All the interviews were conducted remotely over Skype video calls, except one interview which was held on the basis of a face to face meeting. Because the interviewees were located in divergent countries, therefore, a Skype interview was selected as an effective way to hold the interviews with the experts. Prior to the expert interview, a brief video about the research concept, the proposed model and the prototype system was prepared and sent to each expert in order to help them to have an overview of the conducted research and to be familiar with it. The demonstration video is a proximately 15 minutes in length and it is available for access at: https://www.youtube.com/watch?v=ob_AKllblBs&t=807s .

The evaluation process was executed via two stages. Firstly, the invitations emails were sent to the experts seeking their participation on the evaluation process. After the expert accepting the invitation and answering any question that may be raised by him about the evaluation process, the formalities of consent were completed. An ethical approval form about the evaluation process was sent to the experts in order to make them fully understand their right during the participation and also to make them aware that the main purpose of this evaluation is to assess the proposed model, and was to be used as a part of the PhD study. In addition to that, the video about the study was sent to the experts and they could watch the video at their own time and convenience. Moreover, some experts were preferring to read further about the conducted study, therefore, some supportive documents and academic papers, which have been published by the author regarding the study, were sent to the them in this regards.

The second stage of the evaluation process was interviewing each of the experts individually and staring the evaluation process. As mentioned previously the Skype video call was selected as approach to conduct an expert interview, and the average time that spent with

each participant was 27 minutes long. During each interview a pre-defined set of opened ended questions were asked and detailed answers were gained from the experts. Thus, different aspects in relation to the evaluated study have been discussed in more details with each expert.

The next section gives image about the scope of the evaluation process, and the reasoning and logic behind the selection of the interview's questions.

7.3 Evaluation Scope

The evaluation questions were designed in a manner that examine the proposed model in relation to several important aspects, therefore, the covered aspect during the evaluation process were:

- Validity of the research problem
- Feasibility at the operational level
- Utilising the concept of response taxonomy
- Utilising the concept of compliance points system
- Possibility Implementation of the proposed model
- The simulation tool (prototype system)
- Usefulness of the propose model
- Strengths & weaknesses

Thus, a total of 8 questions were created to obtain perspectives regarding different aspects on the study to give a clear picture about it. The evaluation questions are given as follows:

1. **What are your thoughts of the identified research problem?** The main aim of this question was to investigate the validity of the research problem and how the field experts see such a problem.

2. **How realisable/attainable/feasible do you feel this model is at the operational level?** It is vital to investigate the realizability and feasibility of the proposed model if it implemented in the real environment. The experts within the field of information security can give insight into how effective the model is.
3. **What do you think about utilising the concept of response taxonomy for the non-compliance behaviour in enhancing users' compliance?** The concept of response taxonomy for the non-compliance behaviour is new concept and it will be valuable for the author to gain experts feedback on that concept.
4. **What do you think about utilising the concept of compliance points system to monitor the compliance levels in order to gain insight on users' behaviour and Implemented information security policies?** A compliance points system is a novel approach and has not yet employed with the information security policies, therefore, it is necessary to investigate experts' opinion about it.
5. **To what extent do you feel the simulation have provided a robust validation of the approach?** The simulation process has been developed to visualise and explain the proposed model. Prior to interview each expert a demo of the system will be presented to the participant via watching a video on the YouTube (15 minutes) in order to provide them with a better insight into how it works. Therefore, this question was designed to investigate whether the simulation process was clear and covering all the aspects.
6. **How realisable/attainable/possible do you feel this system is?** The aim behind this question was to find out how easy it is to implement the proposed model, the possibility of deploying such a system from the perspective of the experts.
7. **To what extent do you think having the proposed model can assist organisations in monitoring and measuring users' behaviour with each element of the security**

policy in a dynamic way? If the proposed model is implemented by an organisation, can the model help it to monitor and measure the users' behaviour as well as gaining insight on the implemented security policy.

8. **What do you feel are the particular strengths & weaknesses of the developed system and any barriers using such a system?** This question aims to find out the opinion of the subject-matter experts regarding strengths, weakness or any barriers of deploying the proposed model.

As it is noted above, the questions were designed to mainly evaluate the entire approach towards the development of the model of monitoring security policy compliance. Therefore, the experts' feedback and responses were grouped and analysed based upon the above-mentioned questions. The next section describes the experts who participated in the evaluation.

7.4 Interviewees

This section gives more details about the chosen experts, who took part in this evolution, alongside the justification of selection these experts. Since the study is regarding the users' behaviour with the information security policies, the selected experts were taken from suitable backgrounds so that they already have the needed expertise and knowledge to evaluate the proposed model. Experts from different backgrounds including academic and industry were selected to evaluate the proposed model in order to gaini opinions from different environments, academics and practitioners.

The internet was used to search for the appropriate experts, and the selection criteria were made based on the following points:

- Members of scientific conferences committees related to the research area
- Authors of work thematically related to research articles in scientific journals.

- Scientists from related fields working also as lecturers or as administrative staff members in educational institution.
- Practitioners and professionals in the field of information security, information security officers or administrations

A list of candidates was made and the final 14 experts from the academic and professional backgrounds were selected are listed below. The experts can be divided into two categories whether academics (7 experts) or practitioner (7 experts).

7.4.1 Academics

A1- **Prof. Rossouw von Solms** is a professor and director of the Centre for Research in Information and Cyber Security, School of ICT, Nelson Mandela Metropolitan University (NMMU), Port Elizabeth, South Africa. He supervises many PhD and postdoctoral students in the field of Information Security and IT Governance. Rossouw has published and presented in excess of one hundred and fifty academic papers in journals and conferences, both internationally and nationally. Most of these papers were published and presented in the field of Information Security.

A2- **Prof. Stephen V. Flowerday** is presently a professor focusing on Information Security at the University of Fort Hare, South Africa. He is also lecture in the following two subjects: Information Security and Research Methods. Stephen has supervised postgraduate students and published extensively within his research field, East London, South Africa. Over the last twelve years, he has authored in excess of 70 refereed publications and have presented papers in various countries. Furthermore, he acts as a reviewer for conference publications and academic journals. He has supervised more than 30

postgraduate students to completion and am currently supervising many of master's and doctoral students in the field of Information Security.

A3- **Prof. Simon Tjoa** is a lecturer/ Security Analyst in the Department of Computer Science and Security at St. Poelten University of Applied Sciences, Austria. His fields of interest are Business Process Management, Risk Management, Information Security Management, Digital Forensics, Critical Information Infrastructure Protection, Business Continuity Management. He has more than 17 years' experience in field of information security. Prof. Simon has several industry recognised certifications including ISO 22301 Lead Auditor, Certified Information Systems Auditor (CISA). Certified Information Security Manager (CISM).

A4- **Dr. Christos Kalloniatis** holds a PhD from the Department of Cultural Technology and Communication of the University of the Aegean and a master degree on Computer Science from the University of Essex, UK. Currently he is an assistant professor in the Department of Cultural Technology and Communication of the University of the Aegean. Dr Kalloniatis' main research interests are the elicitation, analysis and modelling of security and privacy requirements in traditional and cloud-based systems, Privacy Enhancing Technologies and the design of Information System Security and Privacy in Cultural Informatics. He is an author of several refereed papers in international scientific journals and conferences and has served as a visiting professor in many European Institutions. Prior to his academic career Dr Kalloniatis has served at various places on the Greek public sector including the North Aegean Region and Ministry of Interior, Decentralisation and e-Governance. He is a lead-member of the Cultural Informatics research group

as well as the privacy requirements research group in the Department of Cultural Technology and Communication of the University of the Aegean and has a close collaboration with the Laboratory of Information & Communication Systems Security of the University of the Aegean. Dr Kalloniatis has also served as a member of various development and research projects.

A5- **Dr. Spiro Samonas**, is currently an assistant professor in information systems at California State University, Long Beach, USA. Prior to this appointment, he was a visiting assistant professor in computer information systems at Louisiana Tech University and a post-doctoral research fellow in cyber-security at Virginia commonwealth University. His research focuses on digital deception and digital crime, and the socio-technical aspects of information security. His academic research focuses on an assortment of governance and policy issues that are pertinent to Information Security, such as cyber-crime and cyber-fraud, the insider threat, managerial autonomy and information security compliance, and polymath education in information security management.

A6- **Dr. Malcolm Pattinson** is a researcher in the Business School of the University of Adelaide and an Information Security Consultant, Australia. He has been lecturing and researching in the area of information security for more than 20 years. His current research focuses on the human aspects of information security and he is widely published in this area. He has been an active member of the Adelaide Chapter of ISACA for more than 15 years and has the certifications CISA, CISM and CGEIT. He is also a Member IFIP TC-

11 Working Group 11.12, Human Aspects of Information Security & Assurance (HAISA).

A7- **Dr. Nader Sohrabi Safa** is currently working lecturer at the University of Warwick, UK. He received his PhD from Faculty of Computer Science and Information Technology, Information System Department, University of Malaya. He is a member of IFIP TC 11 Working Group 12. He also is a member of committee in several annual conferences and reviewer in several journals. His research interest is in the domain of human interaction with systems and human aspects of information security. Also, his research focuses on Human Aspects of Information Security in Organizations in postdoctoral study.

7.4.2 Practitioners

P1- **Sofoklis Kotsaris** is an information security professional focused on the areas of risk analysis, threat assessment, cyber security and compliance, security policies development, security awareness and advanced security solutions implementation. Sofokils is a senior information security consultant and risk management consultant at PwC Belgium. Before that he was an information security consultant at PwC Greece. He has a master's degree in information security from Glamorgan University, UK. Sofokils has several industry recognised certifications including certified Information Systems Security Professional (CISSP), Certified Information Security Management Systems (ISMS) Lead Auditor, Certified Information Systems Auditor (CISA), COBIT 5 Foundation.

P2- **Mamdoh Alzhrani** is an information security expert in Cyber Risk Management and Strategic Analysis with over 14 years of experience in

diverse technical, senior management advisory and consultancy positions. He is currently working at the National Commercial Bank in KSA as a senior information security officer. He gained a MSc degree in computer system security at University of south wales (UK). Mamdoh has several industry recognised certifications including Certified Ethical Hacker (CEH), Certified Security +, GIAC Certified Incident Handler (GCIH), Certified Information Security Manager (CISM), GIAC Continuous Monitoring Certification (GMON).

P3- **John Finch** is the Information governance manager for Plymouth City Council, responsible for Data protection, security policy development and management, managing the Information Asset Register managing security incidents, providing security advice for the Council and partners, providing security awareness education for senior management. Previously, John spent 7 years in a technical security role, as IT Security manager for Plymouth City Council, managing the compliance of the Council network and technical breaches. John has been chair of several regional security forums, including the SW WARP and Devon Information Security partnership, and has been a conference speaker at National Information Security conference in 2008 and 2010. He was involved with the delivery of the IA guidelines for the Public Services Network delivered by the cabinet office. John is a current CISSP, and undertook an IT master's degree at Plymouth University in 2001.

P4- **Usman Quresh** is currently working at Shared Services Connected Ltd, UK as a test tanager. He is an experienced IT Contractor with over fifteen years' commercial experience with over nine years in testing. Also, he was an incident management analyst at SQS grump, London, UK He gained his MSc

degree in computer forensics, information security, from the University of Bradford in 2009.

P5- **Dr. Georgios Magklaras** is a computer scientist working as a Senior Computer Systems Engineer at the University of Oslo, in Norway. He is an information security researcher and developed methods in the field of insider IT misuse detection and prediction. He is also an active systems administrator information security consultant and Information Technology practitioner working with High Performance Computing. His research was initially concerned with ways to classify computer security incident management responses. However, his attention was drawn to the problem of misuse detection. Magklaras developed one of the first methods to systematize the misuse detection and misuse prediction techniques. Prior working at the University of Oslo, Magklaras has worked in various technical and scientific positions for many of companies and organizations, including those of Sequent Computer Systems, Boeing and IBM UK. He has held many of professional affiliations, including those of an IEEE affiliate member, USENIX, SAGE/LOPSA and Red Hat Certified Engineer. He has held the position of Secretary (since 2005) and Chair (since 2010) of the Technical Management Project Committee of the EMBnet organization.

P6- **Nick Sharratt** is an enterprise security architect at Plymouth university. Sharrat Sibt gained his BSc in Computer Science from Aston University in 1991. He has more than 20-year of experience in the field of information security and systems management.

P7- **Saud Al-otaibi** is an IT professional with 15+ years in the field of information security. He is currently working as a cyber security advisory at KPMG Saudi.

He previously served at Saudi Telecom Company (STC) as monitoring supervisor in security operation centre which handling & investigate all security incident that reporting from multiple security systems such as: firewalls, IDS, IPS, from 2004 till 2008. Also he worked at Alinma Bank as manager of security infrastructure from 2008 till 2012. Saud has several industry recognised certifications including Certified Information Systems Security Professional (CISSP), Certified in Project Management Professional (PMP), Certified Ethical Hacker (CEH), Certified EC-Council Certified Security Analyst (ECSA), Certified ArcSight Certified Security Analyst (ACSA), Certified in IT Infrastructure Library (ITIL).

7.5 The Experts' Feedback

The evaluation questions were designed in a way that examines the proposed model in terms of different aspects including, validity, usability, efficiency, reliability and weakness. An open-closed question was used as an effective method towards encourages a full and meaningful answer from the interviewees. Moreover, there was a live meeting with each expert of the participants to voice feedback and provide interactive opinion on the effectiveness of the approach and its prototype system. Prior to starting each interview, the interviewee was asked if the research concept was clear, to ensure that a general understanding of the proposed model was obtained.

In order to compare the differences or similarities in experts' opinions regarding same question, each question posed to the participants is analysed and discussed. Therefore, this way was very beneficial to gain more comprehensive analysing and discussing on each question in individual manner. In the next sections feedback of each expert is analysed, and general conclusions were made based on each expert point of view.

7.5.1 Validity of the Research Problem

The main aim of this part of the evaluation was to investigate how the identified research problem was seen by the experts. In general, all the interviewed academics and practitioners agreed that the research problem undertaken was valid, as well as they strongly believed that it is still open issue.

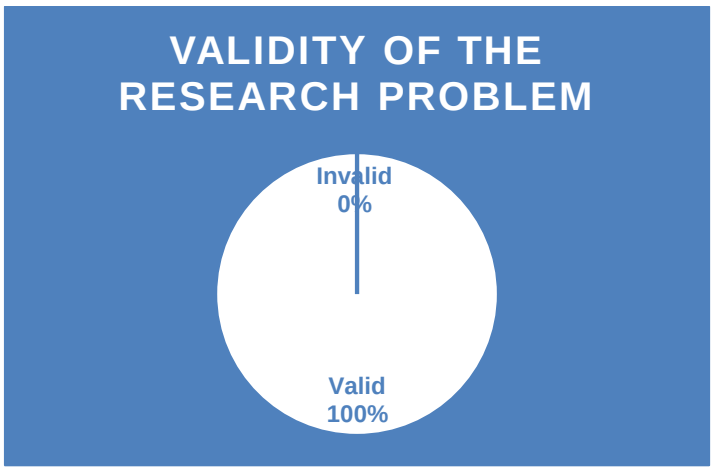


Figure 7.1 Experts' feedback on the validity of the research problem

- Academics

  The research problem was considered as valid by A1, and he said that '*'it is international problem; it is right over all in industries, in fact it is getting worst. So, I totally agree with you the problem that you have identified is a real problem that needs to be researched and solutions need to be devised for industry because industry has not got the answers to solve this problem so I totally concur with the problem statement as you got it''*. A2 shared this view, he thought that the research problem was relevant, it was very top, and it needs to be researched. In addition, A3 considered the problem identified with the users' compliance was quite realistic, and one of the common problems, which is how to measure an information security policy compliance. A4 supported this perspective; he mentioned that the questions raised are totally very interesting. He also indicated that it was very good to have this kind of

research, since users are one of the most important factors to guarantee the successful of an information security within an organization. A5's opinion was also on the same direction as the others, he agreed that the taken research problem was genuine, due to human aspect involved within this problem. A6 indicated that the problem of non-compliance is big and very important problem. He also mentioned, it is not being studied very much and it normally requires the use of psychologist in terms of behavior, knowledge and attitude. The last academic interviewed was A7, stated that it is a valid problem; many organizations are facing this problem of the noncompliant users. Moreover, he believes that the insider threat exists and needs more attention to be paid in finding effective solutions to mitigate it.

- Practitioners

  P1 had a strong belief that the research problem is common issue for every company and it is about user awareness in the end. Additionally, he sees the enforcement of such security policies as an effective solution towards mitigate this issue. P4 recognised the problem', saying security is a concern of all organizations in this era of rapid advancement in information technology. He added that the biggest challenge to implement those policies are: negligent, unaware or naïve behaviours of users. More supportive, P5 and P6 indicated that the way the research identified the problem domain was adequate and they believe that the research problem is still an open issue. In other words, they said it certainly exists because trying to identify patterns of behaviour and where to priorities attention and how to deal with it properly, it is certainly a challenge. P7 was of the same opinion of the others but with different wards, he said that the identified research problem is a serious gap in the security

framework and common weakness in many organizations and infrastructures, and find a solution for this problem will help an organization to raise the security awareness.

7.5.2 Feasibility at the operational level

The main aim behind this section is to analyse the experts' feedback regarding the realizability, attainability and feasibility of the proposed model at the operational level. The majority of the experts indicated that the proposed model is very feasible and attainable at the operational level. Some concerns regarding the proposed model were raised, which are the psychological factor that the model may have upon users, the ability for monitoring users' behaviours technically and the ethical issue of the behaviour monitoring. However, the great majority of the experts' responses to this question were affirmative.

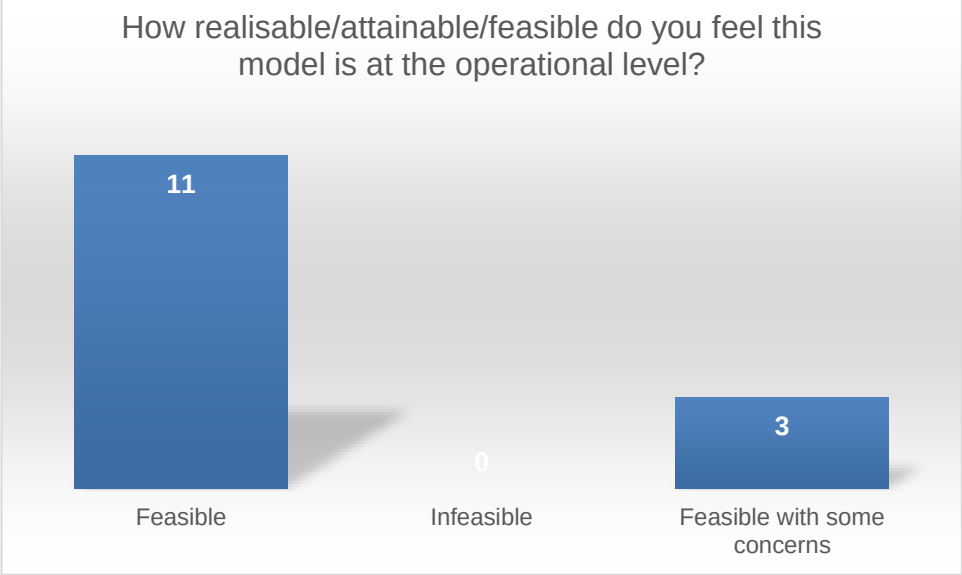


Figure 7.2: Experts' feedback on the feasibility at the operational level

- Academics

  A1 said that the research is on the right direction, but there are some ethical issues involved with the model, and that because of being the users are monitored, are they aware of that, is there a clear mechanism. He added that the ethical issue is a problem that needs to be addressed. He continues by saying that it is not that difficult to check

technical problems but for behavioural problems is not that easy to report that. A2's response was positive, stating that the used approach would be very feasible to be implemented in reality. However, his concern was about resources management or what he was calling resource intensive, which is how to manage a big amount of data. A3 believed that the proposed model will be very feasible depending on how many logs the model is able to process. He also suggested establishing a bridge between log analysis tools and the proposed approach in which the model is combined with some logs correlation systems, such as Logstash, Kibana and Elasticsearch. A4 shared the same opinion; saying is very applicable and very feasible to be applied in a real organisation. Also, he suggested that users need to be trained and informed that the proposed model is a tool that will help them in dealing better with the security policy, not for threatening them, nor as a penalty tool against them. A5 found himself not entirely sure how this is going to work, though he understood that it can be configured according to the need of a particular organisation and can be flexible. He also was of the belief that the model would be feasible for large organisations with adequate resources in place but it might be not feasible for a small or medium size enterprise. A7 thought that in somehow the proposed model is realisable, attainable and possible; such a system can be developed. However, A6 responded by saying that, an organisation may have some difficulties in implementing this system because users do not like been monitored or compared against others.

- Practitioners

  P1 mentioned that the approach is feasible but the hardest part will be the reporting of non-compliance with the policies. P2 was convinced that it is very realisable and very feasible and the application in real word will be fantastic to be applied. He also added

that it would be a challenging to apply this model on a user based but if it is possible to take the result of the compliance status of group of users and then start looking at each group behaviour or compliance rate, it will be fantastic. P5 stated that the model will be viable depending on how the data is fed into the system and what kind of data is fed into the system. Moreover, he argued that users' privacy, and content monitoring poses a challenge may face the system implementation. P6 mentioned that it could be done, it can be tweak in terms of things what need to be recorded and what can be detect, so the principle is definitely doable, the details of what the model can record would be the challenge. P4 and P7 had the same opinion on the possibility of implementing such a system in a real environment. However, P3 held the contrary view that that in theory, it is an interesting model, in its own, it may be difficult to implement in practical sense due to two issues. Firstly, politics issue, it will be difficult to monitor all users within an organisation especially with users who have high positions in an organisation. Secondly, he said that all what we need is only enforcing the policies using technical solutions rather than character monitoring.

7.5.3 Thoughts on using the concept of response taxonomy for non-compliance behaviour

This question was designed to get feedback from the interviewed experts regarding utilising the concept of response taxonomy for non-compliance behaviour within the proposed model. As explained in previously chapters, the model has two categories of response for non-compliant behaviour: raising awareness of a security policy and enforcement of a security policy, and therefore, each category is composed of sub-responses, which are designed to increase severity levels in a gradual manner. The feedbacks of the experts on this concept were of the general opinion that it would make difference in changing users' behaviour towards compliance.

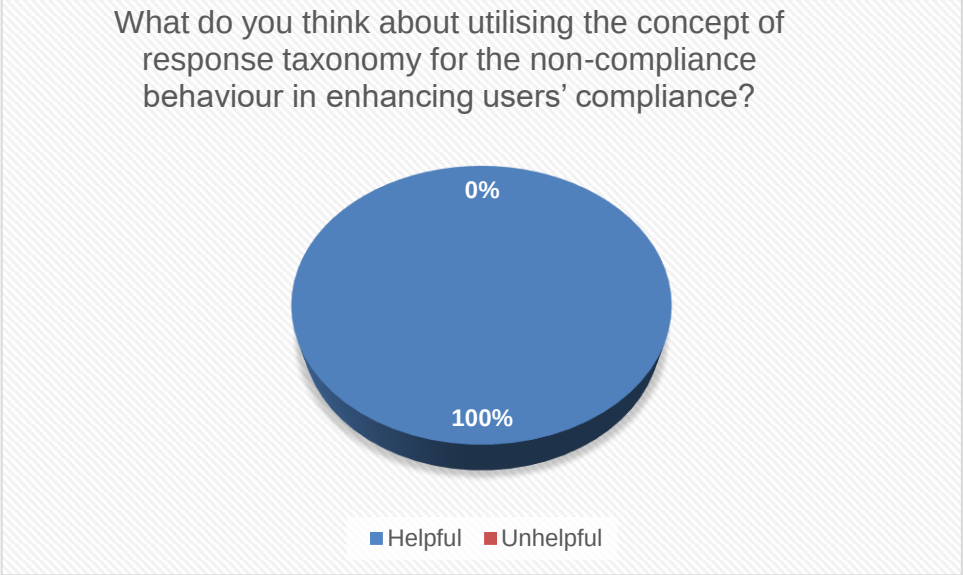


Figure 7.3: Experts' Thoughts on using the concept of response taxonomy for non-compliance behaviour

- Academics

  A1 stated that the response taxonomy for the non-compliance behaviour would be helpful in enhancing the overall compliance with information security policies. He added that there may be a psychological problem using this concept, since the users may feel very bad when they get notified that they made a mistake, so advice about how to phrase that response may be needed from psychologist people accordingly. A2 sees the approach of response taxonomy as an interesting way. A3 was very positive with the concept, saying it would be a good approach. He also mentioned that from his experience, the effects of this concept will be bigger and people will become more serious, when the response taxonomy comes to the advanced levels. A4, A5 were generally agreed on the concept of response taxonomy, A6 indicated that concept is fine if the proposed model could record or capture all users' behaviours. A7 thought that the approach is good and it can assist towards the behaviour change of non-compliance users.

- Practitioners

P1 simply agreed on the concept of the response taxonomy and he pointed out that it makes sense because it focuses on a targeted response based on certain behaviour of a user. This opinion also was supported by P2 and P5, he indicated that It seems very logical, very acceptable and it will drive users to comply. He also mentioned that the colours used within the response taxonomy will be challenging to some extent because users do not like the fact that they are being highlighted as red or yellow or any colour. In addition, he suggested that would be a better approach to link whatever they doing in terms of the policy violation to certain threats e.g. if a user is doing a certain behaviour like visiting bad website, there should be some sort of awareness message telling him if you do this you could compromise the whole organisation and it can be liked it certain threats. P3 was interested in the concept, saying ‘’I do like the idea of identifying behaviours’’. Further to this, he suggested that If the proposed model is also monitoring a behaviour of a computer identified, for example, does it have standard applications in store for whatever reason, patches missing and vulnerabilities are reported on that etc. P4 pointed out that this model can be used to create a fear of being noticed as a noncompliant user and being watched for any noncompliant, and therefore, this will encourage users to be more vigilant in terms of security policies and move from being noncompliant to compliance. P6 though was that it is a good one, using the time dimensions or time element on it was a great idea and it makes complete sense. P7 was of the same opinion, saying, the current actions and response levels are good and will raise awareness of the non-compliant users. However, his suggestion was to add training or quiz as one of the response taxonomy. He gave an example, when a user violates a password policy by choosing a simple password, such as 123456, the response taxonomy system will require this user to complete an online training about the password policy.

7.5.4 Thoughts on using the concept of compliance points system

In this section, the posed question aimed at discovering opinions of the interviewed experts in related to utilizing the concept of compliance points system within the proposed model. To what extent this concept may help organisations towards enhancing the compliance levels and gaining insight on users' behaviour and the implemented information security policies. Experts were of the general opinion that the proposed concept would be very beneficial.

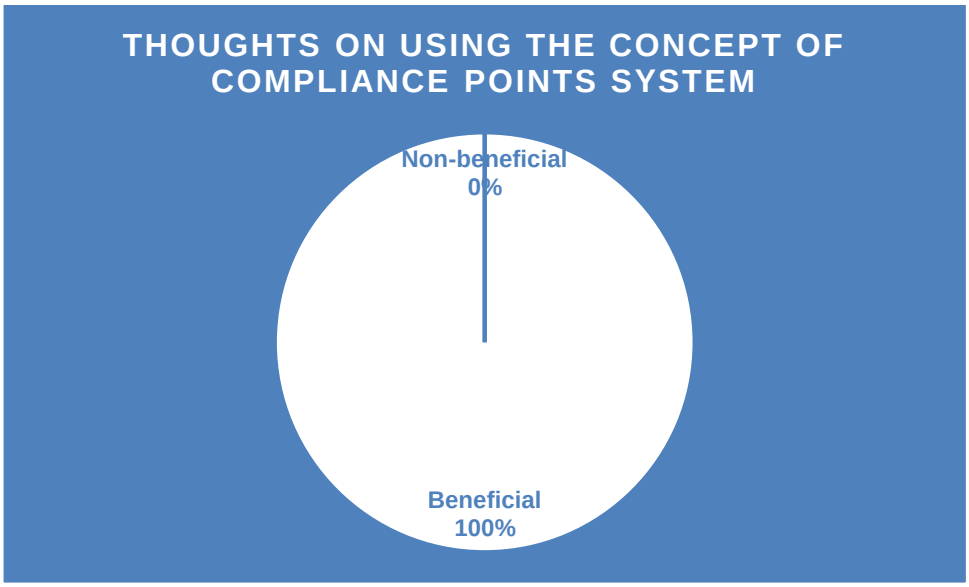


Figure 7.4: Experts' thoughts on using the concept of compliance points system

- Academics

  A1 though the concept of using the compliance points system was a good idea. He also mentioned that from an employer point of view there is a lot of advantages, but from a user point of view it could be problematic if he/she knows being monitored all the time so it depends on how the model advertise and make publicly the assessment. A2 said '' *I think this a good novel aspect in the sense that you mentioned that you mention that it was used in marketing, I do think there is merit in using points system''*. He also indicated that he knows similar points' concept, and it is used in his university for individuals' performance agreements and it affects performance from management perspective. A3 also supported the idea, and his advice for a further

enhancement was to use ISO 27001, appendix A, it would be very helpful if there is a mapping between violations and the ISO 27001 domains. A4 was totally agreed with the concept, and he suggested using zero and positive marks, not negative marks. In other words, he suggested using a threshold for the compliance points, for example, the weak user will take low positive mark and the good one high positive mark, for the organisation number one is negative but the user will not see the negative mark, in order to consider the psychological factor. A5 mentioned that it makes a lot of sense and some graphs are well presented in MATLAB. A6 said that the concept is fine if the model could record or capture all behaviours. Furthermore, his concern was about an ethical issue with the monitoring process. A7 was on the same direction of accepting the compliance points' concept, saying it is a useful approach.

- Practitioners

  P2 indicated that it is a fantastic system and will provide so much value for group HR for executive level on to what extent each department, each group or each section is complying to the information security policies. P4 said that this model can be used to create a fear of being noticed as a noncompliant user and being watched for any noncompliant. He also added this concept will encourage users to be more vigilant in terms of security policies and move from being noncompliant to compliance. P1, P5 and P7 viewed the concept as an interested approach. P5 liked the idea of presenting the compliance points trends over time and see both individuals and aggregate level pictures of how people are complying, he thought that it was a useful metric.

  However, just one expert believed the opposite, P3 stated that it may be difficult to implement because people may not like the points scoring and they view it in different ways and they can view it very negative.

7.5.5 Possibility Implementation of the proposed model

This question was designed to investigate to what extent the proposed model can be implemented from the interviewed experts' point of view. The experts were of the belief that it would be possible to deploy such a system.

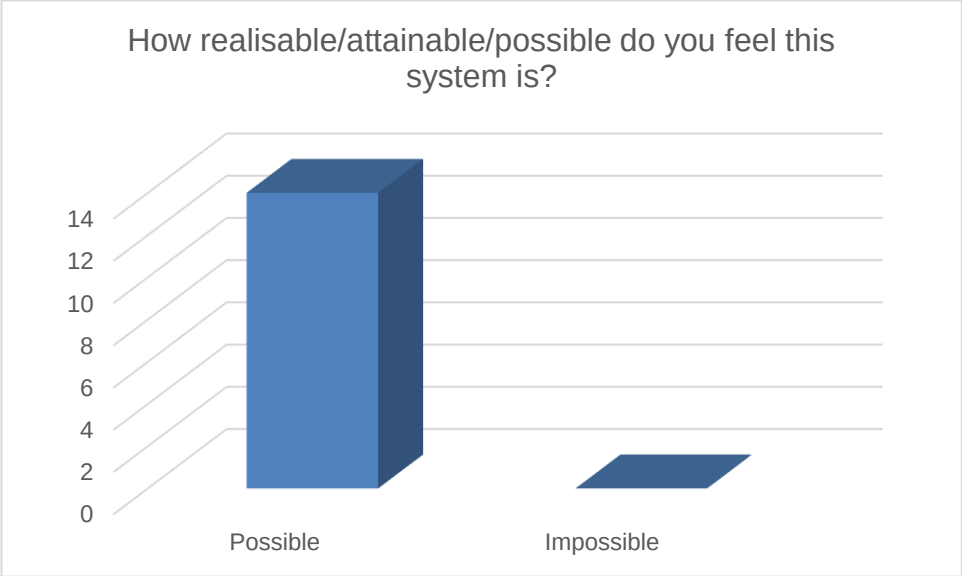


Figure 7.5: Experts' thoughts on the possibility implementation of the proposed model

- Academics

  A1 stated that the model can be implemented based on the extent to which it will be possible to capture and assess behavioural actions. A2 indicated that the concept is doable. This was supported by A3, he thought that it is very feasible, because nowadays compliance issues are raising and companies are searching for new solutions to measure it. A4 shared this view, said it is realisable and it has started logic of mapping the security policy on something more technical. A5 and A6 mentioned that it is theoretically feasible but it all down to the configuration in an organisation. A7 mentioned that it is feasible and such a system can be developed.

- Practitioners

P1, P2, P6 and P7 indicated that the model would be very possible to be implemented. P3 stated that theoretically it will be feasible but there may be a cost to pay for IT services. P4 stated that how feasible a system will be for an organization will depend on a number of things: 1) Organizational policies on monitoring user activates. 2) Determining cost of investment & its return. 3) Life cycle of the system. P5 thought it is viable and what he liked about the system form an operation point of view and a research point of view is that the model has basis to visualise data and results about users and security policies.

7.5.6 Thoughts on the simulation tool (the prototype system)

This section analyses feedback as regards the usefulness of the simulation tool, which used to give visualisation on the proposed model and its concept. The interviewed experts were asked to what extent they feel the simulation tool have provided a robust validation of the approach. Experts interviewed were of the general opinion that the prototype system was beneficial enough to visualise the main concept of the proposed model.

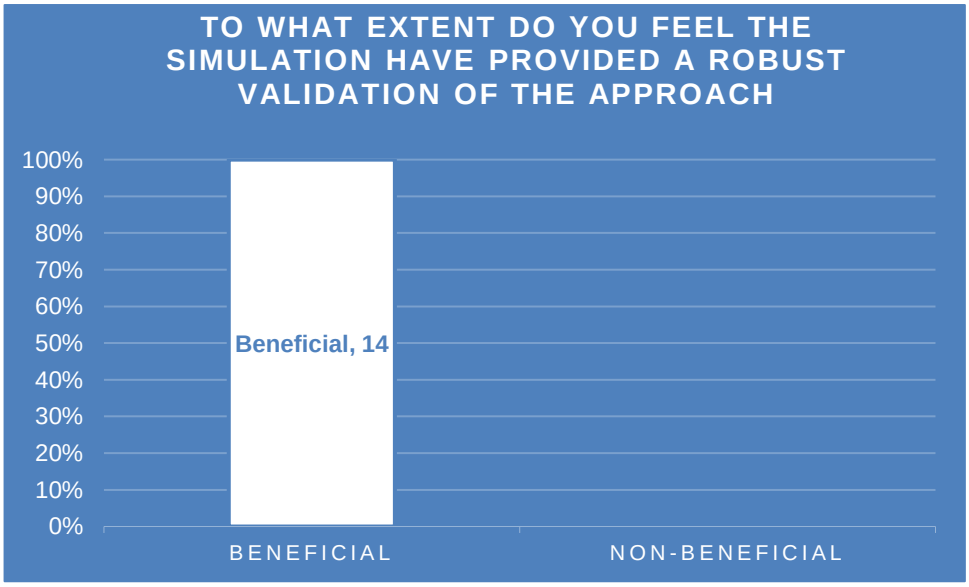


Figure 7.6: Experts' thoughts on the simulation tool (the prototype system)

- Academics

  A1 and A2 were in complete agreement that the prototype system was a validation of the model, and it works. A3 and A4 indicated that the simulation was clear and useful, but the used data was not taken from a real data so that is considered as a limitation of the simulation. However, A7 said, experts advise us to use real data but sometimes is not possible to use a real data so a simulation approach can help in this situation. A5 said that the simulation did a good job in descripting the model and giving an idea about how it is work in realty. A6 mentioned that the simulation did well and the picture was clear by the prototype system. He also added that the tool has visualised the research concept.

- Practitioners

  P1 and P7 indicated that the simulation was okay, very practical and very clear. P2 said it is very robust and it shows clearly what the compliance system will look like. He also added that it might need some enhancement in terms of the interface if this product will be some sort of production somewhat in future. P3 found the concept is very impressive and the work that put in is very palatable. P4 mentioned that the simulation provided a good overall approach, explaining different aspects of security monitoring and auditing alongside a mechanism of incentivising users to be more compliant. P5 and P6 indicated that it was good it adds sense, but they asked for more scenarios to be used with the simulation process.

7.5.7 Usefulness of the proposed model

It is vital to investigate the benefits that an organisation may gain by implementing the proposed model. The interviewees generally agreed that the model would be beneficial to organisations.

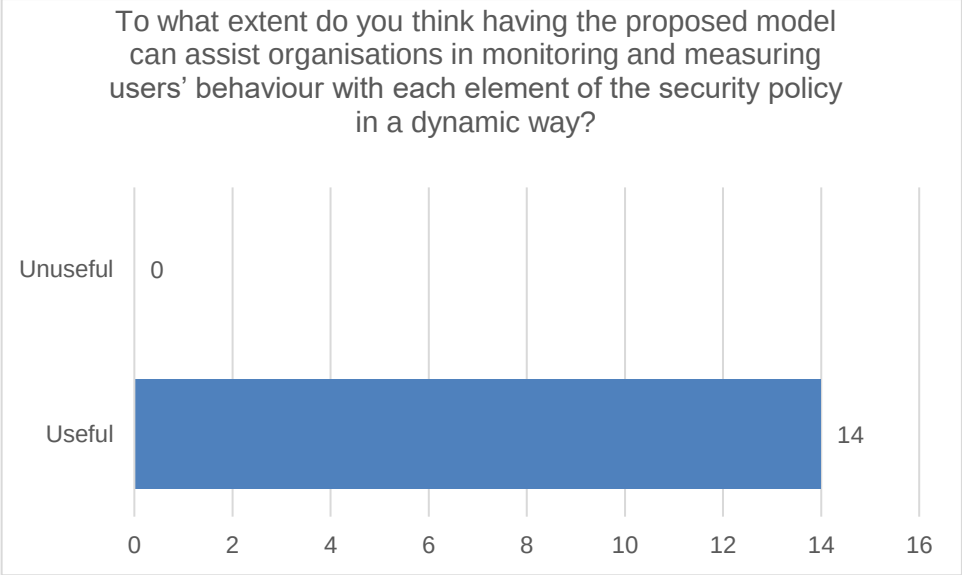


Figure 7.7: Experts' thoughts on usefulness of the proposed model

- Academics

  A1 said that it seems movements in the right direction but it should be accepted by the users and not seen as invasive. A3 mentioned that the model would be quite powerful tool, if it can somehow couple it the existing tools, such as security information and events management systems and somehow establish to bridge. A2, A4, A5 and A7 believed that the there is a lot of value in the proposed model. A6 indicated that it will be useful for an organisation, but users may do not like been monitored or compared.

- Practitioners

  P2 simply agreed and stated that it is very useful; it would be a good idea if the author proposes this model to security venders. P3 mentioned that it does monitor the compliance in a very efficient but need to consider other factors that may affect users' behaviour. P4 said that he is sure that the proposed model can help organisations performing regular audits on its security policies. P1 and P5 indicated that is quite good. P6 said '' *Your system model approach gives individuals reporting you can set metric on those and you can get exception reports out of it if trends going on wrong direction you can drilling to that to get down into individuals and you can measure*

the successive targeted action on trends over times, yah it looks like a good approach to do that''. P7 agreed that this model will help the administrator by saving the time and focus only on security policies that have noncompliant behaviours.

7.5.8 Discussion

This section analyses feedback from the interviewed experts regarding the proposed model strengths and weaknesses. The experts were of the general opinion that the model addresses a problem and contribute a new knowledge to the information security policy domain.

In answer to this question, A1 and A5 found the strength of the model to be that employers will have more proof and assurance that their users are following policies, adds a lot of value on this issue. A2 and P1 had the same opinion, the organisations will be able to drill down to individual aspect within a security policy and could have an employee in front of the security officer and look at a specific aspect and see if they comply or not. A3's opinion was that the strength of the model would be very easy to use. A4 and P5 believed the strength of the approach to be the manner it attempted to map between the security policies and users' behaviour, understanding how where enforcing the security policy and having an online tool in real time basis to monitor the users and identify which is their weaknesses is very important. A5 and P3 mentioned that the model is aware that human behaviour is key, and it covers a very important problem and having a solution for it. A7 was of opinion that it presented an approach that can measure users' compliance and can give them points. P2 indicated that this system can be developed to measure group to group or department to department performance in terms of information security policy compliance. He added that it would provide huge and effective type of output and results to highlights where the areas or departments that need more focus are or more enhancement, more security awareness, more security training, more attention from the information security side. P4 meanwhile thought

the strength of the approach was, the system provides an in-depth data for analysis, which can certainly point out the potential security holes with in an organization at user level. P6 believes that the positive issue was the using of targeted response for users' behaviours, which is the response taxonomy concept within the model.

As regards weaknesses, the concern of ethical and psychological issues regarding monitoring users' behaviours was raised by A1 and A4. Furthermore, A3 thought that the used data to run the model was not real data. A7 mentioned that some of security policies may difficult to measure or to get input about users' behaviours. P3 argued that in realty monitoring all users maybe challenging because people should be treated differently depending on their rule in the organisation, politicians, e.g. senior managers they should have to get special treatment. P4 highlighted that there is a potential impact of the system on the overall performance of the organizational infrastructure. P3 believed that if the system relies on humans inputting information into the system about compliance or not then it got potential weakness in that part.

7.6 Conclusion

After designing the proposed model and simulating it using the prototype system, it was significant to evaluate the model by interviewing different experts with different backgrounds from academic and industry sectors. All the interviewed people are considered as experts in the study domain and the research matter. For purpose of interviewing them, the selected questions were designed to holistically cover the main areas of this research including, usefulness, feasibility, technical capabilities, strength and limitations.

To summarise, the interviewed experts agreed that the identified research problem is a real problem that needs to be researched and solutions need to be devised. Furthermore, it can be stated that the overall feedback of the interviewed experts about the proposed model was very

encouraging and positive. The expert participants thought that the proposed model addresses the research gap, and offers a novel approach for the management of information security policies. The majority of participants are of the opinion that the using of response taxonomy for non-compliance behaviour and the concept of compliance points system will encourage users towards the compliance behaviour. In addition, they are very interested with the simulation tool and believe that it played a significant role in descripting the model and giving idea about how it works, if it deploys in a real environment.

However, it was found that despite the satisfactory experts' feedback, some experts raised some issues that need to be considered. The ethical or privacy of users during the monitoring process should be taken in to account. Moreover, the psychological aspect should be considered within the proposed model and therefore the users should consider system as a security tool that will help them and their organisations, not as a punishment tool against users. Another limitation was found over the evaluation process, which is using simulated data to run the prototype system. Furthermore, there was a concern regarding, cost, resources usage, and the ability of monitoring some behaviours.

The future research can focus upon some areas of the proposed model that may require further research. This study would be extended further based on the experts' feedback and the shortcomings that need to be enhanced, in order improve the overall performance of the proposed model.

Chapter Eight

Conclusions and Future Work

8. Conclusion & Future Work

8.1 Introduction

After designing, simulating and evaluating the proposed model, this chapter concludes the work performed during this thesis by providing a general overview of the study. It also highlights the achievements of the research and discusses the limitations of the research along with several potential future works.

The main objective of this research was to define and propose an advanced model or approach that able to provide a comprehensive framework for raising the level of compliance amongst end-users, with the aim of monitoring, measuring and responding to users' behaviour with an information security policy. The proposed approach is based on two main concepts: taxonomy of the response strategy to non-compliance behaviour, and a compliance points system. The response taxonomy is comprised of two categories: awareness raising and enforcement of the security policy. The compliance points system is used to reward compliant behaviour, and penalise noncompliant behaviour.

This objective was achieved by investigating the current stat of the art to define the gap as regards the information security policies and users' behaviours, by carefully reviewing the possible and most appropriate approaches to tackle the problem. Thus, a comprehensive model was designed and a prototype system developed to simulate the proposed model using different scenarios to validate the defined concept, as well the proposed model and its prototype system were evaluated by experts within the research domain.

8.2 Achievements of Research

Overall, the research aims were achieved through meeting the following objectives, which were initially set in Chapter 1:

Objective 1: To develop an awareness of state-of-the-art information security policies, including the problems associated with these policies and the available solutions.

Chapter 2 has described state-of-the-art information security policies with the aim of developing a thorough understanding of them. Types of information security policies and types of information security policy users are both discussed. It gave a close look at the current extent of use of information security policies by organisations. Furthermore, approaches used in policy enforcement and monitoring are covered by this chapter. In addition, it provided an overview of some of the current key issues and challenges related to information security policies.

Objective 2: From previous literature understand the issues that surround effective information security awareness.

Chapter 3 has presented a review of the literature on information security awareness. It also provided an overview of the current methods used to raise information security awareness, discussing both their advantages and disadvantages. This chapter concluded by outlining persuasive technology and its great value in the information security awareness area. Moreover, the problem of one size fit all is the current used approach and need to be solved.

Objective 3: Reviewing the potential behaviours of users with an information security policy as well as factors that influence their behaviours.

Chapter 4 has discussed the users' behaviours in relation to information security policy, presenting all the significant behaviours. It also addressed insider threats in more detail in order to gain a thorough understanding of this term. Lastly, the chapter explained the factors that influence user behaviour that is either compliant or non-compliant with such information security policies.

Objective 4: Proposing a novel model that aims at enhancing the compliance level of users based on two main concepts: taxonomy of the response strategy to non-compliance behaviour, and utilizing the compliance points system

Chapter 5 has proposed a novel model, which aims at increasing the compliance level of a user by monitoring and measuring their behaviour. The model is intended to provide a comprehensive framework for raising the level of compliance amongst end-users, with aims of monitoring, measuring and responding to users' behaviour with an information security policy. The novelty of the proposed model depends upon three significant aspects: monitoring, response taxonomy and using a compliance points system. These aspects are utilised to enhance the awareness and compliance of end-users.

Objective 5: Developing a prototype system to simulate the proposed model using several scenarios.

In chapter 6, a practical implementation of the prototype system was designed and developed based upon the proposed model. MATLAB environment was selected to develop the prototype system, a simulation based approach was used as an input data in order to run and demonstrate the prototype functionalities. Therefore, five scenarios of some of the potential behaviours of users have been created in which they are used to run the prototype system. A wide variety of results and charts were obtained from the prototype system regarding the five scenarios. The simulation was useful in demonstrating how the processes for the model might be in the future or the real environment.

Objective 6: Conducting a series of expert-based evaluations involving experts from different backgrounds, academic and industry.

An evaluation for the entire research and for the proposed model is presented in chapter 7. The expert participants were 14 people, academics and practitioners, have taken part in this evaluation. The overall feedback of the interviewed experts about the research, as a whole and the proposed model, was very encouraging and positive. In addition, the strengths and limitations of the proposed model were recognised and flagged for further research work.

8.3 Limitations of Research

Although the achievements of the research programme, there are some areas that need to be considered. The key limitations of the research are briefly listed below.

1. Considering the research nature, implementing the proposed model in a real environment was challenging, due to the fact that this research was conducted by an individual PhD researcher limited by certain resources and timeframe. Therefore, implementing and evaluating the proposed model in practical sense can give better understanding the effectiveness of it.
2. The psychological factor was out of the research scope. The proposed model may have some psychological impacts upon users therefore this issue need to be considered by studying the potential impacts and the best solutions.
3. Behaviours of users with some information security policies may be difficult to be monitored electronically and therefore these behaviours are reported manually, for example security officer or managers can report violations as a manual input.
4. A default setting for the response taxonomy for the non-compliance behaviours is five levels of responses, in which the severity of the response to any violation is escalated from Level 1 to Level 5. However, organisations can customize these levels of responses to the number that suits their individual needs. To determine the appropriate number of responses, the system need to be implemented in an organisation for a

certain period of time in order to decide the most suitable number of responses based on how the users behave with these responses.

Despite the limitations mentioned above, the work still considered valid as illustrated previously in the experts' evaluation feedback.

8.4 Future research

The main achievements and limitations of the research have been mentioned in the previous sections. And as any research, there are several opportunities that need further research and improvements. These suggestions are outlined below:

1. A complete version of the prototype system need to be developed based on the proposed model and implemented in a real environment within an organisation. This will be beneficial in order to understand the effectiveness of such a system in encouraging users to be compliant with the information security policies. Moreover, making the system working in a live environment will facilitate evaluating the system and finding any limitations.
2. Identifying any psychological impacts on users when the concept of compliance points system is applied in an organisation. And if there is an impact, determine the best solutions to mitigate that impact, such as considering motivational and persuasion factors.
3. Further investigation into the response taxonomy for the non-compliance behaviours; determine the best response strategy to the non-compliance behaviours. During this study five levels of responses have been suggested in order to explain the proposed model functionalities. However, further research is needed to gain insight into the best responses types and the number of these responses to be used within the proposed model.

8.5 The importance of information security compliance

Users being compliant with the information security policies of their organisation is the key to strengthen information asset security (Yazdanmehr & Wang 2015). Therefore, when employees have a good compliance level with security policies, this positively affects the overall security of an organization. However, employees' compliance with information security policies is still of great concern to many organizations (Hwang et al. 2017). And as reported in the literature, the effectiveness of such information security policies is still threatened by user non-compliance, due to malicious behaviour, negligent behaviour or unaware behaviour.

Thus, it is important to investigate the ability to encourage users to comply with their information security policies by implementing some important factors, such as monitoring, persuasion, awareness and enforcement, together in one framework. As such, dynamic response to users' behaviour may be an effective solution towards raising compliance levels. The main objective of the proposed model is the individualisation and personalisation of the response. There are targeted responses for each employee when non-compliance behaviour has occurred. Each user is given a targeted response, such as raising security awareness, based on their behaviour events and the response type focuses on the element of the policy that they have violated. The use of persuasive technology in motivating behavioural change has recently gained the attention of many researchers as a useful approach to promoting change. It is now being applied in many domains, such as marketing, health and psychology. Motivation and deterrents are examples of persuasive techniques, such as rewards and sanctions as motivation and deterrence, respectively. As such, a scoring points system (or compliance points system) is used to reward or punish users to motivate or deter them.

There are two main reasons why the proposed work in this study is deemed necessary and worthwhile. Firstly, no studies have been known to address targeted and on-going compliance raising with regard to security policy. Secondly, while theoretical research has investigated factors affecting employee behaviour in relation to compliance with information security, none has employed these factors in an integrated framework. From the perspective of the author, the proposed model can assist an organisation to gain insight into two different aspects regarding the security policy itself and the user behaviour.

References

References

Abawajy, J., 2014. User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, 33(June 2015), pp.236–247. Available at: 10.1080/0144929X.2012.708787%5Cnhttp://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=94615346&site=ehost-live&scope=site&authtype=shib&custid=s8000044.

Al-Omari, A., El-Gayar, O. & Deokar, A., 2011. Security policy compliance: User acceptance perspective. In *Proceedings of the Annual Hawaii International Conference on System Sciences*. pp. 3317–3326.

Alfawaz, S., Nelson, K. & Mohannak, K., 2010. Information security culture: A behaviour compliance conceptual framework. In *Conferences in Research and Practice in Information Technology Series*. pp. 47–55.

AlgoSec, 2013. *The State of Network Security 2013 : Attitudes and Opinions An AlgoSec Survey The State of IT Security*, Available at: http://www.algosec.com/resources/files/Specials/Survey files/State of Network Security 2013_Final Report.pdf.

Anon, 2009. Common sense guide to prevention and detection of insider threats 3rd edition–version 3.1. In *Published by CERT*. pp. 1–88.

Badie, N. & Lashkari, A.H., 2012. A new Evaluation Criteria for Effective Security Awareness in Computer Risk Management based on AHP. In pp. 9331–9347.

Bashorun, A., Woewui, A. & Parker, D., 2013. Information security: To determine its level of awareness in an organization. In *In 2013 7th International Conference on Application of Information and Communication Technologies*. Ieee, pp. 1–5. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6722704.

Baskerville, R. & Siponen, M., 2002. An information security meta-policy for emergent organizations. *Logistics Information Management*, 15(5/6), pp.337–346.

Bauer, S., Bernroider, E. & Chudzikowski, K., 2013. End User Information Security Awareness Programs for Improving Information Security in Banking Organizations: Preliminary Results from an Exploratory Study. *Proceedings of the Eighth Pre-ICIS Workshop on Information Security and Privacy*, pp.1–16.

Bowen, B.M. et al., 2009. Baiting inside attackers using decoy documents. In *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering*. pp. 51–70.

Bowen, P., Hash, J. & Wilson, M., 2006. *NIST Special Publication 800-100 - Information Security Handbook: A Guide for Managers*,

Bulgurcu, B., Cavusoglu, H. & Benbasat, I., 2009. Effects of individual and organization based beliefs and the moderating role of work experience on insiders' good security behaviors. *Proceedings - 12th IEEE International Conference on Computational Science and Engineering, CSE 2009*, 3, pp.476–481.

Bulgurcu, B., Cavusoglu, H. & Benbasat, I., 2010. Information Security Policy Compliance: An Empiracal Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly*, 34(3), pp.523–548.

Bullee, J.W.H. et al., 2015. The persuasion and security awareness experiment: reducing the success of social engineering attacks. *Journal of Experimental Criminology*, 11(1), pp.97–115.

Busch, M. et al., 2016. Persuasive information security: Techniques to help employees protect organizational information security. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 9638, pp.339–351.

CERT® Division, 2013. Unintentional Insider Threats : A Foundational Study. , (August), p.91. Available at: www.sei.cmu.edu.

Chan, H. & Mubarak, S., 2012. Significance of Information Security Awareness in the Higher Education Sector. *International Journal of Computer Applications*, 60(10), pp.23–31.

Chen, C.C., Medlin, B.D. & Shaw, R.S., 2008. A cross-cultural investigation of situational information security awareness programs. In *Information Management & Computer Security*. pp. 360–376.

Cheng, A. et al., 2014. Designing and Conducting Simulation-Based Research. *Pediatrics*, 133(6), pp.1091–1101.

Cheng, L. et al., 2013. Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers and Security*, 39(PART B), pp.447–459. Available at: http://dx.doi.org/10.1016/j.cose.2013.09.009.

Chuvakin, A., 2010. *The Complete Guide to Log and Event Management*, Available at: http://www.novell.com/docrep/2010/03/Log_Event_Mgmt_WP_DrAntonChuvakin_March2010_Single_en.pdf.

Colwill, C., 2009. Human factors in information security: The insider threat – Who can you trust these days? In *Information Security Technical Report*. Elsevier Ltd, pp. 186–196. Available at: http://linkinghub.elsevier.com/retrieve/pii/S1363412710000051 [Accessed September 8, 2014].

Creswell, J.W., 2007. *QUALITATIVE INQUIRY & RESEARCH DESIGN Choosing Among Five Approaches* 2nd ed., CA: Thousand Oaks.

Crossler, R.E. et al., 2013. Future directions for behavioral information security research. In *Computers & Security*. Elsevier Ltd, pp. 90–101. Available at: http://linkinghub.elsevier.com/retrieve/pii/S0167404812001460 [Accessed July 11, 2014].

D'Arcy, J. & Hovav, A., 2007. Deterring internal information systems misuse. *Communications of the ACM*, 50(10), pp.113–117.

D'Arcy, J., Hovav, A. & Galletta, D., 2009a. User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. In *Information Systems Research*. pp. 79–98.

D'Arcy, J., Hovav, A. & Galletta, D., 2009b. User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, 20(1), pp.79–98.

Dang-Pham, D., Pittayachawan, S. & Bruno, V., 2014. Towards a complete understanding of information security misbehaviours: A proposal for future research with social network approach. *Proceedings of the 25th Australasian Conference on Information Systems, ACIS 2014*, (2012).

Disterer, G., 2013. ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*, 4, pp.92–100. Available at: 10.4236/jis.2013.42011%5Cnhttp://search.ebscohost.com/login.aspx?direct=true&db=i3h&AN=89254050&site=ehost-live.

Dooley, K., 2002. Simulation research methods. In " Companion to Organizations, Joel Baum (ed.), pp. 829–848.

Door, B. & Valentine, D.T., 2016. *Essential MATLAB for engineers and scientists* 6th ed., Todd Green.

Economist Intelligence Unit EIU, 2009a. *Managing virtual teams Taking a more strategic approach*,

Economist Intelligence Unit EIU, 2009b. *Power to the people? Managing technology democracy in the workplace*, Available at: http://graphics.eiu.com/marketing/pdf/Technology Democracy.pdf.

Elmrabit, N., Yang, S.H. & Yang, L., 2015. Insider threats in information security categories and approaches. In *2015 21st International Conference on Automation and Computing: Automation, Computing and Manufacturing for New Economic Growth, ICAC 2015*.

Endsley, M., 1995. A taxonomy of situation awareness errors. *Human factors in aviation operations*, pp.287–292. Available at: http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:A+Taxonomy+of+Situation+Awareness+Errors#0 [Accessed January 19, 2015].

EU, 2009. *Power to the people? Managing technology democracy in the workplace*,

EY, 2016. *Managing insider threat A holistic approach to dealing with risk from within*, Available at: http://www.ey.com/Publication/vwLUAssets/EY-managing-inside-threat/$FILE/EY-managing-inside-threat.pdf.

Filkins, B. & Radcliff, D., 2008. *Data Leakage Landscape : Where Data Leaks and How Next Generation Tools Apply*, Available at: http://www.sans.org/reading-room/whitepapers/analyst/data-leakage-landscape-data-leaks-generation-tools-apply-34695.

Fogg, B., 2009. A behavior model for persuasive design. In *Proceedings of the 4th International Conference on Persuasive Technology - Persuasive '09*. p. 1. Available at: http://portal.acm.org/citation.cfm?doid=1541948.1541999.

Fogg, B., 1998. Persuasive computers: perspectives and research directions. In *... the SIGCHI conference on Human factors in computing ...*. pp. 225–232. Available at: http://www.scopus.com/inward/record.url?eid=2-s2.0-

0031622928&partnerID=40&md5=def85e2425dac867d2d330b62b204ef9%5Cnhttp://dl.acm.org/citation.cfm?id=274677%5Cnhttp://dl.acm.org/citation.cfm?id=274677.

Furnell, S., 2006. Malicious or misinformed? Exploring a contributor to the insider threat. In *Computer Fraud and Security*. pp. 8–12.

Furnell, S. & Clarke, N., 2012. Power to the people? The evolving recognition of human aspects of security. In *Computers & Security*. Elsevier Ltd, pp. 983–988. Available at: http://linkinghub.elsevier.com/retrieve/pii/S0167404812001228 [Accessed October 19, 2014].

Furnell, S. & Thomson, K.-L., 2009. From culture to disobedience: Recognising the varying user acceptance of IT security. *Computer Fraud & Security*, 2009(2), pp.5–10. Available at: http://linkinghub.elsevier.com/retrieve/pii/S1361372309700193 [Accessed October 23, 2014].

Global consulting firm Protiviti, 2014. *Bridging the Data Security Chasm*, Available at: http://www.protiviti.com/en-US/Pages/IT-Security-and-Privacy-Survey.aspx.

Greene, G. & D Arcy, J., 2010. Assessing the Impact of Security Culture and the Employee-Organization Relationship on IS Security Compliance. In *5th Annual Symposium on Information Assurance*. pp. 1–8. Available at: http://www.albany.edu/wwwres/conf/iasymposium/proceedings/2010/ASIA10Proceedings.pdf#page=51.

Greitzer, F.L. et al., 2013. Psychosocial modeling of insider threat risk based on behavioral and word use Analysis1. In *E - Service Journal*. p. 106–138,141. Available at: http://www.jstor.org/journal/eservicej.

Greitzer, F.L. et al., 2014. Unintentional Insider Threat: Contributing Factors, Observables, and Mitigation Strategies. In *2014 47th Hawaii International Conference on System Sciences*. Ieee, pp. 2025–2034. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6758854 [Accessed December 21, 2014].

Guido, M.D. & Brooks, M.W., 2013. Insider threat program best practices. In *Proceedings of the Annual Hawaii International Conference on System Sciences*. pp. 1831–1839.

Haeussinger, F.J. & Kranz, J.J., 2013. Information Security Awareness: Its Antecedents and Mediating Effects on Security Compliant Behavior. *International Conference on Information Systems*, (August), pp.1–16.

Hanley, M. et al., 2011. An Analysis of Technical Observations in Insider Theft of Intellectual Property Cases.

Harris, M. & Furnell, S., 2012. Routes to security compliance: Be good or be shamed? *Computer Fraud and Security*, 2012(12), pp.12–20. Available at: http://dx.doi.org/10.1016/S1361-3723(12)70122-7.

Herath, T. & Rao, H.R., 2009. Protection Motivation and Deterrence: a Framework for Security Policy Compliance in Organisations. *European Journal of Information Systems*, 18(2), pp.106–125.

Huang, D.L. et al., 2011. Factors affecting perception of information security and their

impacts on IT adoption and security practices. In *International Journal of Human Computer Studies*. pp. 870–883.

Hwang, I. et al., 2017. Why not comply with information security? An empirical approach for the causes of non-compliance. *Online Information Review*, 41(1), p.null. Available at: http://www.emeraldinsight.com/doi/abs/10.1108/OIR-11-2015-0358.

ISACA, 2012. COBIT 5 Introduction. Available at: https://www.isaca.org/COBIT/Documents/An-Introduction.pdf.

ISO, 2013. *SO / I BSI Standards Publication nformati on technol ogy — Securi ty techni ques — nformati on securi ty management systems — Requi rements*,

Johnson, B. & Turner, L., 2003. *Data collection strategies in mixed methods research*,

Jones, A. & Colwill, C., 2008. Dealing with the Malicious Insider. In *Australian Information Security Management Conference*.

Khan, B. et al., 2011. Effectiveness of information security awareness methods based on psychological theories. In *African Journal of Business Management*. pp. 10862–10868. Available at: http://www.academicjournals.org/AJBM/abstracts/abstracts/abstracts2011/28Oct/Khan et al.htm [Accessed November 16, 2014].

Kirlappos, I., 2016. *Learning from" shadow security": understanding non-compliant behaviours to improve information security management*. University College London.

Kirlappos, I., Parkin, S. & Sasse, M.A., 2015. " Shadow Security " as a tool for the learning organization. In SIGCAS Computer & Society, pp. 29–37.

Kirlappos, I., Parkin, S. & Sasse, M.A., 2014. Learning from "Shadow Security" : Why understanding non-compliant behaviors provides the basis for effective security.

Kirlappos, I. & Sasse, M.A., 2014. What usable security really means: Trusting and engaging users. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 8533 LNCS, pp.69–78.

Knapp, K.J. et al., 2009. Information security policy: An organizational-level process model. In *Computers & Security*. pp. 493–508. Available at: http://www.sciencedirect.com/science/article/B6V8G-4WSHK03-2/2/65673d7d064cc45cd182b82622c6acda.

Knapp, K.J. et al., 2009. Information security policy: An organizational-level process model. In *Computers & Security*. Elsevier Ltd, pp. 493–508. Available at: http://linkinghub.elsevier.com/retrieve/pii/S0167404809000765 [Accessed September 9, 2014].

Koh, K. et al., 2005. Security Governance : Its Impact on Security Culture. In *Proceedings of The third Australian Information Security Management Conference*. pp. 1–12. Available at: http://igneous.scis.ecu.edu.au/proceedings/2005/aism/koh.pdf.

Kowaski, E., Cappelli, D. & Moore, A., 2008. *Insider Threats Study: Illicit Cyber activity in the Information Technology and Telecommunication Secror*, Mellon Universit.

Kraemer, S., Carayon, P. & Clem, J., 2009. Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computers and Security*, 28(7), pp.509–520. Available at: http://dx.doi.org/10.1016/j.cose.2009.04.006.

Kuzel, A.J., 1992. *Sampling in qualitative inquiry.*,

Magklaras, G.B. & Furnell, S.M., 2002. Insider threat prediction tool: Evaluating the probability of IT misuse. *Computers and Security*, 21(1), pp.62–73.

Mathew, S. et al., 2008. Insider abuse comprehension through capability acquisition graphs. In *Proceedings of the 11th International Conference on Information Fusion, FUSION 2008*.

MathWorks, 2016. Cross-correlation - MATLAB xcorr - MathWorks United Kingdom. Available at: https://uk.mathworks.com/products/matlab/ [Accessed November 27, 2016].

May, C., 2008. Approaches to user education. In *Network Security*. pp. 15–17.

Mcbride, M., Carter, L. & Warkentin, M., 2012. *Exploring the Role of Individual Employee Characteristics and Personality on Employee Compliance with Cybersecurity Policies 1*,

Mohamed, A., 2009. Security trends for 2009. Available at: http://www.computerweekly.com/feature/Security-trends-for-2009 [Accessed January 15, 2015].

Morse, J.M., 2000. Qualitative Health Research. *Qualitative Health Research*, 10(1), pp.3–5.

Munshi, A., Dell, P. & Armstrong, H., 2011. Insider threat behavior factors: A comparison of theory with reported incidents. In *Proceedings of the Annual Hawaii International Conference on System Sciences*. pp. 2402–2411.

Northcutt, S., 2014. MGT438: How to Establish a Security Awareness Program. *SANS*. Available at: http://www.sans.org/ course/establish-security-awarenessprogram [Accessed June 6, 2015].

Nostro, N. et al., 2014. Insider threat assessment: A model-based methodology. *Operating Systems Review (ACM)*, 48(2), pp.3–12.

Pahnila, S. et al., 2007. Employees ' Behavior towar ds IS Secur ity Policy Compliance University of Oulu , Department of Information Processing. *October*, pp.1–10.

Park, J.S. & Giordano, J., 2006. Role-based profile analysis for scalable and accurate insider-anomaly detection. In *Conference Proceedings of the IEEE International Performance, Computing, and Communications Conference*. pp. 463–469.

Parsons, K.,McCormac, A.,Pattinson, M., Butavicius, M. & Jerram, C., 2014. A study of information security awareness in Australian government organisations. *Information Management & Computer Security*, 22(4), pp.334–345. Available at: http://www.emeraldinsight.com/doi/abs/10.1108/IMCS-10-2013-0078.

Parsons, K. et al., 2010. Human Factors and Information Security : Individual , Culture and Security Environment. In *Science And Technology*. p. 45. Available at: http://www.dtic.mil/dtic/tr/fulltext/u2/a535944.pdf.

Peltier, T.R., 2005. Implementing an Information Security Awareness Program. In *Edpacs*. pp. 1–18.

Peltier, T.R., 2001. *Information security policies, procedures, and standards: Guidelines for effective information security management*,

PriceWaterhouseCoopers PwC, 2015. *2015 INFORMATION SECURITY*, Available at: http://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-03.pdf.

PriceWaterhouseCoopers PwC, 2014. *INFORMATION SECURITY BREACHES SURVEY 2014*, Available at: https://www.pwc.co.uk/assets/pdf/cyber-security-2014-technical-report.pdf.

Prince, P., 2014. More Than Half of Enterprise Employees Receive No Security Training: Survey Finds. *security week*. Available at: http://www.securityweek.com/more-half-enterprise-employees-receive-no-security-training-survey-finds [Accessed May 1, 2015].

Proctor, R., 2006. *Sensation and perception* 3rd ed., John Wiley and Sons, New York. Available at: http://books.google.com/books?hl=en&lr=&id=2tW91BWeNq4C&oi=fnd&pg=PR23&dq=Sensation+and+Perception&ots=-S0vvB8_SR&sig=zhDe_f5Yl6UBdbWFMGoxD01a3WI.

Puhakainen, P. & Siponen, M., 2010. R ESEARCH A RTICLE I MPROVING E MPLOYEES ' C OMPLIANCE T HROUGH I NFORMATION S YSTEMS S ECURITY T RAINING : In pp. 757–778.

Qudaih, H. a et al., 2014. Security Awareness in an Organization. *Persuasive Technology Contributions Toward Enhance Information Security Awareness in an Organization*, 10(4), pp.180–186.

Richardson, R., 2009. *14th Annual CSI Computer Crime*, Available at: http://www.personal.utulsa.edu/~james-childress/cs5493/CSISurvey/CSISurvey2009.pdf.

Roy Sarkar, K., 2010. Assessing insider threats to information security using technical, behavioural and organisational measures. In *Information Security Technical Report*. Elsevier Ltd, pp. 112–133. Available at: http://dx.doi.org/10.1016/j.istr.2010.11.002.

SANS, 2014a. Information Security Policy Templates. Available at: http://www.sans.org/security-resources/policies/general [Accessed May 15, 2015].

SANS, 2014b. Information Security Policy Templates. Available at: https://www.sans.org/security-resources/policies/.

Sanzgiri, A. & Dasgupta, D., 2016. Classification of Insider Threat Detection Techniques. In *Proceedings of the 11th Annual Cyber and Information Security Research Conference on - CISRC '16*. pp. 1–4. Available at: http://dl.acm.org/citation.cfm?doid=2897795.2897799.

Saran, M. & Zavarsky, P., 2009. A Study of the Methods for Improving Internet Usage Policy Compliance. In *2009 International Conference on Computational Science and Engineering*. Ieee, pp. 371–378. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5283299 [Accessed October 24, 2014].

Shaw, E., Post, J. & Ruby, K., 1999. Insider the mind of insider. In *security management*.

Shaw, R.S.. et al., 2009. The impact of information richness on information security awareness training effectiveness. In *Computers and Education*. pp. 92–100. Available at: http://www.scopus.com/inward/record.url?eid=2-s2.0-56249140028&partnerID=40&md5=0629d34a2b68eef4bc1dc7f7548cd399.

Sheikhpour, R. & Modiri, N., 2012. A best practice approach for integration of ITIL and ISO/IEC 27001 services for information security management. *Indian Journal of Science and Technology Indian J.Sci.Technol*, 5(2), pp.2170–2176. Available at: http://www.indjst.org.

Sheng, S. et al., 2010. Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions. *Proceedings of the …*. Available at: http://dl.acm.org/citation.cfm?id=1753383 [Accessed January 18, 2015].

Shenk, J., 2012. *SANS Eighth Annual 2012 Log and Event Management Survey Results: Sorting Through the Noise*, Available at: http://www.sans.org/reading-room/whitepapers/analyst/eighth-annual-2012-log-event-management-survey-results-sorting-noise-35230.

Sherif, E., Furnell, S. & Clarke, N., 2016. Awareness, behaviour and culture: The ABC in cultivating security compliance. *2015 10th International Conference for Internet Technology and Secured Transactions, ICITST 2015*, pp.90–94.

Shropshire, J. et al., 2006. Personality and IT security: An application of the five-factor model. *Americas Conference on Information Systems*, pp.1–8. Available at: ftp://163.25.117.117/gyliao/PaperCollection/20100116/Personality and IT security- An application of the five-factor model.pdf.

Sikolia, D. et al., 2014. A Theory of Employee Compliance with Information Security. *Midwest Association for Information Systems 2014 Proceedings*. Available at: http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1021&context=mwais2014.

Silowash, G., Cappelli, D. & Moore, A., 2012. *Common Sense Guide to Mitigating Insider Threats 4th Edition*, Available at: http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA585500 [Accessed January 21, 2015].

Siponen, M., Adam Mahmood, M. & Pahnila, S., 2014. Employees' adherence to information security policies: An exploratory field study. *Information and Management*, 51(2), pp.217–224.

Siponen, M. & Vance, A., 2010. Neutralizaiton: New Insights into the Problem of Employee Information Systems Security. *MIS Quarterly*, 34(3), pp.487–502.

Sohrabi Safa, N., Von Solms, R. & Furnell, S., 2016. Information security policy compliance model in organizations. *Computers and Security*, 56, pp.1–13.

Soomro, Z.A., Shah, M.H. & Ahmed, J., 2016. Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, 36(2), pp.215–225.

Stahl, S. & Pease, K.A., 2011. *Seven Requirements for Successfully Implementing*

Information Security Policies and Standards,

Strohmeyer, R., 2011. How to Monitor Your Employees' PCs Without Going Too Far. Available at: http://www.pcworld.com/article/222169/how_to_monitor_your_employees_without_going_too_far.html [Accessed November 1, 2014].

Symantec Corporation, 2014. *Internet Security Threat Report*,

Talib, S., Clarke, N.L. & Furnell, S.M., 2010. An Analysis of Information Security Awareness within Home and Work Environments. *2010 International Conference on Availability, Reliability and Security*, pp.196–203. Available at: http://doi.ieeecomputersociety.org/10.1109/ARES.2010.27.

The European Network and Information Security Agency (ENISA), 2010. *The new users ' guide : How to raise information security awareness*,

Da Veiga, a. & Eloff, J.H.P., 2010. A framework and assessment instrument for information security culture. In *Computers & Security*. Elsevier Ltd, pp. 196–207. Available at: http://linkinghub.elsevier.com/retrieve/pii/S0167404809000923 [Accessed September 20, 2014].

Veiga, a Da & Eloff, J., 2009. A framework and assessment instrument for information security culture. In *Computers & Security*.

Vidyaraman, S., Chandrasekaran, M. & Upadhyaya, S., 2008. The User is not the enemy. Available at: http://www.nspw.org/papers/2007/nspw2007-vidyaraman.pdf.

Wilson, T., 2010. Why Employees Break Security Policy (And What You Can Do About It). Available at: http://www.darkreading.com/risk/why-employees-break-security-policy-(and-what-you-can-do-about-it)/d/d-id/1133433 [Accessed April 10, 2015].

Xue, Y., Liang, H. & Wu, L., 2011. Punishment, justice, and compliance in mandatory IT settings. In *Information Systems Research*. pp. 400–414.

Yayla, A., 2011. Controlling insider threats with information security policies. In *ECIS 2011 Proceedings. Paper 242*. Available at: http://aisel.aisnet.org/ecis2011/242/ [Accessed January 22, 2015].

Yazdanmehr, A. & Wang, J., 2015. Employees' information security policy compliance: A norm activation perspective. *Decision Support Systems*.

Yeo, A., Rahim, M. & Ren, Y., 2008. Use of Persuasive technology to change end user's IT security aware behavior: a pilot study. In *World Academy of Science, Engineering and Technology*. pp. 193–199. Available at: http://www.waset.org/publications/14957.

Appendices

Appendix A: Users Scenarios used within the prototype system.

Appendix B: Experts invitation letter & Ethical approvals

Appendix C: Experts' feedback

Appendix D: Published papers

Appendix A: Users Scenarios used within the prototype system.

Scenario 2: User B violations:

In this scenario, User B was created to simulate unaware behaviour. The violations log file of User B contains one violation of each policy element during the simulation period and this log file is used by the prototype system to simulate Unaware behaviour.

```
01-01-2015 09:00:00 1   User has not locked his PC
02-01-2015 09:30:02 2   Computer Workstations must be shut completely down at the
                        end of the work day
03-01-2015 10:00:00 3   User not keeeping storage device in a secure place
04-01-2015 11:30:40 4   User disabled anti-virus software
20-01-2015 12:00:00 5   Passwords left written down in an accessible location
28-03-2015 14:00:00 6   User has not changed his password
01-04-2015 13:00:00 7   password did not meet the password construction guidelines
01-04-2015 14:03:59 8   Passwords has been be added to or written in an email
                        message
01-04-2015 16:40:01 10 Undertaking deliberate activities that waste staff effort or
                         networked resources
02-04-2015 13:00:00 9  Users are not allowed to utilize password memorization
02-04-2015 13:30:00 20 User played games on the Internet
03-04-2015 17:00:00 17 Personal use of the Internet caused a significant increase
                        in resource demand
03-04-2015 17:00:41 15 Forwarding of company confidential messages to external
                        locations
29-06-2015 16:00:00 11 The organization's email account did not been fundamentally
                        utilized for business that is related to the orgnization
29-06-2015 16:30:00 14 Use the email systems in a way that could affect its
                        reliability or effectiveness, for example distributing chain
                        letters or spam
30-06-2015 08:30:00 19 Download copyrighted material such as music media (MP3)
                        files, film and video files without appropriate approval
30-06-2015 09:30:00 12 organization’s email system has been utilized to create or
                        distribute offensive or disruptive messages.
01-07-2015 11:00:00 18 Download software from the internet without prior approval
                        of the IT Department
01-07-2015 12:00:00 16 User has visited or view illegal materials on the Internet
21-07-2015 17:00:00 13 User has Sent unprotected sensitive or confidential
                        information
```

Scenario 2: User C violations:

In this scenario, User C was created to simulate a changeful behaviour. The violations log file of User C contains 5 or 6 violations with each policy element during the simulation period.

```
01-01-2015 09:00:02 2   Computer Workstations must be shut completely down at the
end of the work day
01-01-2015 10:00:00 3   User not keeeping storage device in a secure place
01-01-2015 11:30:40 4   User disabled anti-virus software
01-01-2015 12:00:00 5   Passwords left written down in an accessible location
01-01-2015 15:00:00 6   User has not changed his password
05-01-2015 14:00:00 7   password did not meet the password construction guidelines
20-01-2015 11:03:59 8   Passwords has been be added to or written in an email
                        message
20-01-2015 16:40:01 10 Undertaking deliberate activities that waste staff effort or
                        networked resources
21-01-2015 13:00:00 9   Users are not allowed to utilize password memorization
23-01-2015 13:00:00 4   User disabled anti-virus software
25-01-2015 13:00:00 17 Personal use of the Internet caused a significant increase
                        in resource demand
```

```
26-01-2015 17:00:00 15 Forwarding of company confidential messages to external
locations
27-01-2015 16:00:00 11 The organization's email account did not been fundamentally
                       utilized for business that is related to the orgnization
03-02-2015 12:00:00 16 User has visited or view illegal materials on the Internet
03-02-2015 14:00:00 16 User has visited or view illegal materials on the Internet
06-02-2015 11:00:00 18 Download software from the internet without prior approval
                       of the IT Department
07-02-2015 15:00:00 4   User disabled anti-virus software
09-02-2015 11:00:00 4   User disabled anti-virus software
09-02-2015 13:00:00 2   Computer Workstations must be shut completely down at the
                       end of the work day
11-02-2015 15:00:00 10 Undertaking deliberate activities that waste staff effort or
                       networked resources
23-02-2015 16:00:00 14 Use the email systems in a way that could affect its
                       reliability or effectiveness, for example distributing chain
                       letters or spame
28-02-2015 11:00:00 19 Download copyrighted material such as music media (MP3)
                       files, film and video files without appropriate approval
01-03-2015 17:00:00 11 The organization's email account did not been fundamentally
                       utilized for business that is related to the orgnization
05-03-2015 11:00:00 18 Download software from the internet without prior approval
                       of the IT Department
05-03-2015 17:00:00 18 Download software from the internet without prior approval
                       of the IT Department
07-03-2015 11:00:00 5   Passwords left written down in an accessible location
08-03-2015 13:00:00 20 User played games on the Internet
15-03-2015 11:00:00 13 User has Sent unprotected sensitive or confidential
                       information
16-03-2015 11:00:00 4   User disabled anti-virus software
17-03-2015 10:00:00 5   Passwords left written down in an accessible location
17-03-2015 12:00:00 16 User has visited or view illegal materials on the Internet
20-03-2015 11:00:00 3   User not keeeping storage device in a secure place
22-03-2015 16:00:00 18 Download software from the internet without prior approval
                       of the IT Department
23-03-2015 11:00:00 8   Passwords has been be added to or written in an email
                        message
24-03-2015 10:30:00 1   User has not locked his PC
29-03-2015 17:00:00 6   User has not changed his password
29-03-2015 18:00:00 7   password did not meet the password construction guidelines
29-03-2015 18:30:00 12 organization’s email system has been utilized to create or
                       distribute offensive or disruptive messages.
01-04-2015 08:00:00 20 User played games on the Internet
01-04-2015 10:00:00 13 User has Sent unprotected sensitive or confidential
                       information
01-04-2015 11:00:00 16 User has visited or view illegal materials on the Internet
01-04-2015 11:30:00 5   Passwords left written down in an accessible locatio
01-04-2015 12:00:00 8   Passwords has been be added to or written in an email
                        message
01-04-2015 13:00:00 4   User disabled anti-virus software
01-04-2015 15:00:00 3   User not keeeping storage device in a secure place
01-04-2015 16:00:00 2   Computer Workstations must be shut completely down at the
                        end of the work day
01-04-2015 17:00:00 11 The organization's email account did not fundamentally
                       utilize for business that is related to the orgnization
01-04-2015 17:30:00 18 Download software from the internet without prior approval
                       of the IT Department
10-04-2015 11:00:00 9   Users are not allowed to utilize password memorization
20-04-2015 11:00:00 15 Forwarding of company confidential messages to external
                       locations
27-04-2015 13:00:00 10 Undertaking deliberate activities that waste staff effort or
                       networked resource
02-05-2015 13:00:00 19 Download copyrighted material such as music media (MP3)
                       files, film and video files without appropriate approval
10-05-2015 15:00:00 1   User has not locked his PC
15-05-2015 12:00:00 14 Use the email systems in a way that could affect its
                       reliability or effectiveness, for example distributing chain
                       letters or spam
```

```
29-05-2015 16:00:00 6   User has not changed his password
10-06-2015 14:30:00 17 Personal use of the Internet caused a significant increase
                       in resource demand
17-06-2015 16:30:00 19 Download copyrighted material such as music media (MP3)
                       files, film and video files without appropriate approval
24-06-2015 15:30:00 12 organization’s email system has been utilized to create or
                       distribute offensive or disruptive messages
30-06-2015 08:30:00 1   User has not locked his PC
30-06-2015 09:30:00 6   User has not changed his password
30-06-2015 10:30:00 7   password did not meet the password construction
30-06-2015 12:30:00 10 undertaking deliberate activities that waste staff effort or
                        networked resource
30-06-2015 13:30:00 9   Users are not allowed to utilize password memorization
30-06-2015 13:30:00 12 organization’s email system has been utilized to create or
                       distribute offensive or disruptive messages
30-06-2015 15:00:00 14 Use the email systems in a way that could affect its
                       reliability or effectiveness, for example distributing chain
                       letters or spam
30-06-2015 16:00:00 15 Forwarding of company confidential messages to external
                       locations
30-06-2015 16:40:00 17 Personal use of the Internet caused a significant increase
                       in resource demand
30-06-2015 17:00:00 19 Download copyrighted material such as music media (MP3)
                       files, film and video files without appropriate approva
20-06-2017 11:30:40 4   User disabled anti-virus software
22-06-2017 16:00:00 6   User has not changed his password
22-06-2017 17:30:00 12 organization’s email system has been utilized to create or
                       distribute offensive or disruptive messages
23-06-2017 09:00:02 2   Computer Workstations must be shut completely down at the
                        end of the work day
24-06-2017 15:00:00 3   User not keeeping storage device in a secure place
27-06-2017 12:00:00 5   Passwords left written down in an accessible location
01-07-2017 15:00:00 1   User has not locked his PC
03-07-2017 18:00:00 7   password did not meet the password construction guidelines
07-07-2017 11:03:59 8   Passwords has been be added to or written in an email
                        message
08-07-2017 13:00:00 20 User played games on the Internet
14-07-2017 12:00:00 16 User has visited or view illegal materials on the Internet
21-07-2017 12:00:00 14 Use the email systems in a way that could affect its
                       reliability or effectiveness, for example distributing chain
                       letters or spam
25-07-2017 12:30:00 10 undertaking deliberate activities that waste staff effort or
                       networked resource
29-07-2017 11:00:00 9   Users are not allowed to utilize password memorization
01-08-2017 17:00:00 11 The organization's email account did not been fundamentally
                       utilized for business that is related to the orgnization
15-08-2017 11:00:00 13 User has Sent unprotected sensitive or confidential
                       information
03-09-2017 16:00:00 15 Forwarding of company confidential messages to external
                       locations
07-09-2017 16:40:00 17 Personal use of the Internet caused a significant increase
                       in resource demand
12-09-2017 16:30:00 19 Download copyrighted material such as music media (MP3)
                       files, film and video files without appropriate approval
15-09-2017 11:00:00 18 Download software from the internet without prior approval
                       of the IT Department
15-09-2017 13:30:40 4   User disabled anti-virus software
16-09-2017 16:00:00 6   User has not changed his password
17-09-2017 17:30:00 12 organization’s email system has been utilized to create or
                       distribute offensive or disruptive message
18-09-2017 09:00:02 2   Computer Workstations must be shut completely down at the
                        end of the work day
20-09-2017 15:00:00 3   User not keeeping storage device in a secure place
23-09-2017 12:00:00 5   Passwords left written down in an accessible location
27-09-2017 15:00:00 1   User has not locked his PC
29-09-2017 18:00:00 7   password did not meet the password construction guidelines
30-09-2017 11:03:59 8   Passwords has been be added to or written in an email
                        message
```

```
02-10-2017 13:00:00 20 User played games on the Internet
05-10-2017 12:00:00 16 User has visited or view illegal materials on the Internet
10-10-2017 12:00:00 14 Use the email systems in a way that could affect its
                       reliability or effectiveness, for example distributing chain
                       letters or spam
17-10-2017 12:30:00 10 undertaking deliberate activities that waste staff effort or
                       networked resource
22-10-2017 11:00:00 9   Users are not allowed to utilize password memorization
25-10-2017 17:00:00 11 The organization's email account did not been fundamentally
                       utilized for business that is related to the orgnization
28-10-2017 11:00:00 13 User has Sent unprotected sensitive or confidential
                       information
29-10-2017 16:00:00 15 Forwarding of company confidential messages to external
                       locations
01-11-2017 16:40:00 17 Personal use of the Internet caused a significant increase
                       in resource demand
03-11-2017 16:30:00 19 Download copyrighted material such as music media (MP3)
                       files, film and video files without appropriate approval
04-11-2017 17:00:00 18 Download software from the internet without prior approval
                       of the IT Department
05-11-2017 13:30:40 4   User disabled anti-virus software
06-11-2017 11:00:00 6   User has not changed his password
07-11-2017 10:30:00 12 organization's email system has been utilized to create or
                       distribute offensive or disruptive message
10-11-2017 16:00:02 2   Computer Workstations must be shut completely down at the
                        end of the work day
11-11-2017 12:00:00 3   User not keeeping storage device in a secure place
15-11-2017 11:00:00 5   Passwords left written down in an accessible location
17-11-2017 09:00:00 1   User has not locked his PC
17-11-2017 17:00:00 7   password did not meet the password construction guidelines
20-11-2017 08:03:59 8   Passwords has been be added to or written in an email
                        message
22-11-2017 13:00:00 20 User played games on the Internet
27-11-2017 12:00:00 16 User has visited or view illegal materials on the Internet
01-12-2017 11:00:00 14 Use the email systems in a way that could affect its
                       reliability or effectiveness, for example distributing chain
                       letters or spam
09-12-2017 15:30:00 10 undertaking deliberate activities that waste staff effort or
                       networked resource
13-12-2017 11:00:00 9   Users are not allowed to utilize password memorization
19-12-2017 17:00:00 11 The organization's email account did not been fundamentally
                       utilized for business that is related to the orgnization
20-12-2017 11:00:00 13 User has Sent unprotected sensitive or confidential
                       information
22-12-2017 16:00:00 15 Forwarding of company confidential messages to external
                       locations
27-12-2017 16:40:00 17 Personal use of the Internet caused a significant increase
                       in resource demand
30-12-2017 09:30:00 19 Download copyrighted material such as music media (MP3)
                       files, film and video files without appropriate approval
30-12-2017 16:00:00 18 Download software from the internet without prior approval
                       of the IT Department
```

Scenario 2: User D violations:

In this scenario, the author assumes that User D is forgetful in terms of complying with the information security policies of his/her organisation. During the simulation period, which was three years, starting on 01-01-2015 and ending on 01-01-2018, User D violated each element twice, and the time period between the two violations was six months or more.

```
28-09-2015 10:00:00 3   User not keeeping storage device in a secure place
28-09-2015 11:30:40 4   User disabled anti-virus software
```

27-12-2015 12:00:00	5	Passwords left written down in an accessible location
27-12-2015 14:00:00	6	User has not changed his password
27-12-2015 15:00:00	7	password did not meet the password construction guidelines
27-12-2015 16:03:59	8	Passwords has been be added to or written in an email message
26-03-2016 08:40:01	10	Undertaking deliberate activities that waste staff effort or networked resources
26-03-2016 09:00:00	9	Users are not allowed to utilize password memorization
26-03-2016 10:00:00	17	Personal use of the Internet caused a significant increase in resource demand
26-03-2016 11:00:00	15	Forwarding of company confidential messages to external locations
26-03-2016 12:00:00	11	The organization's email account did not been fundamentally utilized for business that is related to the orgnization
26-03-2016 13:00:00	16	User has visited or view illegal materials on the Internet
26-03-2016 14:00:00	18	Download software from the internet without prior approval of the IT Department
26-03-2016 15:00:00	2	Computer Workstations must be shut completely down at the end of the work day
26-03-2016 16:00:00	14	Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spame
26-03-2016 17:00:00	19	Download copyrighted material such as music media (MP3) files, film and video files without appropriate approval
24-06-2016 11:00:00	20	User played games on the Internet
24-06-2016 12:00:00	13	User has Sent unprotected sensitive or confidential information
24-06-2016 14:30:00	1	User has not locked his PC
24-06-2016 15:30:00	12	organization’s email system has been utilized to create or distribute offensive or disruptive messages.
22-09-2016 10:00:00	3	User not keeeping storage device in a secure place
22-09-2016 11:30:40	4	User disabled anti-virus software
21-12-2016 12:00:00	5	Passwords left written down in an accessible location
21-12-2016 15:00:00	6	User has not changed his password
21-12-2016 14:00:00	7	password did not meet the password construction guidelines
21-12-2016 15:03:59	8	Passwords has been be added to or written in an email message
21-03-2017 15:40:01	10	Undertaking deliberate activities that waste staff effort or networked resources
21-03-2017 16:00:00	9	Users are not allowed to utilize password memorization
21-03-2017 16:20:11	17	Personal use of the Internet caused a significant increase in resource demand
21-03-2017 16:50:00	15	Forwarding of company confidential messages to external locations
21-03-2017 17:00:00	11	The organization's email account did not been fundamentally utilized for business that is related to the orgnization
21-03-2017 17:30:00	16	User has visited or view illegal materials on the Internet
21-03-2017 17:40:00	18	Download software from the internet without prior approval of the IT Department
21-03-2017 18:00:00	2	Computer Workstations must be shut completely down at the end of the work day
21-03-2017 18:10:00	14	Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spame
21-03-2017 18:30:00	19	Download copyrighted material such as music media (MP3) files, film and video files without appropriate approval
19-06-2017 11:00:00	20	User played games on the Internet
19-06-2017 15:00:00	13	User has Sent unprotected sensitive or confidential information
19-06-2017 16:30:00	1	User has not locked his PC
19-06-2017 17:30:00	12	organization’s email system has been utilized to create or distribute offensive or disruptive messages

Scenario 3: User E violations:

User E is very noncompliant with all the elements of the security policies. User E has not gained any compliance points on any of the elements of the policies because User E never passed the elapsed time of each element without a violation. The violations log file of User E contains 13 or more violations during the simulation period.

```
20-01-2015 11:00:00 7   password did not meet the password construction guidelines
22-01-2015 11:30:40 4   User disabled anti-virus software
25-01-2015 09:00:00 1   User has not locked his PC
29-01-2015 16:00:00 5   Passwords left written down in an accessible location
01-02-2015 11:03:59 8   Passwords has been be added to or written in an email
                        message
04-02-2015 17:00:00 15  Forwarding of company confidential messages to external
                        locations
08-02-2015 10:00:00 3   User not keeeping storage device in a secure place
12-02-2015 11:00:00 17  Personal use of the Internet  caused a significant increase
                        in resource demand
17-02-2015 10:00:02 2   Computer Workstations must be shut completely down at the
                        end of the work day
20-02-2015 13:30:00 19  Download copyrighted material such as music media (MP3)
                        files, film and video files without appropriate approval
21-02-2015 13:00:00 9   Users are not allowed to utilize password memorization
25-02-2015 15:00:00 6   User has not changed his password
27-02-2015 16:30:00 14  Use the email systems in a way that could affect its
                        reliability or effectiveness, for example distributing
                        chain letters or spam
28-02-2015 16:40:01 10  Undertaking deliberate activities that waste staff effort
                        or networked resources
04-03-2015 09:00:00 18  Download software from the internet without prior approval
                        of the IT Department
07-03-2015 11:00:00 11  The organization's email account did not been fundamentally
                        utilized for business that is related to the orgnization
07-03-2015 15:00:00 20  User played games on the Interne
08-03-2015 11:30:00 12  organization’s email system has been utilized to create or
                        distribute offensive or disruptive messages.
10-03-2015 14:00:00 16  User has  visited or view illegal materials on the Internet
11-03-2015 17:00:00 13  User has Sent unprotected sensitive or confidential
                        information
15-04-2015 12:00:00 7   password did not meet the password construction guidelines
17-04-2015 15:30:40 4   User disabled anti-virus software
19-04-2015 16:00:00 1   User has not locked his PC
22-04-2015 14:00:00 5   Passwords left written down in an accessible location
24-04-2015 15:03:44 8   Passwords has been be added to or written in an email
                        message
28-04-2015 17:00:00 15  Forwarding of company confidential messages to external
                        locations
02-05-2015 10:00:00 3   User not keeeping storage device in a secure place
05-05-2015 11:00:00 17  Personal use of the Internet  caused a significant increase
                        in resource demand
10-05-2015 10:00:02 2   Computer Workstations must be shut completely down at the
                        end of the work day
15-05-2015 13:30:00 19  Download copyrighted material such as music media (MP3)
                        files, film and video files without appropriate approval
17-05-2015 13:00:00 9   Users are not allowed to utilize password memorization
19-05-2015 15:00:00 6   User has not changed his password
20-05-2015 16:30:00 14  Use the email systems in a way that could affect its
                        reliability or effectiveness, for example distributing
                        chain letters or spam
25-05-2015 16:40:01 10  Undertaking deliberate activities that waste staff effort
                        or networked resources
28-05-2015 09:00:00 18  Download software from the internet without prior approval
                        of the IT Department
01-06-2015 16:00:00 11  The organization's email account did not been fundamentally
```

		utilized for business that is related to the orgnization
08-06-2015 15:00:00	20	User played games on the Interne
11-06-2015 11:30:00	12	organization’s email system has been utilized to create or distribute offensive or disruptive messages.
15-06-2015 14:00:00	16	User has visited or view illegal materials on the Internet
20-06-2015 17:00:00	13	User has Sent unprotected sensitive or confidential information
07-07-2015 12:00:00	7	password did not meet the password construction guidelines
10-07-2015 15:30:40	4	User disabled anti-virus software
12-07-2015 16:00:00	1	User has not locked his PC
15-07-2015 14:00:00	5	Passwords left written down in an accessible location
18-07-2015 15:03:44	8	Passwords has been be added to or written in an email message
21-07-2015 17:00:00	15	Forwarding of company confidential messages to external locations
25-07-2015 10:00:00	3	User not keeeping storage device in a secure place
29-07-2015 11:00:00	17	Personal use of the Internet caused a significant increase in resource demand
03-08-2015 10:00:02	2	Computer Workstations must be shut completely down at the end of the work day
08-08-2015 13:30:00	19	Download copyrighted material such as music media (MP3) files, film and video files without appropriate approval
10-08-2015 13:00:00	9	Users are not allowed to utilize password memorization
12-08-2015 15:00:00	6	User has not changed his password
13-08-2015 16:30:00	14	Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam
18-08-2015 16:40:01	10	Undertaking deliberate activities that waste staff effort or networked resources
21-08-2015 09:00:00	18	Download software from the internet without prior approval of the IT Department
24-08-2015 16:00:00	11	The organization's email account did not been fundamentally utilized for business that is related to the orgnization
02-09-2015 15:00:00	20	User played games on the Interne
04-09-2015 11:30:00	12	organization’s email system has been utilized to create or distribute offensive or disruptive messages.
08-09-2015 14:00:00	16	User has visited or view illegal materials on the Internet
13-09-2015 17:00:00	13	User has Sent unprotected sensitive or confidential information
02-10-2015 12:00:00	7	password did not meet the password construction guidelines
05-10-2015 15:30:40	4	User disabled anti-virus software
07-10-2015 16:00:00	1	User has not locked his PC
10-10-2015 14:00:00	5	Passwords left written down in an accessible location
13-10-2015 15:03:44	8	Passwords has been be added to or written in an email message
16-10-2015 17:00:00	15	Forwarding of company confidential messages to external locations
20-10-2015 10:00:00	3	User not keeeping storage device in a secure place
24-10-2015 11:00:00	17	Personal use of the Internet caused a significant increase in resource demand
28-10-2015 10:00:02	2	Computer Workstations must be shut completely down at the end of the work day
03-11-2015 13:30:00	19	Download copyrighted material such as music media (MP3) files, film and video files without appropriate approval
05-11-2015 13:00:00	9	Users are not allowed to utilize password memorization
07-11-2015 15:00:00	6	User has not changed his password
08-11-2015 16:30:00	14	Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam
13-11-2015 16:40:01	10	Undertaking deliberate activities that waste staff effort or networked resources
16-11-2015 09:00:00	18	Download software from the internet without prior approval of the IT Department
19-11-2015 16:00:00	11	The organization's email account did not been fundamentally utilized for business that is related to the orgnization
28-11-2015 15:00:00	20	User played games on the Interne
01-12-2015 11:30:00	12	organization’s email system has been utilized to create or distribute offensive or disruptive messages.

06-12-2015 14:00:00 16 User has visited or view illegal materials on the Internet
08-12-2015 17:00:00 13 User has Sent unprotected sensitive or confidential information
28-12-2015 11:00:00 7 password did not meet the password construction guidelines
02-01-2016 11:30:40 4 User disabled anti-virus software
05-01-2016 09:00:00 1 User has not locked his PC
07-01-2016 16:00:00 5 Passwords left written down in an accessible location
08-01-2016 11:03:59 8 Passwords has been be added to or written in an email message
11-01-2016 17:00:00 15 Forwarding of company confidential messages to external locations
15-01-2016 10:00:00 3 User not keeeping storage device in a secure place
20-01-2016 11:00:00 17 Personal use of the Internet caused a significant increase in resource demand
23-01-2016 10:00:02 2 Computer Workstations must be shut completely down at the end of the work day
28-01-2016 13:30:00 19 Download copyrighted material such as music media (MP3) files, film and video files without appropriate approval
01-02-2016 13:00:00 9 Users are not allowed to utilize password memorization
02-02-2016 15:00:00 6 User has not changed his password
04-02-2016 16:30:00 14 Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam
07-02-2016 16:40:01 10 Undertaking deliberate activities that waste staff effort or networked resources
11-02-2016 09:00:00 18 Download software from the internet without prior approval of the IT Department
15-02-2016 16:00:00 11 The organization's email account did not been fundamentally utilized for business that is related to the orgnization
22-02-2016 15:00:00 20 User played games on the Interne
26-02-2016 11:30:00 12 organization’s email system has been utilized to create or distribute offensive or disruptive messages.
01-03-2016 14:00:00 16 User has visited or view illegal materials on the Internet
04-03-2016 17:00:00 13 User has Sent unprotected sensitive or confidential information
24-03-2016 12:00:00 7 password did not meet the password construction guidelines
28-03-2016 15:30:40 4 User disabled anti-virus software
01-04-2016 16:00:00 1 User has not locked his PC
02-04-2016 14:00:00 5 Passwords left written down in an accessible location
03-04-2016 15:03:44 8 Passwords has been be added to or written in an email message
06-04-2016 17:00:00 15 Forwarding of company confidential messages to external locations
11-04-2016 10:00:00 3 User not keeeping storage device in a secure place
15-04-2016 11:00:00 17 Personal use of the Internet caused a significant increase in resource demand
19-04-2016 10:00:02 2 Computer Workstations must be shut completely down at the end of the work day
24-04-2016 13:30:00 19 Download copyrighted material such as music media (MP3) files, film and video files without appropriate approval
27-04-2016 13:00:00 9 Users are not allowed to utilize password memorization
28-04-2016 15:00:00 6 User has not changed his password
01-05-2016 16:30:00 14 Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam
02-05-2016 16:40:01 10 Undertaking deliberate activities that waste staff effort or networked resources
06-05-2016 09:00:00 18 Download software from the internet without prior approval of the IT Department
10-05-2016 16:00:00 11 The organization's email account did not been fundamentally utilized for business that is related to the orgnization
15-05-2016 15:00:00 20 User played games on the Interne
21-05-2016 11:30:00 12 organization’s email system has been utilized to create or distribute offensive or disruptive messages.
28-05-2016 14:00:00 16 User has visited or view illegal materials on the Internet
01-06-2016 17:00:00 13 User has Sent unprotected sensitive or confidential information
20-06-2016 12:00:00 7 password did not meet the password construction guidelines

24-06-2016 15:30:40	4	User disabled anti-virus software
28-06-2016 16:00:00	1	User has not locked his PC
29-06-2016 14:00:00	5	Passwords left written down in an accessible location
29-06-2016 15:03:44	8	Passwords has been be added to or written in an email message
01-07-2016 17:00:00	15	Forwarding of company confidential messages to external locations
06-07-2016 10:00:00	3	User not keeeping storage device in a secure place
10-07-2016 11:00:00	17	Personal use of the Internet caused a significant increase in resource demand
15-07-2016 10:00:02	2	Computer Workstations must be shut completely down at the end of the work day
20-07-2016 13:30:00	19	Download copyrighted material such as music media (MP3) files, film and video files without appropriate approval
22-07-2016 13:00:00	9	Users are not allowed to utilize password memorization
24-07-2016 15:00:00	6	User has not changed his password
27-07-2016 16:30:00	14	Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam
28-07-2016 16:40:01	10	Undertaking deliberate activities that waste staff effort or networked resources
02-08-2016 09:00:00	18	Download software from the internet without prior approval of the IT Department
05-08-2016 16:00:00	11	The organization's email account did not been fundamentally utilized for business that is related to the orgnization
11-08-2016 15:00:00	20	User played games on the Interne
16-08-2016 11:30:00	12	organization’s email system has been utilized to create or distribute offensive or disruptive messages.
24-08-2016 14:00:00	16	User has visited or view illegal materials on the Internet
28-08-2016 17:00:00	13	User has Sent unprotected sensitive or confidential information
15-09-2016 12:00:00	7	password did not meet the password construction guidelines
20-09-2016 15:30:40	4	User disabled anti-virus software
24-09-2016 16:00:00	1	User has not locked his PC
25-09-2016 14:00:00	5	Passwords left written down in an accessible location
26-09-2016 15:03:44	8	Passwords has been be added to or written in an email message
28-09-2016 17:00:00	15	Forwarding of company confidential messages to external locations
01-10-2016 10:00:00	3	User not keeeping storage device in a secure place
05-10-2016 11:00:00	17	Personal use of the Internet caused a significant increase in resource demand
10-10-2016 10:00:02	2	Computer Workstations must be shut completely down at the end of the work day
15-10-2016 13:30:00	19	Download copyrighted material such as music media (MP3) files, film and video files without appropriate approval
17-10-2016 13:00:00	9	Users are not allowed to utilize password memorization
17-10-2016 15:00:00	6	User has not changed his password
24-10-2016 16:30:00	14	Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam
25-10-2016 16:40:01	10	Undertaking deliberate activities that waste staff effort or networked resources
28-10-2016 09:00:00	18	Download software from the internet without prior approval of the IT Department
01-11-2016 16:00:00	11	The organization's email account did not been fundamentally utilized for business that is related to the orgnization
06-11-2016 15:00:00	20	User played games on the Interne
15-11-2016 11:30:00	12	organization’s email system has been utilized to create or distribute offensive or disruptive messages.
20-11-2016 14:00:00	16	User has visited or view illegal materials on the Internet
24-11-2016 17:00:00	13	User has Sent unprotected sensitive or confidential information
10-12-2016 11:00:00	7	password did not meet the password construction guidelines
15-12-2016 11:30:40	4	User disabled anti-virus software
20-12-2016 09:00:00	1	User has not locked his PC
20-12-2016 16:00:00	5	Passwords left written down in an accessible location
21-12-2016 11:03:59	8	Passwords has been be added to or written in an email

		message
24-12-2016	17:00:00	15 Forwarding of company confidential messages to external locations
28-12-2016	10:00:00	3 User not keeeping storage device in a secure place
01-01-2017	11:00:00	17 Personal use of the Internet caused a significant increase in resource demand
05-01-2017	10:00:02	2 Computer Workstations must be shut completely down at the end of the work day
10-01-2017	13:30:00	19 Download copyrighted material such as music media (MP3) files, film and video files without appropriate approval
12-01-2017	13:00:00	9 Users are not allowed to utilize password memorization
12-01-2017	15:00:00	6 User has not changed his password
20-01-2017	16:30:00	14 Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam
21-01-2017	16:40:01	10 Undertaking deliberate activities that waste staff effort or networked resources
24-01-2017	09:00:00	18 Download software from the internet without prior approval of the IT Department
28-01-2017	16:00:00	11 The organization's email account did not been fundamentally utilized for business that is related to the orgnization
02-02-2017	15:00:00	20 User played games on the Interne
10-02-2017	11:30:00	12 organization’s email system has been utilized to create or distribute offensive or disruptive messages.
15-02-2017	14:00:00	16 User has visited or view illegal materials on the Internet
20-02-2017	17:00:00	13 User has Sent unprotected sensitive or confidential information
05-03-2017	12:00:00	7 password did not meet the password construction guidelines
10-03-2017	15:30:40	4 User disabled anti-virus software
15-03-2017	12:00:00	1 User has not locked his PC
15-03-2017	14:00:00	5 Passwords left written down in an accessible location
16-03-2017	15:03:44	8 Passwords has been be added to or written in an email message
20-03-2017	17:00:00	15 Forwarding of company confidential messages to external locations
24-03-2017	10:00:00	3 User not keeeping storage device in a secure place
28-03-2017	11:00:00	17 Personal use of the Internet caused a significant increase in resource demand
01-04-2017	10:00:02	2 Computer Workstations must be shut completely down at the end of the work day
05-04-2017	13:30:00	19 Download copyrighted material such as music media (MP3) files, film and video files without appropriate approval
06-04-2017	13:00:00	9 Users are not allowed to utilize password memorization
06-04-2017	15:00:00	6 User has not changed his password
15-04-2017	16:30:00	14 Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam
16-04-2017	16:40:01	10 Undertaking deliberate activities that waste staff effort or networked resources
20-04-2017	09:00:00	18 Download software from the internet without prior approval of the IT Department
24-04-2017	16:00:00	11 The organization's email account did not been fundamentally utilized for business that is related to the orgnization
28-04-2017	15:00:00	20 User played games on the Interne
05-05-2017	11:30:00	12 organization’s email system has been utilized to create or distribute offensive or disruptive messages.
10-05-2017	14:00:00	16 User has visited or view illegal materials on the Internet
15-05-2017	17:00:00	13 User has Sent unprotected sensitive or confidential information
01-06-2017	12:00:00	7 password did not meet the password construction guidelines
05-06-2017	15:30:40	4 User disabled anti-virus software
10-06-2017	12:00:00	1 User has not locked his PC
10-06-2017	14:00:00	5 Passwords left written down in an accessible location
11-06-2017	15:03:44	8 Passwords has been be added to or written in an email message
15-06-2017	17:00:00	15 Forwarding of company confidential messages to external locations
20-06-2017	10:00:00	3 User not keeeping storage device in a secure place

24-06-2017 11:00:00	17	Personal use of the Internet caused a significant increase in resource demand
28-06-2017 10:00:02	2	Computer Workstations must be shut completely down at the end of the work day
01-07-2017 13:30:00	19	Download copyrighted material such as music media (MP3) files, film and video files without appropriate approval
02-07-2017 13:00:00	9	Users are not allowed to utilize password memorization
02-07-2017 15:00:00	6	User has not changed his password
10-07-2017 16:30:00	14	Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam
11-07-2017 16:40:01	10	Undertaking deliberate activities that waste staff effort or networked resources
15-07-2017 09:00:00	18	Download software from the internet without prior approval of the IT Department
20-07-2017 16:00:00	11	The organization's email account did not been fundamentally utilized for business that is related to the orgnization
24-07-2017 15:00:00	20	User played games on the Interne
01-08-2017 11:30:00	12	organization’s email system has been utilized to create or distribute offensive or disruptive messages.
05-08-2017 14:00:00	16	User has visited or view illegal materials on the Internet
10-08-2017 17:00:00	13	User has Sent unprotected sensitive or confidential information
27-08-2017 12:00:00	7	password did not meet the password construction guidelines
01-09-2017 15:30:40	4	User disabled anti-virus software
05-09-2017 13:00:00	1	User has not locked his PC
05-09-2017 14:00:00	5	Passwords left written down in an accessible location
06-09-2017 15:03:44	8	Passwords has been be added to or written in an email message
10-09-2017 17:00:00	15	Forwarding of company confidential messages to external locations
15-09-2017 10:00:00	3	User not keeeping storage device in a secure place
20-09-2017 11:00:00	17	Personal use of the Internet caused a significant increase in resource demand
24-09-2017 10:00:02	2	Computer Workstations must be shut completely down at the end of the work day
28-09-2017 13:30:00	19	Download copyrighted material such as music media (MP3) files, film and video files without appropriate approval
29-09-2017 13:00:00	9	Users are not allowed to utilize password memorization
29-09-2017 15:00:00	6	User has not changed his password
05-10-2017 16:30:00	14	Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam
06-10-2017 16:40:01	10	Undertaking deliberate activities that waste staff effort or networked resources
10-10-2017 09:00:00	18	Download software from the internet without prior approval of the IT Department
15-10-2017 16:00:00	11	The organization's email account did not been fundamentally utilized for business that is related to the orgnization
20-10-2017 15:00:00	20	User played games on the Interne
27-10-2017 11:30:00	12	organization’s email system has been utilized to create or distribute offensive or disruptive messages.
01-11-2017 14:00:00	16	User has visited or view illegal materials on the Internet
05-11-2017 17:00:00	13	User has Sent unprotected sensitive or confidential information
15-11-2017 12:00:00	7	password did not meet the password construction guidelines
20-11-2017 15:30:40	4	User disabled anti-virus software
25-11-2017 16:00:00	1	User has not locked his PC
26-11-2017 14:00:00	5	Passwords left written down in an accessible location
28-11-2017 15:03:44	8	Passwords has been be added to or written in an email message
29-11-2017 17:00:00	15	Forwarding of company confidential messages to external locations
05-12-2017 10:00:00	3	User not keeeping storage device in a secure place
10-12-2017 11:00:00	17	Personal use of the Internet caused a significant increase in resource demand
17-12-2017 10:00:02	2	Computer Workstations must be shut completely down at the end of the work day

20-12-2017 10:30:00	19	Download copyrighted material such as music media (MP3) files, film and video files without appropriate approval
20-12-2017 13:00:00	9	Users are not allowed to utilize password memorization
21-12-2017 15:00:00	6	User has not changed his password
25-12-2017 16:30:00	14	Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam
25-12-2017 16:40:01	10	Undertaking deliberate activities that waste staff effort or networked resources
26-12-2017 09:00:00	18	Download software from the internet without prior approval of the IT Department
27-12-2017 09:00:00	11	The organization's email account did not been fundamentally utilized for business that is related to the orgnization
27-12-2017 15:00:00	20	User played games on the Interne
28-12-2017 11:30:00	12	organization’s email system has been utilized to create or distribute offensive or disruptive messages.
29-12-2017 14:00:00	16	User has visited or view illegal materials on the Internet
30-12-2017 17:00:00	13	User has Sent unprotected sensitive or confidential information

Appendix B: Experts invitation letter & Ethical approvals

The following is a copy of the invitation letter that has been sent to the experts in order to seek their participation on the model evaluation.

Invitation letter

Dear .....

I am writing to you to request your participation in a brief interview. I am a Ph.D. student at Plymouth University. My research concerns users' compliance with the information security policies. The aim of this research is to propose a model that is intended to provide a comprehensive framework for raising the level of compliance amongst end-users, with the aim of monitoring, measuring and responding to users' behaviour with an information security policy. In this reserach, a prototype system was developed in order to visualize the real system of the proposed model of monitoring user's security policy compliance. The prototype system acts as a simulation for the real system in a real environment. Following the development of the system, an expert-based evaluation should take place with the aim of validating the novelty, reviewing the performance and identifying its limitations.

As you are considered one of the experts in this area, your participation in this project would go a long way towards helping me achieve my research goals. I would be extremely grateful if I could interview you via Skype and record your responses to a few questions (8 in total) related to topic. At the beginning of the interview, a demo of the system will be presented to the interviewee (15 minutes) in order to provide them with a better insight into how it works. The interview would last approximately 45 minutes and, should you agree to participate, I would be grateful if you could let me know when you are free to meet via Skype or using any other means you feel may be more appropriate.

I have attached a copy of the interview form for your attention. Your participation is vital to this research. The information and data that you provide will remain confidential, and will only be used for this research.

Kind regards
Mutlaq Alotaibi
PhD Researcher
Centre for Security, Communications and Network Research (CSCAN http://www.cscan.org/),
School of Computing, Electronics and Mathematics (Faculty of Science and Engineering),
University of Plymouth, Plymouth, UK;
Phone: +44(0) 7749770933
Email: mutlaq.alotaibi@plymouth.ac.uk
CSCAN: https://www.cscan.org/?page=studentprofile&id=246

Ethical approvals

RESEARCH WITH PLYMOUTH UNIVERSITY

3 February 2017

CONFIDENTIAL
Mutlaq Alotaibi
School of Computing, Electronics and Mathematics

Dear Mutlaq

Ethical Approval Application

Thank you for submitting the ethical approval form and details concerning your project:

A model for monitoring user's security policy compliance

I am pleased to inform you that this has been approved subject to the following condition:

- The identity of the experts should remain anonymous

Kind regards

Paula Simson
Secretary to Faculty Research Ethics Committee

Cc. Prof Steven Furnell
Prof Nathan Clarke

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

Approval for experts evaluation

4

PS

Paula Simson

Mon 06/02/2017 17:05

To: Mutlaq Alotaibi

Cc: Steven Furnell; Nathan Clarke

Reply all

Dear Mutlaq

Further to my previous email, I can confirm that the condition of the identity of experts remaining anonymous can be removed as long as they have provided explicit consent for their names/identities to be used.

Regards
Paula

Paula Simson | Administrative assistant | Dean's Office | Faculty of Science and Engineering | 009 Smeaton | Ext 84503 | email paula.simson@plymouth.ac.uk
Working hours: Monday – Thursday 09.30 – 17.00 Friday 09.30 – 16.30

Appendix C: Experts' feedback

This section provides more information regarding the evaluation process of the model. It contains the full transcripts of interviews with each of the experts.

Academics:

A1- Prof. Rossouw von Solms,

He is a professor and director of the Centre for Research in Information and Cyber Security, School of ICT, Nelson Mandela Metropolitan University (NMMU), Port Elizabeth, South Africa. He supervises many PhD and postdoctoral students in the field of Information Security and IT Governance. Rossouw has published and presented in excess of one hundred and fifty academic papers in journals and conferences, both internationally and nationally. Most of these papers were published and presented in the field of Information Security.

Q1- What are your thoughts of the identified research problem?

I totally agree with you, it is international problem, it is right over all in industries, in fact it is getting worst. So, I totally agree with you the problem that you have identified is a real problem that needs to be researched and solutions need to be devised for industry because industry has not got the answers to solve this problem so I totally concur with the problem statement as you got it.

Q2-How realisable/attainable/feasible do you feel this model is at the operational level?

I do think you are on the right direction but make sure does not come to complicated and that is a bit of my concern that first if all you know there are some ethical issue involve I think because the users are being monitored, are they aware of that, is there a clear mechanism, so the ethical issue is a problem that need to be addressed. Secondly, how technical it is and so on, to manage to assess to follow up, but it seems to me that you got it sorted out, so that seems to me it can work. And the third thing I want to mention it, how accurate it is, because it is not that difficult to check or technical problems and things like that but for behavioral problems, you know, is not that easy to actually report that, so make sure that you can report behaviors and so on.

Q3-What do you think about utilising the concept of response taxonomy for non-compliance behaviour in enhancing users' compliance?

If I understand you correctly. Thus concept would be helpful but there will be a psychological problem, I have done a thing like that in the past as well and you know the users feel very bad when they get notified that they made a mistake so someway I think it will be good if you get a little bit psychological from the philosophy people because we have chat to a philosophy people how you going to phrase that response, how it is important, because it must not let the user feel bad and so on, it can work but you must be carefully how hat response is going to be.

Q4-What do you think about utilising the concept of compliance points system to monitor the compliance levels to gain insight on users' behaviour and Implemented information security policies?

Again, yeas it a good idea. I think from an employer point of view there is a lot of advantages but again from users point of view if you get ranked any value consistently you are going to be very afraid of doing things and doing your work because you so afraid of making mistakes but again this need to be addressed, but surely from an employer point of view there is a lot of advantages but from a user point of view it can be problematic if I know being monitored all the time. I support the idea but it is need to be done very sensitive that the users do not find themselves always being reported or scoring low against the others, it depends on how you advertise and make publicly the assessment, how various users are actually doing.

Q5-To what extent do you feel the simulation have provided a robust validation of the approach?

Yes, it was good and clear,

Q6-How realisable/attainable/possible do you feel this system is?

It can be implemented. From a technical point of view the challenges will be based on the extent to which it will be possible to capture and assess behavioural actions related to policies. From an ethical/psychological aspect, it will be important not to violate any privacy rights of the user,to make the user feel he/she is being monitored the whole time and it must be motivational to the user and not degrading. Thus, the response to the user is very important and needs to be positive and not negative.

Q7-To what extent do you think having the proposed model can assist organisations in monitoring and measuring users' behaviour with each element of the security policy in a dynamic way?

For what I saw from the demo, it seems definitely movements in the right direction. Currently very little like that is available and employers do not really know how well their users are complying to some, more behavioural policies. this approach/system will definitely help, but it should be accepted by the users and not seen as invasive.

Q8-What do you feel are the strengths & weaknesses of the developed system and any barriers using such a system?

Strengths: definitely that employers will have more proof and assurance that their users are following policies. Adds a lot of value on this issue. Weaknesses: The user side from ethical and psychological point of view. Users must not experience the systems an invasive or 'checking up' on them. The buy-in of the users are important.

A2-Prof. Stephen V. Flowerday,

He is presently a professor focusing on Information Security at the University of Fort Hare, South Africa. He is also lecture in the following two subjects: Information Security and

Research Methods. Stephen has supervised postgraduate students and published extensively within his research field, East London, South Africa. Over the last twelve years, he has authored in excess of 70 refereed publications and have presented papers in various countries. Furthermore, he acts as a reviewer for conference publications and academic journals. He has supervised more than 30 postgraduate students to completion and am currently supervising many of master's and doctoral students in the field of Information Security.

Q1- What are your thoughts of the identified research problem?

Thought of the research problem, I thought was very relevant, I think it is very top, your topic is relevant, I think it should be researched.

Q2-How realisable/attainable/feasible do you feel this model is at the operational level?

My concern was about resource intensive; how do you collect all these data on each user? So, do you not thinks that is a lot of work to do and it says a company had 500 employees and you have go 20 different policy aspect you monitoring on each employee that 10,000 things you need to look at to get update your graph, how you intend to collect the data, it is a resource intensive. I think it feasible, I would to see if that would work, I have seen some like this before but it becomes big and unmanageable sometimes. You need to find way to use these agents widely.

Q3-What do you think about utilising the concept of response taxonomy for non-compliance behaviour in enhancing users' compliance?

I thought your taxonomy was interesting. I want to know about your theoretical foundation, did you based on any theories, I mean when you start talk about enforcement? Because enforcement is a lot of doubt with policy enforcement works, usually theory reason action or theory planed behaviour, which theory you used and then we get on to the enforcement side most of stuff has been tested in the theories. If the user is aware of being monitored this may affect the intentional behaviour but will not affect the unintentional behaviour.

Q4-What do you think about utilising the concept of compliance points system to monitor the compliance levels to gain insight on users' behaviour and Implemented information security policies?

So specifically, about using points, assigning points to user behaviour when it comes to compliance, I think this a good novel aspect in the sense that you mentioned that you mention that it was used in marketing, and we know this concept is used in our university for individual performance agreements and it effects performance from management perspective. We used points also before in mutuality models as well to score them so I do think there is merit in using points system, yes I do agree with that, if you can collect the correct date there is merits.

Q5-To what extent do you feel the simulation have provided a robust validation of the approach?

I feel that was a validation of the model, it works. My question would be back to the begging of the discussion about is it practical, is it too resources intensive but if you can collect all the data, if your agents are able collect all the data and the data is a value, your model seems to work your graphs seem to indicate high risk user, low risk user so from that perspective I fell it works.

Q6-How realisable/attainable/possible do you feel this system is?

I do think it is likely to be implemented soon. but I feel you need to look at what is causing the behaviour risk, what is causing the individual to behave badly, intentionally or unintentionally, I think this will go back to the theoretical side. I think the monitoring side is going be costly and that why I am feel, a small or medium size business is unlikely to use a system unless you provide a small package which easily to downloaded I do know. So, from a large organisation point of view they could probably invest more. I think the concept is doable

Q7-To what extent do you think having the proposed model can assist organisations in monitoring and measuring users' behaviour with each element of the security policy in a dynamic way?

Look I think the dynamic way is interesting because any area field is an issue let say people are changing the password I can go look at that and show it you if it internet usage orb whatever you can go run it, and I think that would be useful if I was trying to make decision based on employee behaviour also if I have a problem with specific employee. I think from the theoretical point of view I think that is fine, just I wonder if you have dashboard in a real time or run it for a week or so.

Q8-What do you feel are the strengths & weaknesses of the developed system and any barriers using such a system?

Look I think if you want the moment monitoring and evaluation of employees' behaviour is discussed everywhere the moment is strength that people current want to monitor behaviour. I think the fact that you able to dill down to individual aspect within a security policy I think that is nice you could have an employee in front of you and look at a specific aspect and see if they comply or not, if they going debt points or not, I think there is ……

There is a question mark about enforcement. There is a doubt with enforcement whether is helpful and works or not whit it comes to security policy compliance, especially if you have unintentionally behaviour and when you start employ enforcement policy, it seems to have a negative effect on employee and it can actually go the wrong way. The second question would be resource intensive but if you feel your agent would work 24/7 drilling through a background and getting this data for you and the data is accurate data then I think employee would accept it.

A3-Prof. Simon Tjoa:

He is a lecturer/ Security Analyst in the Department of Computer Science and Security at St. Poelten University of Applied Sciences, Austria. His fields of interest are Business Process Management, Risk Management, Information Security Management, Digital Forensics, Critical Information Infrastructure Protection, Business Continuity Management. He has more than 17 years' experience in field of information security. Dr. Simon has several industry recognised certifications including ISO 22301 Lead Auditor, Certified Information Systems Auditor (CISA). Certified Information Security Manager (CISM).

Q1- What are your thoughts of the identified research problem?

I think the problem identified with the compliance is quite realistic, is one of the common problem, how to measure the security compliance, I mean there is great deal currently going on with all this I would say data lost prevention tools and the SIEM systems try to somehow monitor a compliance in real time basis but I like the idea to somehow process the logs afterwards to get a scoring system. I think if you make it a feel logs, it would be quite good help to cluster the users into different kind of groups and make targeted awareness nations or training to improve the security situation.

Q2-How realisable/attainable/feasible do you feel this model is at the operational level?

So that depends on how many logs you are able to process, I think you should combine it with some like logs correlation system, e.g logstash, Kibana and elasticsearch. If you somehow can establish to bridge between log analysis and your approach I think it will be very feasible. I think it will be very feasible.

Q3-What do you think about utilising the concept of response taxonomy for non-compliance behaviour in enhancing users' compliance?

I think it would be a good approach but I am not completely sure if it is feasible in a corporate, because I think a lot of people would have to be trained very often, which consume a lot of time of them. So, I was not sure how was you intend to make such a basic awareness. (I explained to him how I am going to do that…) so it just pops up notice saying what you doing currently is wrong so I think from my experience people would just click OK that is the problem, I mean may it help for some people but I think only if it comes to level 3 and yeah its effects will be bigger, people become more serious about that. I think you would have to test it in real users' situation, but from my feeling I would say that should at least some advanced levels, whether block the communication, user or somethings like that.

Q4-What do you think about utilising the concept of compliance points system to monitor the compliance levels to gain insight on users' behaviour and Implemented information security policies?

I think I will be quite idea but I was thinking if it possible to make this compliance behaviour to the ISO as 2701, appendix A so that you know which kind of area or domain the policy breach was, to get indicate of where to improve the information security management system.

2701 standard it is giving the controls in appendix A and I think I would be very helpful if there is a mapping between violations and those domains, like it is in access control area so which domain that is affected because I am like information security officer, I have to somehow check if internal control system is looking fine. Now you are very specified on the users which user has how many compliance violations but another interested point of view would be for some organisations in which area are the most breaches, is it to the confidential information or to the not change passwords correctly, in which domain is an organisation performing not good?

Technical considerations, costs, and performance impacts of the proposed system on an organisation?

I do not think so, because it is not like intended to, it just analysis tool yes, just used for log analysis so I do not think three would be a huge performance decrease in the system.

Q5-To what extent do you feel the simulation have provided a robust validation of the approach?

So I think the simulation of course, yeah if I understood was not like taken from real data so that of course limitation of the simulation, you would have to somehow try to make it real using some real kind of organisations data to show it validity but I think it would be feasible if you ask your partner to get anonymous data of real a company or like that.

Q6-How realisable/attainable/possible do you feel this system is?

I think with a little bit modifications, it could be very feasible for companies, because companies have often the problem that how to log data and they have to somehow process it and some companies does the data just taking the most security incident analysis, which is carried out but they are not taking the data like you for monitoring compliance issues and things like that so that would be very helpful. There is very expensive tool, which try to do the same thing like semantic compliance treat I think, try to monitor compliance. So, I think it is very feasible, nowadays compliance issues are raising I think companies are searching for new solutions to measure it.

Q7-To what extent do you think having the proposed model can assist organisations in monitoring and measuring users' behaviour with each element of the security policy in a dynamic way?

Yeah, it is a good question. If you able to somehow couple it the existing tools out there, like security information and events management systems and somehow establish to bridge then I think it would be quite powerful tool to measure it. An interesting question would be what happen in an organisation if there is a lot of people violating some policies, so you maybe would have to make some response strategy.

Q8-What do you feel are the strengths & weaknesses of the developed system and any barriers using such a system?

I think the strengths, would be very easy to use, I think there is a lot of work down in the visualisation in the analysis of the users, as said the only thing that would I recommend regarding clustering of users would be possible to say maybe those kinds of users can not cooperate with this piece of policy still not aware of something like … so an organisation can make open point trainings for specific users or users groups and you can somehow make targeted groups for security awareness out of it.

The main limitation, I think currently it is not dynamic, it has not been tested, to be tested with real company data, and of course if you have like large company are you would escalate it to such a big company from the prototype you currently have to that extent I think then you would have to make another interface or something like that. But all in all, I think the approach go to the right direction to help the people to make continues logs analysis of security awareness or even by the real-time analysis, like real time display as I said my experience in data lost prevention domains show it help with some users to improve their awareness so I think that it is a right approach.

A4-Dr. Christos Kalloniatis

He holds a PhD from the Department of Cultural Technology and Communication of the University of the Aegean and a master degree on Computer Science from the University of Essex, UK. Currently he is an assistant professor in the Department of Cultural Technology and Communication of the University of the Aegean. He is also a deputy member of the board of the Hellenic Authority for Communication Security and Privacy. His main research interests are the elicitation, analysis and modelling of security and privacy requirements in traditional and cloud-based systems, Privacy Enhancing Technologies and the design of Information System Security and Privacy in Cultural Informatics. He is an author of several refereed papers in international scientific journals and conferences and has served as a visiting professor in many European Institutions. Prior to his academic career he has served at various places on the Greek public sector including the North Aegean Region and Ministry of Interior, Decentralisation and e-Governance. He is a lead-member of the Cultural Informatics research group as well as the privacy requirements research group in the Department of Cultural Technology and Communication of the University of the Aegean and has a close collaboration with the Laboratory of Information & Communication Systems Security of the University of the Aegean. He has served as a member of various development and research projects.

Meeting held over Skype on 02/03/2017 at 11:00 am

Q1- What are your thoughts of the identified research problem?

The questions raised is totally very interesting, it is very good to have this kind of research, users are one of the most important factor to guarantee the successful of an information security within an organization. Overall, your topic is interesting.

Q2-How realisable/attainable/feasible do you feel this model is at the operational level?

I saw the applicability of your model and I saw the tool that you have prepared, which quite interesting, I think the tool that you have design is very applicable and it is very feasible to be applied in a real organisation, I am not 100% sure if it will be easy or applicable for security officers without extensive training but do not say that the development was bad but also should be user friendly, the purpose of the tool is different. I will raise the concern only regarding the capability of the security officer to be able to implement, 100% get out of the tool, how easy it will be, or it will require number of things. There should be better harmonisation regarding the points you know the points allocation, positive and negative, and how we led this negative and positive allocation with the users, so you can try to show a little bit more this is not discouraging for the users but it will be something that will help them in dealing better with the security policy. It not like a penalty tool so we look for a bad user, something that will help us, I will raise this part but as a functionality of the tool, it is very good, I like it a lot.

Q3-What do you think about utilising the concept of response taxonomy for non-compliance behaviour in enhancing users' compliance?

I do agree on that, I think it should be enhanced, I think it is one of the factors that we should address in this kind of work, so I go with it and I support it.

Q4-What do you think about utilising the concept of compliance points system to monitor the compliance levels to gain insight on users' behaviour and Implemented information security policies?

I think this is the most important part of your PhD thesis, how to combine the applicability of the security policy not only from the technical level but also from the user behaviour side so initially I totally agree with that. As I told you before I believe the points system should be in details explain why they will follow this points system and how this points system indeed projects to the necessary level of monitoring people in an organisation so why they will follow this system and do not follow another kind of system of points system. Usually, Mutlaq just remember that the term of points system as we know it usually follows something bad. In based on the idea of the points system regarding the development and securing of the organisation, the organisation will be better by this monitoring not just to identify the weakness led for judging them, I think this should be very distinguishable. If I were you I will try to establish this system in an organisation, I would not have negative marks, I would have zero and positive marks, I would have a threshold, for example, the weak one will take low positive mark and the good one high positive mark, for example, for me number one is negative but the user will not see the negative mark, is the psychological factor. Why am telling you that because if you, for example, go to an organisation and say I will apply this tool, if this tool will stay on the security officer side and no user will see then okay but if you inform the user and say look from now on we will use this tool to monitor your behaviour regarding the feasibility of the security policy, if the user see the negative marks, they will probably hesitate to follow that, so it will act against the willing of the user to be better. However, if every has positive marks psychologically is better but you know that number 1 is weak, number 2 is weak and number 10 is good like this, yeah just keep that in mind. If

you see that we need that because the security officer will keep that and will not disseminate that in an organisation we want to keep it private, the security officer will use this tool to see what happens and then the dissemination plan will be something different it will be respectful the tool, it okay, but if you want publish it and know the user how they will be monitored, having positive mark for everybody, giving your meaning to 1 and 2 and 10 then psychologically may better.

Q5-To what extent do you feel the simulation have provided a robust validation of the approach?

I think the examples that you have done, which examining all important categories was very good, I think they was 14 as I remember. Have you performed this also in a real organisation? Have you considered in small baseness to see how they are react? To examine the capability in real environment. If you can apply it in a small department for example in Plymouth university, just to raise the validation and say that I have applied in customised data set but also in real case study the department of finance in the university of Plymouth, for example. (Mutlaq: explained the situation for him) If it is difficult I would say it is ok for me what you have done

Q6-How realisable/attainable/possible do you feel this system is?

I think it is realisable, because it is a simple system but it has started a logic of mapping the security policy on something more technical, I think it is quite reliable, if it is used by a security officer.

Q7-To what extent do you think having the proposed model can assist organisations in monitoring and measuring users' behaviour with each element of the security policy in a dynamic way?

I think it is very good, I think the applicability of the model is very passed, you can deploy it in an organisation very easily as soon as an organisation get the log files and the format that you wish. I do not know how long you will require to transform the data from the users log file, so maybe a little of work can be done as a special extension in an organisation to be able to customise the output of the data to have it as an input easily to the tool.

Q8-What do you feel are the strengths & weaknesses of the developed system and any barriers using such a system?

Definitely, the positive issue we see here wards that try to bridge the gap between the conceptual text into the capability into users' behaviour which is very important and very difficult, the mapping between the policies and user behaviour, understanding how where enforcing the security policy and having an online tool in real time basis to monitor the users and identify which is their weaknesses is very important because with this kind of tool we can explore educational need for the users training seminars. The drawback of the tool as I told you before, I will raise the part of the psychological aspect of the user in implementing this kind of tool, accepting this kind of tool. I will also increase the traceability of the data collected, so I will make the user traced the tool by applying what increasing their witness

through traceability policy through statement how I will monitor the data and how I will collect the data. I think this is missing from the tool, the handling of the data, how will do it.

A5- Dr. Spiro Samonas:

He is currently an assistant professor in information systems at California State University. Long Beach. prior to this appointment, he was a visiting assistant professor in computer information systems at Louisiana Tech University and a post-doctoral research fellow in cyber-security at Virginia commonwealth University. His research focuses on digital deception and digital crime, and the socio-technical aspects of information security.

Q1- What are your thoughts of the identified research problem?

OK, I agree the taken research problem was genuine, due to human aspect involved within this problem. There is a lot of literature research on the research problem, so the different aspects of compliance have been discussed, different models on compliant and noncompliant behaviour, deviants on security but to my knowledge, I think, I have not seen any other projects, papers talking about points system, so that is a concept that is familiar from drivers licenses this kind of things so points system seems to be good idea, the research problem we know I mean so whether user is compliant or not so then the issue has to do with sanctions, recommendations for changing behaviour and this kind of things, so I think it is an interesting approach, I have not seen it before.

Q2-How realisable/attainable/feasible do you feel this model is at the operational level?

Ok, at the operational level, I am not entirely sure how this is going to work, I understand it can be configured of course according to the need of a particular organisation and can be flexible that is fine, my concern is that you have in the security side of an organisation typically you have limited resources…….it may be difficult for CIO or CISO to dedicate resources to the compliance team to perform this kind of job. On other hand, you may have organisations have dedicated compliance team or quality assurance department and like that and ….....but I would think that this kind of monitoring requires a deep approach in terms of collecting data from noncomplying behaviours at the technical level and informal level , you can create a dash board that can consolidate all kind of information and then based on behaviour you can reward points or detect points but that would require a considerable investment in term of resources to do so. Therefore, I am not sure what kind of organisations would be prepared to do that, I am sure some organisation will but it might be not feasible for a small or medium size enterprise, it only for large organisations. Unless if you find a way that you can make it in a light of package and you build in some capability, so that it is easy for small originations but I am not sure how that would work.

Q3-What do you think about utilising the concept of response taxonomy for non-compliance behaviour in enhancing users' compliance?

I agree with your concept about response taxonomy, I think it workable. Yeah that it is exactly like the points system that we have in driving licence at least in USA, depend on the type of the violation and the time that has elapsed between the previous violation and then

you have an escalation and of course, different level different sanction. I think that is necessary part of the security. There is a value for that, I think there is a need for further research and investigate this concept in real organisation if you have the opportunity that would be a fantastic.

Q4-What do you think about utilising the concept of compliance points system to monitor the compliance levels to gain insight on users' behaviour and Implemented information security policies?

So, as I mentioned before, you are try to build a controlling dashboard that will feeding different types of data with respect to the security policies so the points system as I said is not only to normalise the security policy sanction but also to monitor the behaviour so action for the monitoring will be also be relevant an evident after analysing the data of user behaviour so when you have the weight averages and everything a CAO and CASO will be able to see from the different users behaviours what is wrong of a particular element of the policy and what is the total behaviours of particular user compare to other users, so there is value also in analysing an behaviour in these terms and I think it make a lot of sense some graphs are well presented in MATLAB.

Q5-To what extent do you feel the simulation have provided a robust validation of the approach?

I think I was quite appropriate, so for this kind of model the way you present the simulation and how it works it is explain the model and I can easily relate what you are trying to say in the theoretical description of the model so I think the simulation idea a good job in descripting the model and giving an idea about how it is work in realty.

Q6-How realisable/attainable/possible do you feel this system is?

So, as I mentioned before I think it depends on what kind of business this will applied in, so if you a large organisation with some kinds of resources I think it can work. There is an organisation aspect that you know need to have champions for this kind of particular idea so users not be scared, they do not afraid of making mistakes, and it can easily go wrong with this kind of system because if you have new employee not properly trained or they make mistake they might be inadvertently performing policy violations. It is theoretically feasible but it all down to the configuration in an organisation.

Q7-To what extent do you think having the proposed model can assist organisations in monitoring and measuring users' behaviour with each element of the security policy in a dynamic way?

For each element of the policies drill down and see what is considering normal behaviour from the perspective of user not from the perspective of the policy because whole idea is to create some sort of common understand if policy dictate A and everybody is very much doing B then there is a gap between what a policy says and what people are doing now a CAO and CASO will need to evaluate find a medal grand between A and B. I think there is a lot of

value in that and there is a lot of potential as I said drilling down in each element of the security policy.

Q8-What do you feel are the strengths & weaknesses of the developed system and any barriers using such a system?

So yeah I think we have to do first with organisations resources, how easy going to set up this kind of system because the system works based on the input that it has from different levels of violations and policy compliance, how easy for it to monitor you, the different levels that will have input about users' behaviours so that one thing. The second things is there is an origination element when it come to the a CAO and CASO there position in an organisation and how they going to promote this as a tool that is not going to be perceived as a threat by the employees this is a major issue. Because right now you have all this kind of intrusion detection, intrusion prevention, monitoring systems other systems, these systems are profiling users but perhaps if you doing it in nonintrusive way the user does not about it, in the points system the user will know about it because the system will generate messages and warning an escalations levels is like driving licenses. Organisations structure or business, if you talking about military organisation or government organisation that concern with security I do not thing there will be an issue I think it will be welcome. But it's a very interesting model and I would be interested to see it applied in a real origination and it would be amazing.

A6- Dr. Malcolm Pattinson,

He is a Research Fellow in the Business School of the University of Adelaide and an Information Security Consultant. He has been lecturing and researching in the area of information security for more than 20 years. His current research focuses on the human aspects of information security and he is widely published in this area. He has been an active member of the Adelaide Chapter of ISACA for more than 15 years and has the certifications CISA, CISM and CGEIT. He is also a Member IFIP TC-11 Working Group 11.12, Human Aspects of Information Security & Assurance (HAISA).

Q1- What are your thoughts of the identified research problem?

Problem of non-compliance, this is a big problem, my research all about it. So, it is very important problem, it is not being studied very much, it normally requires the use of psychologist which I have in my team. So, we need to look to behavior knowledge and attitude.

Q2-How realisable/attainable/feasible do you feel this model is at the operational level?

I have some problems with the model. There are some problems of definitions, in video you talked about awareness of security policy, you need to changed it to be awareness of how to behave with a security policy, because the policy tells how to behave so just change the ward. It is important to deal the users awareness of how to behave. We look to 2 aspects of how to behave, psychology and knowledge of how to behave. How to behave can be measured by knowledge and attitude.

Q3-What do you think about utilising the concept of response taxonomy for non-compliance behaviour in enhancing users' compliance?

It is ok but some much behaviour cannot capture by software. There may be an ethical issue with the monitoring process. The problem will be with the accuracy of the result of monitoring. I think the best that we can do is self-recording behaviour, mechanism is by using surveys to see how users behave. The concept is fine if you could record or capture all behaviours.

Q4-What do you think about utilising the concept of compliance points system to monitor the compliance levels to gain insight on users' behaviour and Implemented information security policies?

The points system is a weighing system I think you weight things. I believe that the points system may be not practical, because users do not wish to be rated points and users do not like to compared with others so I think it will be difficult implement it.

Q5-To what extent do you feel the simulation have provided a robust validation of the approach?

I think you did well with your simulation and the picture was clear by the software that you have implemented. So, the tool has visualised your concept.

Q6-How realisable/attainable/possible do you feel this system is?

I would be feasible.

Q7-To what extent do you think having the proposed model can assist organisations in monitoring and measuring users' behaviour with each element of the security policy in a dynamic way?

It will be useful but users may do not like been monitored or compared e.g. sinner mangers, I think if this concept is implemented, the monitoring should be underneath.

Q8-What do you feel are the strengths & weaknesses of the developed system and any barriers using such a system?

Strengths, you are aware that human behaviour is key, you have research a very important problem and having a solution. Weaknesses, I think it may be difficult to be implemented in some organisations.

A7-Dr. Nader Sohrabi Safa

He received his PhD from Faculty of Computer Science and Information Technology, Information System Department, University of Malaya. He is a member of IFIP TC 11 Working Group 12. He also is a member of committee in several annual conferences and reviewer in several journals. His research interest is in the domain of human interaction with systems and human aspects of information security. Also his research focuses on Human

Aspects of Information Security in Organizations in postdoctoral study. Nader currently is working lecturer at University of Warwick UK.

Meeting held over Skype on 01/03/2017 at 9:00 am

Q1- What are your thoughts of the identified research problem?

Research problem most probably is about complying with organizational policies and procedures and it is a valid problem so many organizations are facing this problem of the noncompliant users. I think the insider threat exists and needs more attention to be paid in finding effective solutions to mitigate it.

Q2-How realisable/attainable/feasible do you feel this model is at the operational level?

In terms of operational level, the part that you collect data is important, if you can find a real data is very good but I know that it is very hard to find and collect a real data for its moment is acceptable is that it is simulated because I can understand you have restricted time for your research you cannot spent 10 years for your PhD and it is logical to simulate this part but always we should consider that if we can have real data is better but in this level as what you have in your project is acceptable.

Q3-What do you think about utilising the concept of response taxonomy for non-compliance behaviour in enhancing users' compliance?

I can understand in this system you consider a points based system, if users comply the system increase points and if they do not comply they lose points. And these points can be like an alarm for them that when they lose a lot of points it means that their behaviour is not good they do not comply but when they earn more points it is mean their behaviour is acceptable and is good, I think this approach is good and it can change behaviour.

Q4-What do you think about utilising the concept of compliance points system to monitor the compliance levels in order to gain insight on users' behaviour and Implemented information security policies?

If you empirically and really can use this approach in an organisation is good, as I told you when they lose points it shows that their behaviour is not good and when they earn points it means that their behaviour is good, but you should think how empirically you can run it in an organisation, how you want to controls really their behaviour, maybe this is an important challenge in your research that empirically how you want to run or use this approach in an organisation and really control their behaviour. However, overall is acceptable and it is a useful approach.

Q5-To what extent do you feel the simulation have provided a robust validation of the approach?

As I told you experts advise us to use real data but sometimes is not possible to use a real data so a simulation approach can help in this situation. However, you should think how you can near this data to the real data. For example, if I tell you, your data is not close to real data

what is your answer to me? (I answered him). If you can consider one or two of these data from real data, it increases the validity of your research, maybe you can say the changing passwords data is a real data that I collected from somewhere, mix it with real data, maybe if you can, but if you cannot, it is okay. Do you understand what I mean? this increase reliability, this just a suggestion but overall is acceptable I ask you a question that reviewer or examiner maybe aske you later.

Q6-How realisable/attainable/possible do you feel this system is?

Somehow is realisable, attainable and possible. Possibility is high we can consider points based system and control behaviour. you should discuss and justify this part in your thesis in your defence, possibility is high, attainability is also high, you can develop such a system is attainable.

Q7-To what extent do you think having the proposed model can assist organisations in monitoring and measuring users' behaviour with each element of the security policy in a dynamic way?

I give you a score between medium and high. If we consider 3 levels low, medium and high.

Q8-What do you feel are the particular strengths & weaknesses of the developed system and any barriers using such a system?

The most challenge I think is how to monitor uses behaviour, but I think it is not impossible to do so. The positive aspect is that you presented an approach that can measure compliance and you can give them a points, this is important when we can measure it then we can control it and improve it and this is strengths aspect of your model. I think the weaknesses of your model is that some of security policies are difficult to measure or to get input about users' behaviours but some of policies are easy to monitor.

Practitioners:

P1-Sofoklis Kotsaris:

He is an information security professional, focused on the areas of risk analysis, threat assessment, cyber security and compliance, security policies development, security awareness and advanced security solutions implementation. Sofokils is a senior information security consultant and risk management consultant at PwC Belgium. Before that he was an information security consultant at PwC Greece. He has a master's degree in information security from Glamorgan University, UK. Sofokils has several industry recognised certifications including certified Information Systems Security Professional (CISSP), Certified Information Security Management Systems (ISMS) Lead Auditor, Certified Information Systems Auditor (CISA), COBIT 5 Foundation.

Meeting held over Skype on 21/02/2017 at 11 am (27 mins).

In the beginning he said:

It looks very interesting, very complete and everything. My only concern is regarding the violations, who inside a company will report this kind of violations, most of the time employees do not follow the existing policies so from my experience the hardest and tricky part is the reporting of these violations. If you have those violations, may be if you have monitoring tools and how you can have those violations, if you have this input, then yes it is a very nice model to measure the compliance and of course the user behaviour as you said in your conclusion.

Q1- What are your thoughts of the identified research problem?

I think is a common issue for every company. It is a bout user awareness in the end, anything you can enforce compliance somehow.

Q2-How realisable/attainable/feasible do you feel this model is at the operational level?

I think it is feasible but the hardest part will the reporting of non-compliance with the policies. How can you identify the violations first and if you identify them how do you report them?

Q3-What do you think about utilising the concept of response taxonomy for non-compliance behaviour in enhancing users' compliance?

I think it make sense because it focuses on targeted response.

Q4-What do you think about utilising the concept of compliance points system to monitor the compliance levels in order to gain insight on users' behaviour and Implemented information security policies?

I would be very useful, it is like the benefits true/false because you monitor users' behaviours and you can see the status of each of policy, and may be if you identify certain gap, you can change some part or customise it in order to make it more applicable to your business environment.

Q5-To what extent do you feel the simulation have provided a robust validation of the approach?

The simulation was okay, very practical and very clear.

Q6-How realisable/attainable/possible do you feel this system is?

I think it is feasible but the biggest problem would be identification of the non-compliance with the policies, how do you identify or trigger these kind of non-compliance with the policies. This my concern because I am not talking about technical, or using tools for monitoring but some policies I difficult to monitor for example clear desk policy, how you are going to monitor that, you need someone there to check everybody. It depends on an organisation size and available resources; I thank this is the big problem but beside that I think the model can work.

Q7-To what extent do you think having the proposed model can assist organisations in monitoring and measuring users' behaviour with each element of the security policy in a dynamic way?

I think you can provide a lot of input on how applicable it is policy can be to the company, so if certain policy not followed then some wrong is there.

Q8-What do you feel are the particular strengths & weaknesses of the developed system and any barriers using such a system?

The barriers I told you before how you identify the non-compliance behaviour or the users' violations. The strength I think is about your last comments, on the video, that you can have an input view on your employees' behaviour or users' behaviour and then on effectiveness of your existing policies.

P2- Mamdoh Alzhrani:

Mamdoh is information security expert in Cyber Risk Management and Strategic Analysis with over 14 years of experience in diverse technical, senior management advisory and consultancy positions. He is currently working at the National Commercial Bank in KSA as a senior information security officer. He gained a MSc degree in computer system security at University of south wales (UK). Mamdoh has several industry recognised certifications including Certified Ethical Hacker (CEH), Certified Security +, GIAC Certified Incident Handler (GCIH), Certified Information Security Manager (CISM), GIAC Continuous Monitoring Certification (GMON).

Meeting held over Skype on 21/02/2017 at 2 pm

Q1- What are your thoughts of the identified research problem?

I think is an authentic idea, I have not seen any idea like this in the field, I have been work in the field for many years and I have not seen any technology that is doing the same. I have face nothing similar to this idea that will measure the compliance of users based on a defined set of policy.

Q2-How realisable/attainable/feasible do you feel this model is at the operational level?

It is very realisable and very feasible and the application in real word will be fantastic to be applied in a group set of users, I would say it would be a challenging to apply this model on a user based but if you can take the result of the compliance status of group of users and then start looking at each group behaviour or compliance rate, it will be fantastic. For example, if I am the security in an organisation and I want to measure how effective is my awareness and how effective is my policies that I already introduced and my pervious marketing of information security among multiple sections of the organisation that am working on, for example, you will have HR department and legal department so the policy should measure the users inside HR and the users inside legal and then I could be presented to executive level or manager level saying this how HR compliance this how legal compliance so the end result

will be some sort of one result or dashboard or graph showing and explaining how the group as an overall behaving and to what extent they are complying the security policies that I enforced.

Q3-What do you think about utilising the concept of response taxonomy for non-compliance behaviour in enhancing users' compliance?

It seems very logical, very acceptable to some extent, from my experience in the field it will challenging to some extent because users do not like the fact that they are being highlighted as red or yellow or any colour, I would think there would be a better approach to link whatever they doing in terms of the policy violation to certain threats e.g. if a user is doing a certain behaviour like a visiting bad website, there should be some sort of awareness message telling him if you do this you could compromise the whole organisation and you can like it the certain threats like for example in Saudi nowadays we have Shimon, we can say visiting similar website can led the organisation to be impacted by virus like Shimon this is an example but in general I would yes especially it categorise in two types, it will drive users to comply.

Q4-What do you think about utilising the concept of compliance points system to monitor the compliance levels in order to gain insight on users' behaviour and Implemented information security policies?

It is a fantastic system. I think it will provide so much value for group HR for executive level on to what extent each department, each group or each section is in compliance to the information security policies.

Q5-To what extent do you feel the simulation have provided a robust validation of the approach?

It is very robust; I think it shows clearly what the compliance system will look like. It might need some enhancement in terms of the interface if this product will be some sort of production somewhat in future.

Q6-How realisable/attainable/possible do you feel this system is?

I think it is very realisable but would need some sort of policy testing to which extent the policy is robust the system will do. It based on the policy that you trying to measure so I think the system should be used in places where the policies are mature enough where the people who are using the system are aware of what you are trying to measure.

Q7-To what extent do you think having the proposed model can assist organisations in monitoring and measuring users' behaviour with each element of the security policy in a dynamic way?

I think it is very useful. If I have a product now that providing the same system I would not hesitate to use it as long as it is simple, not providing more complex situation in my

organisation I would use it immediately. I think it would be a good idea if you propose this model to security venders.

Q8-What do you feel are the particular strengths & weaknesses of the developed system and any barriers using such a system?

I believe the weaknesses would be in the contents side, so if you know what type of policy that you are measuring, you will have a fantastic type of a system that measure a compliance for departments/groups. I think whoever implement this system will face a challenge in following and comparing user to user but if this was switched somehow to be based on group evaluation or group comparison based on collected points and based on the compliance points it will be a fantastic because at the end of the day in business as usual we do this type of comparison and we do try to look for some sort of evaluation for each department to what extent they are compliant to our information security so I would say the weaknesses would be in the policy side. The strengths you can develop this system to measure group to group or department to department performance in terms of information security policy compliance it would provide huge and effective type of output and results to highlights where are the areas or departments that need more focus or more enhancement, more security awareness, more security training, more attention from the information security side. However, still doing this system on user to user it will be challenging because most of organisations have a lot of users but if you start applying this on groups or department, the results will be amazing.

P3-Mr John Finch:

John Finch is the Information governance manager for Plymouth City Council, responsible for Data protection, security policy development and management, managing the Information Asset Register managing security incidents, providing security advice for the Council and partners, providing security awareness education for senior management. Previously, John spent 7 years in a technical security role, as IT Security manager for Plymouth City Council, managing the compliance of the Council network and technical breaches. John has been chair of several regional security forums, including the SW WARP and Devon Information Security partnership, and has been a conference speaker at National Information Security conference in 2008 and 2010. He was involved with the delivery of the IA guidelines for the Public Services Network delivered by the cabinet office. John is a current CISSP, and undertook an IT master's degree at Plymouth University in 2001, with a thesis in Approaches to establishing IT security culture.

Meeting held in person on 03/03/2017 at 2pm

The concept theoretically is good, technically many terms, one it will not solve a problem here and will need factor in the human element, for example, in our organisation obviously, security is a very important thing but we have things a lot down and technical control enforced and other things which may affect by security we have got other measurements, some of them performance measure. In theory, it is an interesting model, in its own, it will be

very hard to implement in practical sense. Purely, because of the politics, relying on technical rather than character monitoring and it is potentially trying to solve an issue we can identify in other ways.

Q1- What are your thoughts of the identified research problem?

As just I said, it is, we do view this is a problem, the behaviours that not been secure will materialise in other aspects if someone is work…….good concept, in reality implementing this will be nearly impossible, in my organisation maybe others it could but here not.

Q2-How realisable/attainable/feasible do you feel this model is at the operational level?

It may be difficult, because it is too generic, but the whole is points scoring, it is not the one that people enjoy, to see that been marked on just behaviour etc. We do other ways of managing people behaviours and it is more by understanding what the landscape of threats.

Q3-What do you think about utilising the concept of response taxonomy for non-compliance behaviour in enhancing users' compliance?

I do like the idea of identifying behaviours, I think this model would be very very useful if you took human elements out (I asked him what you mean here by human element). Here you are monitoring the behaviours of humans, you have got emotions and others factors in the large which affect it. If this model is monitoring for example a behaviour of a computer identified, yes it does have standard applications in store for whatever reason, patches missing, vulnerabilities is reported on that etc. Reporting totally on objective basis on computer that would be more palatable.

Q4-What do you think about utilising the concept of compliance points system to monitor the compliance levels in order to gain insight on users' behaviour and Implemented information security policies?

Difficult to implement, the whole concept that someone is being marked on his behaviour does not go down well especially in this organisation. People may not like the points scoring and they view it in different ways and they can view it very negative.

Q5-To what extent do you feel the simulation have provided a robust validation of the approach?

Very good the simulation, was very good, the concept is very impressive and the work that put in is very palatable.

Q6-How realisable/attainable/possible do you feel this system is?

It is possible theoretically, purely, because of all the human element and politics we would have to do, for example, we can buy policy system, tell the people what the security is and what healthy and safety policy is, we purchase that about 10 ago never implemented it, because of the politics and just telling people what policy is, because there is fact such as ok so what happens is somebody does not click on, what action do we take but there maybe

other underlining factors never got implemented. It can help us but implementing such a monitoring system on users' behaviours politician would not accept that. Also, another factor is to install something like this in a corporate environment there is a cost, because we have to pay for IT services.

Q7-To what extent do you think having the proposed model can assist organisations in monitoring and measuring users' behaviour with each element of the security policy in a dynamic way?

Yes, it does monitor the compliance in a very efficient way but need to consider others factors into, which does do affect person behaviour. it is like the speed camera, if you go pass a speed camera at 30, you get a ticket regardless. If you go pass a speed camera 50 because had an injury and you need a medical treatment, you still get a ticket.

Q8-What do you feel are the particular strengths & weaknesses of the developed system and any barriers using such a system?

The barriers will be human elements, politics, and people do not like being monitored to this extent and many organizations looking to ward an output based working scenarios so staff monitored what they produced at the end of the day. As I said that concept of monitoring behaviour if applied to a computer itself so you can identify these computers with a higher security risk this concept is wanted. We do recognise human element is a big risk area but humans got feelings.

Strengths, very well developed, it does got a lot of details and analysis and it is consistent. But in reality, it may challanging be consistent because People have to be treated differently depending on their rule in the organisation, our politicians, senior managers they should have to get special treatment.

P4-Usman Quresh,

He is currently working at Shared Services Connected Ltd, UK as a test tanager. He is an experienced IT Contractor with over fifteen years' commercial experience with over nine years in testing. Also, he was an incident management analyst at SQS grump, London, UK He gained his MSc degree in computer forensics, information security, from the University of Bradford in 2009.

Q1- What are your thoughts of the identified research problem?

Security is a concern of all organizations in this era of rapid advancement in Information Technology. Based on this concern almost every organization puts in place a security policy. And as identified the biggest challenge is to implement those policies, and very correctly pointed in the presentation are the causes i.e. negligent, unaware or naïve behaviour towards security. Malicious intent is something which I don't think can be as much covered by policies, as by implementing the correct procedures.

Q2-How realisable/attainable/feasible do you feel this model is at the operational level?

I think it is very realisable. It is in human nature that unless there is a reward for doing something or a fear of not doing something, it loses interest very soon. The model described in the presentation offers two benefits. First of all a very good monitoring tool which can be used by organizations to keep a check on its employees for compliance or non-compliance to the organizational policies, and secondly this can be used as a way or rewarding and punishing employees accordingly.

Q3-What do you think about utilising the concept of response taxonomy for non-compliance behaviour in enhancing users' compliance?

Based on the point explained above, this model can be used to create a fear of being noticed as a noncompliant user and being watched for any noncompliant. This will encourage users to be more vigilant in terms of security policies and move from being noncompliant to compliance

Q4-What do you think about utilising the concept of compliance points system to monitor the compliance levels in order to gain insight on users' behaviour and Implemented information security policies?

In addition to the positive uses of compliance points system mentioned above. The model can also be used by large organization by utilizing collected data for a longer period of time to create user groups based on different profiles. Then different groups can be put under observations based on their levels.

Q5-To what extent do you feel the simulation have provided a robust validation of the approach?

I think the simulation provided a good overall approach, explaining different aspects of security monitoring and auditing alongside a mechanism of incentivising users to be more compliant. But I would be better if technical details are included which details the actual process of monitoring of the security policies. i.e. explaining how and where the security policies will be added within the system and how each newly added policy will be monitored.

Q6-How realisable/attainable/possible do you feel this system is?

How feasible a system will be for an organization will depends on a number of things.

a- Organizational policies on monitoring user activates.
b- Determining cost of investment & its return
c- Life cycle of the system

So, the proposed system even being very robust & arcuate will have to exhibit the return on investment to be significant enough, in order to convince higher management to invest in it. I suggest to perform a proof of concept on the system, which will further help improve the system.

Q7-To what extent do you think having the proposed model can assist organisations in monitoring and measuring users' behaviour with each element of the security policy in a dynamic way?

I am sure that the proposed model can help organisations performing regular audits on its security policies. But the only thing missing in the presentation is that it fails to explain how this monitoring will be done i.e. how will the proposed system know if a user has downloaded prohibited material? How system records failed login attempts?

Q8-What do you feel are the particular strengths & weaknesses of the developed system and any barriers using such a system?

Even though the presentation provides an overview of the proposed system for monitoring and rewarding users, which will help users moving from non-compliance to a more compliance approach to security policies. The presentation is lacking any technical details cost & performance impact. What will happen if a large organization has a large number of security policies and a very large number of users and the main business of organization largely depends on the performance of its infrastructure? It would be better if a proof of concept is done on this system and then based on that, there should be optimum use requirements i.e. The system will have minium to no impact on the performance of the organizational infrastructure if the number of policies is not more than XXX and number of users at any given time not more than XXXX

Strengths: If implemented in a manor it is presented, the system provides an in depth data for analysis. Which can certainly point out the potential security holes with in an organization at user level. In other words can be used as a good security audit tool.

Weaknesses: The only weakness I can think of is the impact of the system on the overall performance of the organizational infrastructure. More checks you will have put in more burden it will put on the infrastructure. i.e. every time user performs a task that gets validated against rules, then obviously, it will have an impact on the overall performance.

P5- Dr. Georgios Magklaras:

He is a computer scientist working as a Senior Computer Systems Engineer at the University of Oslo, in Norway. He is an information security researcher and developed methods in the field of insider IT misuse detection and prediction. He is also an active systems administrator information security consultant and Information Technology practitioner working with High Performance Computing. His research was initially concerned with ways to classify computer security incident management responses. However, his attention was drawn to the problem of misuse detection. Magklaras developed one of the first methods to systematize the misuse detection and misuse prediction techniques. Prior working at the University of Oslo, Magklaras has worked in various technical and scientific positions for a number of companies and organizations, including those of Sequent Computer Systems, Boeing and IBM UK. He has held a number of professional affiliations, including those of an IEEE affiliate member, USENIX, SAGE/LOPSA and Red Hat Certified Engineer. He has held the position of Secretary (since 2005) and Chair (since 2010) of the Technical Management Project Committee of the EMBnet organization.

Meeting held over Skype on 21/02/2017 at 11 am (60 mins).

In the beginning he said:

The concept is really interesting because in an essence what really is left to me is that you are trying to make a model to visualize compliance and non-compliance and this actually a useful thing for organizations. I am overall positive to the idea. However, I have many points about your presentation. The first impression that I have is that you are making a formwork that presumes a certain organization or structure in a certain size of organizations e.g. you assumed that there is line manger you assumed the need to escalate things but what about, for example, smaller organisations where the hierarchy is more flat let say a company of 10 people how could your model work there and there are many of them. Am I right in assuming that your model actually assumes a certain organisation hierarchy, right, an organisation of certain size. Ok that is fine. There is an important issue that is the time dimension of your model so obviously the idea you trying to give is that at least with the way you visualise the results in Matlab is that more navigation over a certain period of time being that week months whatever your position into the model, the worst user am I right, well, that an interesting way of looking at it but let me give you an example where this would flag at least in our organisation we are also a large organisation in The University of Oslo, we have around 50,000 users, in our own systems what we do to judge the severity or the point where we actually need to escalate or cut some body account is not the repeated occurs of an event that we weighted and we give weight we just flag the event, so for example it okay for us for someone to download illegal content and we can flag that over time , but for other certain things for example sharing or releasing certain bits of information via web service that would actually mean flag and we do no care if it a user does it once or twice or three times over time if he does it once then we take him off. So you really need to think a bit about that because I know that over time, time is very important component in a model obviously you have your points system there, which has a logic but for certain things that does not work because the severity of some violations.

Q1- What are your thoughts of the identified research problem?

Yes, you set out problem, which is clearly identifiable, for example how to measure a compliance, I mean it is an important problem not everybody has a clear picture of what compliance is people talk about security policies but they do not actually have a model description of how or what does it mean mathematically or scholastically to be compliant, which you are trying to do and how to visualize that for the purposes of identifying threats, so I thank the way you identified the problem domain is adequate.

Q2-How realisable/attainable/feasible do you feel this model is at the operational level?

When you make a model, this what I told you earlier, the answer is depends on the type matrix that you are going to use, for example as I mention earlier, in practice it will not be feasible to choose matrix of the type email behaviour or contents or webpage content ok this is not only due to user privacy concerns but this is also a problem when comes to the wealth of date collection that you’re going to use, another weakens of your model from an

operational point of view is that it assumes the presence of a central account infrastructure whether is that LDAP or Active directory or whatever, this may be true for many organisations but there are many organisations that they do not have that, they have for example a less connection of devices, like for example a taxi company that has terminals on the taxi mobile terminals they do not necessarily have a central redis authentication server or an active directory server so that you can monitor things from user data base, the way we saw this with one is that we actually put every things that we got into a central DB and then try to make sense of the date there by means of clients server software but you operationally if you want monitoring all this things for let say a large organisation you can have a serious big date issue there, you can for example monitor all the network connection in the large organisation, you can monitor all the email traffic, they could be thousands of emails per day outside the user privacy concern, but you could monitor other things for example you could monitor what kind of devices connect? what open ports these devices have, collectively, from a router what are the top traffic destinations? Are they Tornado sites, or others websites for example Nefarious website, these are the sort of things that you actually can collect from a central point. If you are actually considering for example I saw your example a policy of the type how quickly someone locks the screen if you try to do that on a large organisation, that can be a headache, I am talking operations now. So when you are trying to make a monitoring infrastructure, which is vital, because it has to feed your model with data, you should not understate the overhead of the monitoring process. So in a way I am not saying that your model is not viable what I am saying is that it will be viable depending on how you feed the data into it and what kind of data you feed into it.

Q3-What do you think about utilising the concept of response taxonomy for non-compliance behaviour in enhancing users' compliance?

Q4-What do you think about utilising the concept of compliance points system to monitor the compliance levels in order to gain insight on users' behaviour and Implemented information security policies?

I think it is an interested approach, I think the points you right rewarding users with more points that are trying to comply a compliant user, compliant category, but again you that serious to reconsider the time dimension, because for example the time dimension will keep rewarding incrementally more points to a user that is you know he is really nice person, he is fully compliant but the question here for many organisations is to actually detect the non-compliance so in a way yes there is a human aspect of rewarding people that are following the law but technically here your main objective is actually to detect and visualise the people that did not follow the law and in such sense really people might question your points system for example incrementing points over a number of time to compliant users. For me another approach would be to set a compliance threshold and say if you have a certain number of points there whether you do it over let's say over one week or one month you are compliant in the fact that you have for example 60 compliance over 6 months or 20 compliance points over 2 months if you have not done some anything else does not add any meaning, ok you either compliant or noncompliant so but again weighting negatively things like for example

certain things that read flags so your score has a meaning for non-compliance people has some sense.

Q5-To what extent do you feel the simulation have provided a robust validation of the approach?

The matrix is good, the way for example you choose your tabular data in the way you actually have dimensioned the result and the security policies in MATLAB is good it adds sense, but either if you want to validate data model you using the world validation you need to have a much more complex scenario of users that are have ups and downs I think this is because your present things like User A with a sense and people that are really bad like user D and E etc. what I feel you need to show to add some validity and again I understand this data are theatrical they are not actual data is people are in between in more examples or how someone goes from the non-compliance to compliance inversion. I think this would actually add to the theoretical validation of the model.

Q6-How realisable/attainable/possible do you feel this system is?

As I said, I think it is a very interesting system provided that you pick up with the right data. I think it is viable what I do like about the system form an operation point of view and a research point of view you have basis to visualise things, ok, which is in the world of research and operations like for example in depth in your presentation where actually you have compliance points on policy element and you show the graph what actually the optimal and how the user is deviate, I think this is a very interesting concept it has a good basis, however, the viability of the approach comes when you put things into practice for example when I first deployed my system beyond the research prototype into a real world system people it took me one year to really fix things or user to be happy and make sense of the date, ok, so what I am trying to say to you is that you can make more data when comes to theatrical end use of showing how your model actually in simulated mode would comply with marginal users. This is the value of the research but the viability of this system can only be judge if for example your mange to generates some data and replay these scenario or different scenarios over a model and show how the way you visualise this results and display the score over let's say 20 users not only five can make or break the difference if someone saying I used tool I need to pick this user to enforce the policy and this tool help me to do that , I mean as a research I appreciate what you are trying to do, but in the real world if you show this lets say an operational person or an information security officer that actually a manger he going say to you please explain to me how should I read this graphs over the data to generate clear suggestions on which user to target, so what you doing here is introducing the many dimensions of the problem you have aspects of visualising and modelling I have not seen your equations, you do not show your equations in the presentation you mentioning to some equations because this is very important for the model , so but from what I can see from the short presentation like the 5 or 6 mins in MATLAP simulation this is what I can tell you. This is work that should really continue in that you should really weight more with some actual data if possible I do not know what Steve and Nathan say about that or whether if you have other projects in the research group right now that can assist you in this, but one thing

that you can do from day one is add more users that are actually are marginal the walk between compliance and non-compliance because this is what happens in the real world, in the real world we do not have only good and bad people, we have people that are good, and thy are not complying at a certain point, whether intentional or unintentional does not matter but you have users fluctuating between what acceptable and not acceptable everyone knows that in the real world from empirical experience.

Q7-To what extent do you think having the proposed model can assist organisations in monitoring and measuring users' behaviour with each element of the security policy in a dynamic way?

In a dynamic way, yes actually is quite good. In the sense that you show a gin behaviours and compliance deviations over time so from that perspective I thinks it is good but aging going to the viability that I mention early am not going to repeat that.

Q8-What do you feel are the particular strengths & weaknesses of the developed system and any barriers using such a system?

.The weakness is essentially the fact that you cannot, it depends on the matrix that you use for example things in the real word like user privacy concern, monitoring implementation headache with big date and trying to get data from central point these are I will not call it weakness for the model but threats for its viability, so for example you should make a model that a relies less on things for example email traffic or the content of webpages or what a user downloads why do not you monitor from a router what sort of web sites are visited collectively by an organisation, many organisations do that and they have a right to do so as part of engaging with threats on network but they do not have the right to go down to individual workstations or phones of users and collect the data there. Another important point that I would like to say I would be interesting to see how your model will visualise the results again if you put effort to produce a matrix that you can collect easily, and produce meaning by MATLAB in your tabular data form meaningful graphs this is strength of your model and show what is the value of dynamically watching a user going from compliance to non-compliance and back to compliance and monitoring deciding what to do enforcing or not to enforcing compliance by using the graph.

P6-Nick Sharratt:

He is an enterprise security architect at Plymouth university. Sharrat Sibt gained his BSc in Computer Science from Aston University in 1991. He has more than 20-year of experience in the field of information security and systems management.

It is an interesting video and idea. I like the idea.

Q1- What are your thoughts of the identified research problem?

The identified research problem, it is an open issue; it certainly exists because trying to identify patterns of behaviour and where to priorities attention and how to deal with it

properly, it is certainly a challenge and this will give a mechanism to deal with that, I am not aware if somebody done the same sort of thing.

Q2-How realisable/attainable/feasible do you feel this model is at the operational level?

Depending on having access on the rule behavioural information we track back to the user other than that it is perfectly doable and there is key thing you seem to have it in there e.g clear desk policy which would obviously need mangers and other people to be recording a non-compliance and things which might be seen as too much of an overhead the people to take on but it will come down to policy and the individual things that seen is important to comply with in an organisation. I think it could be done it can be tweak in terms of things what need to be recorded and what you can detect so the principle is definitely doable, the details of what you record would be the challenge.

Q3-What do you think about utilising the concept of response taxonomy for non-compliance behaviour in enhancing users' compliance?

I think it is good one, using the time dimensions or time elements on it was a great idea and it makes complete sense.

Q4-What do you think about utilising the concept of compliance points system to monitor the compliance levels in order to gain insight on users' behaviour and Implemented information security policies?

I really like the idea of presenting the trends over time and see both individuals and aggregate level pictures of how people are complying, I thought that was a useful metric.

Q5-To what extent do you feel the simulation have provided a robust validation of the approach?

It was tricky to understand exactly from the video how your simulation is run. It appears to be you look at two extremes, the complete compliant and the worst one, but I think you possibly can do with a bit modelling around more realistic behaviour, the sort of in between states, certainly the extremes you have modelled are important but I think possible you may look to more scenarios, when you have a lot of users around the middle do you still get useful pictures from it.

Q6-How realisable/attainable/possible do you feel this system is?

I think it is definitely doable, there was nothing I thought that it was impossible

Q7-To what extent do you think having the proposed model can assist organisations in monitoring and measuring users' behaviour with each element of the security policy in a dynamic way?

Your system model approach gives individuals reporting you can set metric on those and you can get exception reports out of it if trends going on wrong direction you can drilling to that

to get down into individuals and you can measure the successive targeted action on trends over times, yah it looks like a good approach to do that.

Q8-What do you feel are the particular strengths & weaknesses of the developed system and any barriers using such a system?

As a bit I do not see this before, it may be there but I do not come across with the idea of time metric, and particularly the breaking thing down if it has been a part of the same incident or being forgiven a new thing if it is in certain period of time and things and automating that time impact on users score of compliance seem really very powerful idea. In terms of the automated escalation. It very dependent on some indication of compliance or not and some of the policies that not necessary going to be possible to be automated so if you rely on humans inputting information into the system about compliance or not then it got potential weakness there but again that is down to the individuals choose to policies and things you need prioritise and to look at in a systematically approach so it may be applicable in some areas than others and some policies and things than others.

P7- Saud Al-otaibi:

He is an IT professional with 15+ years in the field of information security. He is currently working as a cyber security advisory at KPMG Saudi. He previously served at Saudi Telecom Company (STC) as monitoring supervisor in security operation centre which handling & investigate all security incident that reporting from multiple security systems such as: firewalls, IDS, IPS, from 2004 till 2008. Also he worked at Alinma Bank as manager of security infrastructure from 2008 till 2012. Saud has several industry recognised certifications including Certified Information Systems Security Professional (CISSP), Certified in Project Management Professional (PMP), Certified Ethical Hacker (CEH), Certified EC-Council Certified Security Analyst (ECSA), Certified ArcSight Certified Security Analyst (ACSA), Certified in IT Infrastructure Library (ITIL).

Meeting held over Skype on 17/02/2017 at 4 pm

Q1- What are your thoughts of the identified research problem?

I think the identified research problem is a serious gap in the security framework and common weakness in many organization and infrastructure. In my opinion, find a solution for the selected problem will help the organization to raise the security awareness and that will lead to increase their security profile.

Q2-How realisable/attainable/feasible do you feel this model is at the operational level?

Based on my experience, I found this model applicable and realisable and could implemented in the operation environment specially that the model address two factors: user behaviours & policy effectiveness and against the time dimension. this model will be more affective if it’s integrated with other centralized systems such as active directory and domain controller.

Q3-What do you think about utilising the concept of response taxonomy for non-compliance behaviour in enhancing users' compliance?

I think the current actions and response level is good and will raise the awareness of non-compliance user. However, I suggest to add the training or quiz as one of response taxonomy system. For example: when a user violates the password policy by using a simple password such as 123456. the response taxonomy system will enforce this user to complete an online training about the password policy.

Q4-What do you think about utilising the concept of compliance points system to monitor the compliance levels in order to gain insight on users' behaviour and Implemented information security policies?

This is a very important system and function; it will encourage the users to comply with the pollicises as much as they can.

Q5-To what extent do you feel the simulation have provided a robust validation of the approach?

For me the simulation was very clear and the concept of the system has presented clearly.

Q6-How realisable/attainable/possible do you feel this system is?

We all know that, the human factor is the weaker point in the security domain. The only way to solve this issue is to raise the awareness of users by using a system like this one. If I want to build a secure environment, I will make sure to use this system for all users.

Q7-To what extent do you think having the proposed model can assist organisations in monitoring and measuring users' behaviour with each element of the security policy in a dynamic way?

This facture will help the administrator by saving the time and focus only on the non-compliance policy.

Q8-What do you feel are the particular strengths & weaknesses of the developed system and any barriers using such a system?

Strength: the using of targeted response for users' behaviours, or response taxonomy concept.

Appendix D: Published papers

Journal publication:

1- M. Alotaibi, S. Furnell and N. Clarke, ‘’A Novel Model for Monitoring Security Policy Compliance ‘’, Journal of Internet Technology and Secured Transactions

Conference publication:

1- M. Alotaibi, S. Furnell and N. Clarke, ‘’ Information Security Policies: A Review of Challenges and Influencing Factors ‘’In Internet Technology and Secured Transactions (ICITST), Spain, 2016 11th International Conference for (pp. 352-358). IEEE.

2- M. Alotaibi, S. Furnell and N. Clarke, ‘’ TOWARDS DYNAMIC ADAPTION OF USER'S ORGANISATIONAL INFORMATION SECURITY BEHAVIOUR ‘’ In Australian Information Security Management Conference, Australia, 2015, pp. 28-36