2023

Adaptive Cybersecurity Training Framework for Social Media Risks

Ben Salamah, Fai

UNIVERSITY OF
PLYMOUTH

Adaptive Cybersecurity Training Framework for Social Media Risks

by

Fai M S M E Ben Salamah

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

DOCTOR OF PHILOSOPHY

School of Engineering, Computing, and Mathematics

July 2023

Acknowledgements

This Ph.D. thesis is the outcome of a challenging journey, but at the end of this journey, I found myself a different person.

Many people have contributed to this journey immensely, without which, perhaps, I would not have reached this stage. First and foremost, I express my gratitude and obeisance to Allah – the Almighty for providing me with enough strength and resilience to accomplish this ambitious task. Second, I would like to thank the individuals who supported me immensely. My sincere gratitude will first go to my supervisory team. I would like to express my kind gratitude to Dr. Marco Palomino, the director of studies. "Thank you, for being very supportive and flexible to me." Kind gratitude to Dr. Maria Papadaki also, "Your unwavering support and assistance mean a lot to me". I would also like to take this opportunity to express my appreciation to my other supervisors, Dr. Matthew Craven, and Prof. Steven Furnell, for their valuable assistance and suggestions in completing this thesis.

I wish to forward my heartfelt thanks to my beloved parents, mama Afaf and baba Mostafa for their kindness and abundance of love and support, and to my better half, my husband Mohammed Alrumaih – thank you for being patient and positive with me, your kind words, your love, and your interest in my work has made my dream come true, "I love you." How can I forget my children Jasem, Salah, and Daniah? "I'm grateful that you have been with me throughout the whole thing and have given me so much love, courage, and support, I love you all". My sister-in-law Monera Alrumaih? Thank you for being always with me, "I love you too."

I acknowledge with thanks the government of my country Kuwait, the Civil Service Commission, for granting me the scholarship and sponsoring my undertaking of this Ph.D. programme. Lastly, I would like to thank the University of Plymouth and special thanks to the Doctoral College for their useful guidance and support.

Author's declaration

At no time during the registration for the degree of Doctor of Philosophy has the author been registered for any other University award without prior agreement of the Doctoral College Quality Sub-Committee.Work submitted for this research degree at the University of Plymouth has not formed part of any other degree either at the University of Plymouth or at another establishment.

Word count for the main body of this thesis: **48,732**

Signed: Fai M. Ben Salamah

Date: 28/07/2023

Abstract

Adaptive Cybersecurity Training Framework for Social Media Risks

Fai M S M E Ben Salamah

Social media has become embedded in our everyday lives, personal activities, and the workplace. Thus, educating users on emerging cybersecurity challenges for social media has become imperative. In this project, a systematic literature review (SLR) was conducted and a mix of approach analyses to derive a framework that identifies the activities involved in adapting cybersecurity training for social media risks. I collected answers from 641 Kuwaiti employees in various sectors: education, healthcare, leadership and management, arts, entertainment, the police, and military, and interviewed 25 people who serve as policymakers, cybersecurity trainers, and those who have experienced cybersecurity training before. The study found that a one-fits-all training approach is highly ineffective, as people's understanding and knowledge can vary greatly. Features such as gender, age, educational level, job roles, and the trainees' training preferences and perceptions are essential considerations for developing a robust training system. Additionally, the study found that job role and age constitute the main factors associated with social media cybersecurity risks. The findings reveal that employees working in the business and financial sectors are the riskiest group, as far as cybersecurity is concerned. Female employees are more vulnerable to cyberattacks than male employees, and the youngest employees are the most risk prone, employees with less than two years of experience, and those who are 55 years old or more, need more cybersecurity training, due to their lack of awareness on the subject. This work has led to formulate a risk equation that can assist policymakers and training providers in defining countermeasures against risks and prioritize the training for those who need it the most. The framework and its process were validated through several strategies involving 38 case studies, surveys, and interviews. The novel contribution of this research is the proposal of the framework, which is a high-level, holistic framework that can support and promote organizations in mitigating social media risks.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

This chapter provides an overview of our research study, the problem's background, and the area of study. In this chapter, the study objectives and questions will be reviewed along with the research contributions. The data collection process and the study's methodology will be given at the conclusion.

Being a company's employee requires interacting with coworkers and a challenging cybersecurity environment, because cybersecurity combines human and technological skills to defend against cyberattacks (Suryotrisongko & Musashi, 2019).

Existing literature has yet to do much to address cybersecurity issues and challenges from a human perspective. Standing on technology systems to combat cyberattacks in organizations while ignoring the role of the employees' weaknesses is considered a significant problem in the cybersecurity domain. Organisations should understand that cybersecurity is more than just information technology systems; it also addresses how humans utilise information systems and risky activities that lead to vulnerabilities (Triplett, 2022).

According to the Data Breach Investigations Report (2020) humans play a part in cyber threats. Human weaknesses, social engineering within phishing emails, and intentional misuse were at the top of cyberattack dangers (DBIR, 2020). The Business Crime Survey (BRC, 2015), reported that one of the primary concerns of online fraud between 2014 and 2015 was the growing threat from employees within the organisation, indicating that the vulnerable link in the cybersecurity chain is the human factor (Sasse et al., 2001; Sasse & Flechais, 2005; Nurse et al., 2011; Anwar et al., 2017; Chapple et al., 2021).

Human factors are utilised by cybercriminals to gain unauthorised access, get credentials,

and infect systems with malware (Kadena & Gupi, 2021). However, many businesses continue to think that cybersecurity is a purely technical issue (Dhakal, 2018). Due to this, it is difficult for employees today to have the appropriate level of security awareness (Bada & Nurse, 2019).

Numerous studies have sought to explain and classify the threats posed by hackers to organisational employees. However, organisations confront the need for security-specific scales to evaluate the human perspective on cybersecurity (Rahman et al., 2021). This is due to the need for employees to gain a deeper understanding of their role in data protection, software, and systems, the level of risk associated with the assets, and how their negative online behaviours could place these assets at risk (Hadlington, 2017).

Poor organization-level planning, lack of attention to detail, and ineffective communication play a significant role in this area (Hadlington, 2018). Therefore, it is crucial for businesses to recognize that cybersecurity risk management is an integral component of workplace culture and grows from ongoing activity awareness (Cybersecurity, 2018). According to Haeussinger & Kranz (2017), most organisational incidents are either the direct or indirect result of human errors (Tsokkis & Stavrou, 2018; Jamil et al., 2018). Nevertheless, technical solutions alone are insufficient to address all cybersecurity concerns (Stockhardt et al., 2016). The issue is that while it encourages the finding of personal identity, human behavior is still the weakest link in an information system (Terlizzi, 2019). As a result, cybersecurity researchers concur that awareness is necessary to adapt behavior but regrettably is not always sufficient because behavior change is challenging and requires time (Gjertsen et al., 2017).

On the other hand, social media is a relatively recent phenomenon; however, it is likely to remain here for a long time and further flourish in terms of its use in the days ahead. In fact, social media has become inevitable across all kinds of industries - whether in education or the manufacturing sector. Many social networking sites such as Facebook, LinkedIn, Instagram, and Twitter are being extensively used for communication within and outside the organisation. These platforms have become so important that people, are spending a significant amount of time on messaging and receiving information from each other. Most companies make use of social media platforms for their marketing plans and canvassing their products and services. The point is that social media continues to play a crucial role in a variety of sectors.

It is true that social media has transformed the communication landscape in a significant manner; however, it poses some imminent dangers. Currently, a large proportion of the population across the world is inclined to share information. It is also true that social media can be of great help to meet firms' business objectives, but yet, at the same time, it can also impact organisations negatively if cyber-attacks and cybersecurity threats are not properly understood and remedied effectively. Even after so many years and numerous efforts put in by experts to thwart cyber-attacks, cybercrimes keep occurring and hackers still find a favorable milieu to attack.

This study aims to find how and why an adaptable social media cybersecurity training system is sufficient to raise awareness and enhance each employee's learning environment. This process is known as customized learning. The customized approach is a methodical approach to knowledge that focuses on personalizing learning to match learners' abilities, preferences, needs, and purposes while retaining access to fields requiring 21st-century skills (Walkington & Bernacki, 2020). Customizing learning is therefore a broad tool to change current knowledge paradigms.

1.1 Background to the problem

Social media is based on the notion of community and relationships. As such, the very nature of social media expects users to trust in each other and interact. Unfortunately, uncontrolled trust and incautions interaction may lead to vulnerabilities, which are often exploited by hackers (Aldawood & Skinner, 2019; European Network and Information Security Agency (ENISA), 2019). As time passes by, and technology progresses, hackers are likely to employ more and more advanced techniques and make their attacks harder to manage and prevent (European Network and Information Security Agency (ENISA), 2010)—fool proof protection is unlikely to be available any time soon (Alshaikh et al., 2019). Awareness of cybersecurity threats seems quite low, particularly when it comes to social media. Many people appear to have little idea about what and how much information they can share without taking unacceptable cyber risks (Parsons et al., 2014; Blackburn et al., 2018; Zhang & Gupta, 2018; Thakur et al., 2019).

Given that the increase of security breaches has occurred due to poor cybersecurity awareness (Alshaikh et al., 2018), I intend in this study to raise such an awareness as one of the topmost priorities of organisational management (Ghazvini & Shukur, 2016).

I concentrated on social media in particular because social media management is now integral to many organisations' marketing and communication strategies, offering direct and effective communication with customers and employees.

However, the risks of their improper use are far from understood by users, 95% of whom end up sharing private confidential information inadvertently (Milkovich, 2021). Moreover, social media and the majority of other current technologies were not created with built-in defenses against hackers (Ferrara, 2019). Therefore, the need to educate users on the emerging cybersecurity challenges for social media is imperative; yet, despite a variety of training approaches, such as testing (Alshaikh et al., 2018), analyzing real cases, video training (Tayouri, 2015), discussion (Scholl et al., 2018), E-learning (Haeussinger & Kranz, 2017), gaming (Awojana & Chou, 2019) and gamification (Gjertsen et al., 2017) the same mistakes are being consistently repeated (Furnell & Vasileiou, 2017). Existing training approaches do not cater for different types of employees, their level of awareness, learning objectives and learning styles (Christopher et al., 2017; European Network and Information Security Agency (ENISA), 2019; Caulkins et al., 2016).

According to the European Network and Information Security Agency (ENISA), raising cybersecurity awareness must be a continuous process (European Network and Information Security Agency (ENISA), 2019). Indeed, ENISA suggests analyzing gaps and vulnerabilities that exist within organisations to foster user awareness. Then, a strategic plan needs to be in place to ensure protection against cyber threats, and the success or failure of the entire process should be evaluated.

The literature review reveals that users differ in their perceptions, preferences and approaches towards cybersecurity training and learning. The employees' perception that this training does not meet their needs is the major problematic issue in the cybersecurity training field. This suggests that the factors that influence the adoption of cybersecurity training are restricted and need to be improved (Haeussinger & Kranz, 2017).

As a result, previous research recommended that cybersecurity threats among various user categories (such as male vs. female IT experts vs. non-experts, older vs. younger users, etc.) be thoroughly considered (Zwilling et al., 2019; Schürmann et al., 2020).

Gender plays a pivotal role in adopting cybersecurity measures (Akbari Koochaksaraee, 2019; Anwar et al., 2017; Venter et al., 2019; Lin & Wang, 2020; Dhakal, 2018; Jin et al., 2018). Age is another demographic factor that plays a crucial role (Hadlington, 2018;

Saridakis et al., 2016; George et al., 2020) in following cybersecurity protocols. Expertise and skills obtained are crucial in thwarting security threats (Gratian et al., 2018; Green, 2016). Any familiarity with online security threats helps users in mitigating their effects significantly (Jeske & Van Schaik, 2017). It is important to notice here that those who perceive risk on social media possess different habits and attitudes toward cybersecurity practices (Van Schaik et al., 2018).

While raising cybersecurity awareness is one of the most challenging issues for most organisations today (Bada & Nurse, 2019), one cannot claim that a particular organisation exhibits a higher level of security awareness than other organisations (Ghazvini & Shukur, 2016). That is because every organisation has its own vision and approach to meet their objectives. In fact, more research is needed to establish how organisations manage their risks and how they formulate their social media policy and control (Demek et al., 2018).

With the global outbreak of COVID-19, most of the workforce compulsively operate from their homes. They use social media to stay in contact with their colleagues, clients, or customers. Griffin (2021) argues that cyber-attacks have increased considerably during this trying time. Hackers have been employing a myriad of social engineering techniques these days that include luring users to open attachments forwarded by them (Lallie et al., 2021).

Currently, social media users across the world have been expanding rapidly; the total number of users has gone past 3.8 billion, which constitutes close to 60% of the current world population (Kemp, 2020).

Surprisingly, a large proportion of these users do not even know how damaging it could be for them - not only socially but also economically (Milkovich, 2021). Therefore, it is important to find a strategy that promotes social media users' awareness. Through the creation of a system for security awareness training and the general use of end-user security restrictions and privacy shield tools for social media, this study seeks to assist the organisation in making its technological and financial investments more effective.

Although social media policies (SMPs) are thought of as a logical limit, little research has been done on them (Banghart et al., 2018). It appears that even though organisations probably have SMPs in place, they do not make them publicly available online. Also, it seems that SMPs do not seek to increase public consciousness (Bada & Nurse, 2019). Due of the difficulty in efficiently managing social media risk, many organisations opt to

absorb it in a reactive approach rather than formally controlling risk (Demek et al., 2018).

Another issue is that many users are unaware of how to use the privacy settings tools that social media platforms offer (Wisniewski et al., 2017). They therefore require additional education to comprehend the security technologies developed to enable people to protect their data and privacy (Nyoni & Velempini, 2018).

In addition, most users do not use the security policy settings offered by social media, and they have failed to manage its features (Bhatnagar & Pry, 2020), which indicates that the language used in its writing is too technical for most users to understand (Nyoni & Velempini, 2018). This is the main cause of their failure, as people by nature need to know and understand what they are supposed to do.

Researchers discovered that users unintentionally post sensitive information on social media and struggle to distinguish between sensitive and non-sensitive information (Nyoni & Velempini, 2018), which makes it easier for hackers to carry out their mission. Regrettably, users frequently struggle to understand how to make their online communications secure (Scholefield & Shepherd, 2019). On the other hand, harmful software transmitted through social media more efficiently makes viruses and Trojans available, therefore, organisations should give staff members clear advice on how to handle social media use (Das & Patel, 2017).

Some contend that social media users should abide by safety rules and be secure, however social media content is difficult to manage because it is dependent on a third party, 'cloud' programmes. As a results, deterrent and punishment do not work to enhance adherence to security policies, yet training and awareness could help (Gasiba et al., 2021).

Specialists are beginning to rely on training to increase greater awareness. However, it was discovered that many cybersecurity trainings are ineffective because they are repetitive and do not encourage users to apply security ideas critically (Tayouri, 2015). Additionally, they are frequently offered in a 'one-size-fits-all approach' (Furnell & Vasileiou, 2017), without taking variation into account. Additionally, studies revealed that the methods used to give cybersecurity training are insufficient (Ghazvini & Shukur, 2016). Also, it is difficult to simulate the complex and challenging circumstances that lead to this cyber vulnerability in training environments (Nicholson et al., 2016).

Efforts that emphasize adaptive cybersecurity training for social media are generally scarce. Regardless of whether their methods are beneficial or not, it has been discovered

that every organisation tries to implement its policies in a variety of ways. People continue to make the same error even after reading and receiving policies; businesses heavily invest in employee training. However, the issue is not with the training itself; rather, it is with the trainees. They will not pay attention if they do not get used to the exercises, and the training will not produce the desired results which is changing people behavior.

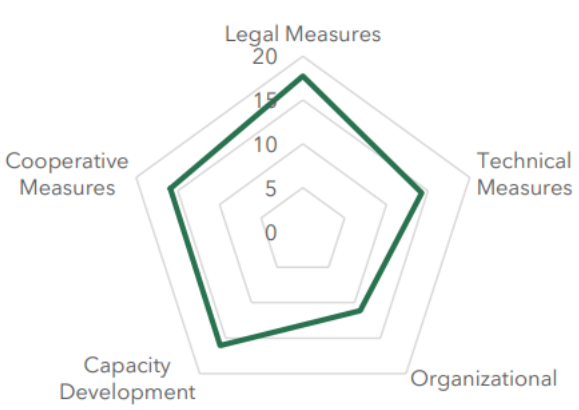
1.2 Study Area

The area of interest is Kuwait City; therefore, it is advantageous to learn more about Kuwaiti personnel and our motivations for choosing this society.

East of the Arab world is where the city of Kuwait is situated, sharing borders with Saudi Arabia to the south and Iraq to the north. Kuwait is one of the top oil producers and energy sources in the world, with a total size of 17,820 square kilometers. Kuwait has a population of about 3.9 million people (William, 2022).

Among the five Arab nations, Kuwait is seen as one that is increasingly using social media (Alansari et al., 2019). On the other hand, by 2035 it will be anticipated that all firms in Kuwait will be addressing their outcomes and services within digital flows, using the same fundamental technique, the internet (Alenezi, 2019).

Kuwait was placed 66th globally and 6th among Arab nations in the 2020 Global Cybersecurity Index (ITU, 2022), with a score of 75.07 out of 100 on the questionnaire of the global cybersecurity scores and ranking of countries (pls, refer to Figure. 1.1 for more details).



Development Level:
Developing Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
75.05	17.74	14.25	11.13	16.05	15.90

Figure 1.1: Kuwait Cybersecurity Index ITU (2022)

Kuwait was ranked number 8 for email virus and number 6 for spam assaults in a 2018 Symantec report (Cleary et al., 2018). According to Alenezi (2019), maintaining privacy and cybersecurity in enterprises is Kuwait's second-biggest concern. The government of Kuwait, on the other hand, is extremely concerned about cybersecurity risks. They are making a significant effort to provide a proper framework that helps reducing cybersecurity-related issues and warnings (ITU, 2022). The Communications and Information Technology Regulatory Authority (CITRA) organized the 'National Cyber Security Strategy': this strategy was developed in 2014 to safeguard sensitive and vulnerable national infrastructure assets. Due to the variety of warnings and cyber risks demands made against corporations and people, this method challenges the Kuwaiti government (CITRA, 2022).

In response to these effects, Kuwait's ministry of interior established a special department called 'Fight against Electronic Crime' to maintain the security in the state. Kuwait also passed the first e-crime law that year (2015) (Alansari et al., 2019). Additionally, the Kuwaiti Ministry of Interior made an effort to increase people's security knowledge by posting a number of brochures on its website and social media platforms in an easy-to-understand manner. These brochures explain how people can safeguard themselves in a variety of daily circumstances, including shopping and lodging. They employ simple language and visual aids to explain how to reduce risks; they also adopt a storytelling

technique to provide their suggestions and an actual incident that might occur when using social media. They make reference to a wide range of other issues, including two-step authentication, password security, and who should be notified in the event of an incident.

Given that they stated that all of their inquiry is top-secret, they provide their contact information in the event that anyone has any issues or concerns (of interior Kuwait, 2022).

Today, there are many organisations in Kuwait that manage the tasks related to cybersecurity training, including (CITRA, CAIT, the ministry of the interior, and others). However, much of this training is intended for government employees who work in the public IT sectors. However, I do say that our research was the first to identify Kuwaiti personnel on the subject of raising social media cybersecurity awareness through adaptive training.

1.3 Study Scope

The major objective of this thesis is to examine a novel strategy for adaptive cybersecurity training for social media by better understanding user behaviors and perceptions of cybersecurity training as well as by examining the risk that such an employee poses to the organisation due to using social media. In Table 1.1, the study's objectives and the relevant research questions that support them are described.

Table 1.1: Thesis objectives and relevant research questions.

Objective	**Research Question**	**Chapter**
To examine the variables influencing people's preferences for cybersecurity training and factors encouraging the adaptive training.	RQ1. What differences exist between trainees' preferences for cybersecurity training? RQ2.What factors encourage adaptive cybersecurity training?	Chapter 4

To analyze the risks and challenges related to social media cybersecurity in organisations.	RQ3. What elements affect an employee's potential level of risk when using social media? RQ4.What challenges do cybersecurity formulators, trainers, and policymakers encounter in their work?	Chapter 5
To find weaknesses and limitations in earlier attempts to provide adaptive cybersecurity training.	RQ5. What limitations existed in earlier attempts to develop human factors-based adaptive cybersecurity training?	Chapter 6
To build a prototype system that replicates the suggested framework while employing different scenarios, as well as to offer novel methods for adaptable cybersecurity training for social media users.	RQ6. What new techniques have been discovered in this research to build an adaptive cybersecurity training for social media in organisations?	Chapter 7
To conduct a series of evaluations involving a representative sample of social media users to gain insight into framework practical effectiveness.	RQ7.What evaluation techniques and approaches are being used to verify the framework's effectiveness?	Chapter 8

To create recommendations in accordance with prior objectives for the deployment of our adaptive cybersecurity training and examine their generalizability.	RQ8. What recommendations for developing adaptive cybersecurity training in organisations can be derived from the research objectives? RQ9.What are the chances and difficulties for applying the findings to other locations, cultures, or peoples?	Chapter 9

1.4 Thesis Outline

This research consists of nine chapters. The current chapter presents a broad introduction to the research, including the background of the problem, the significance of the study, and study scope. In **Chapter** 2 the literature reviews are conducted, this chapter focuses on the risks associated with using social media and how previous works attempted to construct technical and non-technical defenses against these threats. Following that, the chapter including the state-of-the-art literature on adaptive cybersecurity training. The body of the thesis is presented in **Chapter** 3 that discusses the approach utilized to gather the data for this project, which enabled me to develop cutting-edge methods for an adaptive cybersecurity training system for social media and **Chapter** 4 summarises our initial investigation's findings and preliminary findings and disregarded the factors that encouraged our candidates to receive adaptive training. Aiming to evaluate aspects of our candidates' social media cybersecurity risk, **Chapter** 5 examines these issues.

Chapter 6 is devoted to our theoretical framework; it discusses the gaps and insights gained from preceding frameworks, models, and approaches in this area which assisted me in creating our novel framework. Following by **Chapter** 7 that describes the evolution of our framework; as this chapter goes in-depth on the motivations, domains, and metrics of our proposed framework. However, **Chapter** 8 focuses on the experimental procedures used to validate our proposed framework, the strategies I used to do so, the participants in this stage, and the outcomes of these validations. The thesis is finally concluded in **Chapter** 9 by summarising the research findings in terms of how they address the research objectives and by outlining challenges and potential for further study.

1.5 Data Collection Process and Methodology

The flowchart of the study methodology for each research question is presented in Figure 1.2 below. In this thesis, quantitative and qualitative approaches were combined. In terms of framework validation, case studies were conducted. However, the reader is directed to the particular chapters to explain each data collection method and the corresponding analyses thoroughly.

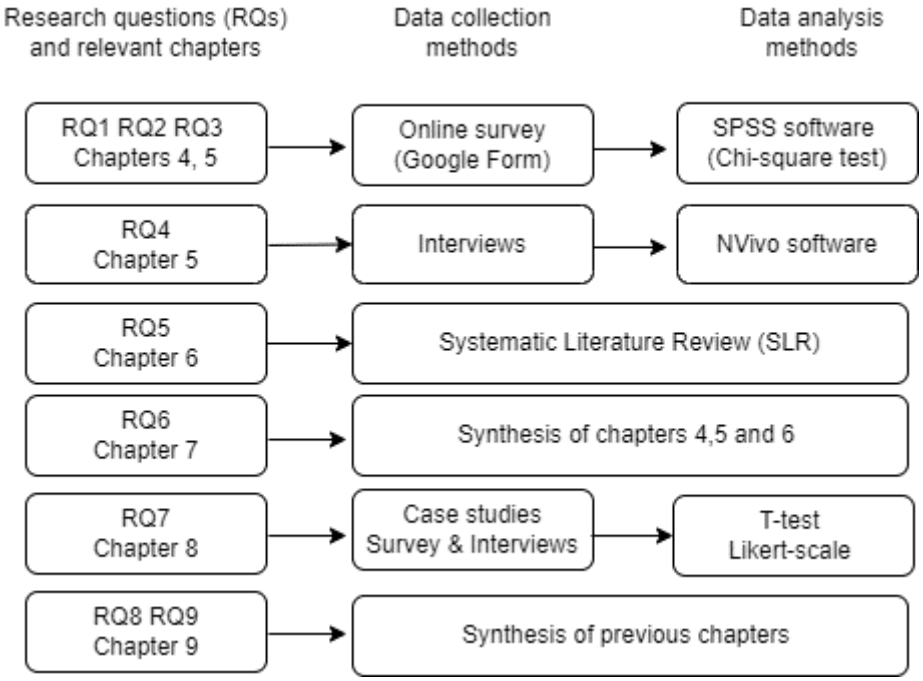


Figure 1.2: Flowchart of the study methodology

Chapter 2

Background

This chapter focuses on the most prominent social media risks, followed by how experts attempted to mitigate these threats through technical and non-technical approaches. The chapter examines state-of-the-art cybersecurity training approaches by assessing the improvements made in cybersecurity training and the initiatives made to make the training adaptive.

2.1 Introduction

Researchers argue that social media has become vulnerable to hacking activities or cyber threats considerably (Ghafir et al., 2018). A variety of studies indicate that hackers are active on social media sites for fulfilling their objectives (Aldawood & Skinner, 2018). The very nature of social media platforms allows participants to have trust in each other when they interact creating gaps and vulnerabilities. This makes the job of hackers relatively easy. At times, it becomes easier for hackers to perform their tasks due to the strong inclination of the majority of the population towards social media platforms.

As such, people often compete among themselves to increase their fan followings, and in their bid to do so they disclose their private information enabling hackers to perform their illegal or unethical activities including economic crimes with ease (Zhang & Gupta, 2018).

Further to this, user awareness is quite low when they share their private information on social media platforms because they have no idea what information to share and how much information to share without taking any cyber risks (Van Schaik et al., 2018).

Surprisingly, people will sometimes put their trust in an anonymous account. Blackburn

et al. (2018) experimented to evaluate users' level of awareness on social media sites; they forwarded more than 1600 massages via Facebook from unknown user accounts and discovered that users could be tricked easily. In other words, hackers can easily collect information they need from naïve account holders to commit illegal or unethical activities on social media.

Although many social media sites such as Twitter do not ask for many details from users to prevent hacking, hackers apply their intelligence in analysing the content posted by users in their accounts and find their way to commit some unethical or illegal activities (Thakur et al., 2019). The following sections will cover the most prevalent social media risks as well as an analysis of the most recent methods and solutions for reducing their impact.

2.2 Social Media Risks

Our research focuses on the risks associated with social media cybersecurity and looks for techniques to eliminate them for users. Therefore, it is beneficial to outline the most pertinent social media threats that users may experience on these networks. To understand cybersecurity threats in more detail, it is important to understand the variety of techniques that hackers employ in their endeavors. I will go deeper into the most prominent social media hacking, which will be described in the following subsections, based on the variety of malicious acts carried out by hackers on social media.

2.2.1 Identity Fraud

Identity fraud or theft involves hackers using personal information in an unethical manner (Irshad & Soomro, 2018). There are two ways to accomplish this: either the offender makes a fake profile of the victim and then interacts under that pretext, or the offender steals the victim's password or gains access to their social media account in some other way, then uses that account to represent the victim. What happened in California is an illustration of such an instance: a teenager was sentenced to up to a year in a juvenile facility for using another student's Facebook password to post sexually explicit content about the victim (Reznik, 2012).

It is estimated that at least 10 million Americans have become victims of 'Identity Fraud'

so far on social media alone. These kinds of activities cause some kind of negative effect on innocent users of the accounts. As per CBS News, as much as 47% of the identity fraud victims get their credit scores rerated on the lower side, even 11% have issues in getting proper jobs (if they are already unemployed), and as large as 70% of them earn bad name due to such incidents with them. A significant proportion of victims face some kind of emotional issue (Irshad & Soomro, 2018).

2.2.2 Spam Attacks

Millions of fake accounts on social media were apparently under the control of spammers who wanted to influence people's behaviour (Ferrara, 2019). Spam poses severe security issues on social media sites creating confusion and threat perceptions among social media participants. Spammers can publish links to social media networks anonymously, directing unsuspecting visitors to spam Web sites. Moreover, social media sites do recognise another type of spam attack called 'friend spam' (Blackburn et al., 2018) through which people receive unwanted friend requests without any reason whatsoever. At the end of 2008, the Kaspersky Lab collection had more than 43000 spam files related to social media (Luo et al., 2009).

2.2.3 Malware Attacks

Malware contains various threats, including viruses, worms, trojans, bots, and other dangerous code (Green, 2016). The Malware attack aims at gaining access to devices to destroy the network or the device itself; the malicious software disrupts not only the operations of a computing device but also existing cybersecurity walls (Yang et al., 2019).

In one of the notable cybercrimes that occurred with Sony Pictures during 2014, sensitive information including unpublished movies were stolen by cyber attackers, and their social media accounts were also hacked (Jardine, 2015). In 2015, hackers took hold of Delta Airlines' server and posted some disturbing content on their social media accounts, which emphasize that hackers may have an obscure purpose when they conduct such unethical activities (Zhang & Gupta, 2018).

2.2.4 Sybil Attacks

Sybil or fake accounts are created on social media as the agents of hackers, essentially to help hackers to conduct malicious activities (Blackburn et al., 2018). While fake profiles or fake request may not be always toxic, it certainly falls under the category of cyber-attack.

The following describes the Sybil attack scenario: Attackers send numerous friend requests from fake accounts, and some genuine users may unwittingly accept them and become Sybil attack victims. Attackers can spam, phish, and engage in other undesirable activities in the target networks once real users accept friend requests from Sybil identities (Jethava & Rao, 2022). As a result, the sybil attack seeks to trick common users into taking actions that benefit the attackers (Zheng et al., 2017).

Attackers can easily create many Sybil or fake profiles on social media. For instance, fake accounts on Facebook increased from 5.5% to 16% in 2020 (Jethava & Rao, 2022). The most disturbing aspect is that it is difficult to detect such accounts; more often, they are organised as legal accounts but aim at performing unethical or illegal activities sneakily. While research reveals that it is difficult to combat a Sybil attack, it goes without saying that the major challenge for experts lies in finding and detecting Sybil accounts (Zheng et al., 2017).

2.2.5 Social Engineering and Phishing Attacks

Social engineering is a technique of extracting confidential information such as passwords, banking details, or any other information of importance (Jamil et al., 2018), and phishing is the practice of using both technological and social engineering techniques to persuade a user to disclose personal information (Gupta et al., 2016).

According to recent studies and surveys, social engineers are responsible for 84% of successful cyber-attacks (Salahdine & Kaabouch, 2019). Aldawood & Skinner (2019) opine that social engineering could have many ways to execute their malicious intentions. Usually, phishers look innocent to the users because they seem to provide some useful information to account holders (Zhang & Gupta, 2018). A large proportion of phishers commit their crimes by offering a free giveaway or inviting users to play some games or asking users to complete some important survey (Irshad & Soomro, 2018), they resort to these attacks when there is no way to breach a system with no technical flaws. According

to the United States Department of Justice, social engineering attacks are one of the world's most frightening risks (Salahdine & Kaabouch, 2019).

Parker & Flowerday (2020) argue that social engineering is rampant on most social media platforms. For example, in 2019, phishing on Instagram and Facebook increased by 74.7% over the previous year. This could be due to some features associated with some specific platforms, like overflowing emojis, the shortened link, or a large amount of personal data available.

Even the most cutting-edge businesses are susceptible to phishing attacks, as was the case with Swedish bank Nordea in 2007 when phishers successfully sent fake emails to their bank customers, leading them to install the 'haxdoor' Trojan disguised as anti-spam software, causing the bank to lose over 7 million Euros. A subsequent phishing email attack from Lithuania cost those two global digital titans, Facebook and Google, 100 M$ (Clavin,D, 2022).

2.2.6 Impersonation

With the explosion of social media, a different kind of cyber-attack called 'social media impersonation' has been in practice (Zarei et al., 2020). Reports of impersonation attack on Instagram only increased 155% in the 12 months to March 2022 (Downes, 2022). Social media impersonation involves pinching someone's identity and pushing it forward as if they are a legitimate entity (Uzun et al., 2018). One of the impersonating cases on social media was a lady in New Jersey who was charged with creating a fake Facebook profile in order to assume the identity of her ex-husband to demonstrate that he is a drug addict (Gharawi et al., 2021).

2.2.7 Hijacking

Hijacking aims at stealing a whole session key to be used as a remote control; therefore, it poses serious risks for social media account holders (Khandpur et al., 2017). In this way, hackers can enter into users' data systems while controlling them remotely. Any web interaction between client and services give way to this kind of attack. As such, hackers usually target those social media accounts which use a non-secure connection (HTTP), especially in public Wi-Fi or in Local Area Networks (LAN) (Hossain et al., 2018). This kind of attack becomes possible because users ignore warning messages and enter the

web browser without realising the consequences.

A twenty-year-old girl who had her email account hijacked after changing her password using only publicly available information about her from Google and Wikipedia (Aïmeur & Schőnfeld, 2011) ,and a Twitter account of the Russian prime minister at the time, Dmitry Medvedev, was stolen in 2014, and the hackers tweeted anti-Putin tweets to the 2.5 million followers demonstrates that hackers have a variety of motivations for committing hijacking (Harding, 2014).

As such, one of the greatest hijacking cases was observed during September 2018 when as many as 50 million Facebook accounts were compromised when hackers stole Facebook access tokens of the users through which they got control of these accounts (Elliott, 2018) . This means that it is not only that individuals are vulnerable, but even companies with such large establishments are also vulnerable to hijacking attack .

2.2.8 Image Retrieval and Analysis

Users have to understand that the internet is public, and when they share their pictures on it they are typically sharing them with strangers (Edgar & Manz, 2017). It may be interesting to know the consequences of such actions when one US soldier posted pictures of their helicopters on social media sites in 2007. The Iraqi revolutionary armed forces, by taking a clue from those pictures, not only located the helicopter but also successfully destroyed it (Green, 2016). Additionally, social engineering attacks benefit from having images of their victims on social media because it makes their task simpler (Hadnagu, 2019).

According to Zhang & Gupta (2018), each of the above-discussed cyberattacks does not have an equal bearing on users. While it is estimated that malware, social phishing, impersonation, and hijacking rank high in the lists for their negative consequences, spamming and sybil attack rank low in creating their impact on users. Identity fraud is mostly associated with having an average impact on users. The idea is that there are numerous methods and techniques used in cyberattacks to breach social media accounts, and therefore individuals and firms must arm themselves in several ways to thwart the efforts of social media hackers.

2.3 Developing a Defense against Social Media Risks

The preceding paragraphs have explained that social media threats are actual and that protecting ourselves from them is crucial. Even if an organization does not use social media, it is nevertheless exposed to risks because their employees probably are (Green, 2016). Finding methods to guarantee security and privacy on social media networks is therefore essential, even though it is challenging given that social media requires frequent upgrades to keep up with the deployment and dynamic development of the technology (Zhang & Gupta, 2018).

To find any gaps and limitations, I looked for the attempts made by subject-matter specialists to reduce these risks. The efforts being made by professionals to reduce social media risks, both technically and non-technically, are the focus of the subsections that follow.

2.3.1 Technological Defense Tools

Many popular social media accounts provide a convenient service to maintain security (Mousavi et al., 2020), such as the 'second authentication' which is often part of two-factor authentication, in which a four or six-digit code is forwarded to the registered mobile number that remains valid only for a few minutes. Second level authentication is also done when a user accesses their account from another browser (Guerar et al., 2018). This feature could guard against hijacking attacks. Similarly, a Sybil attack can be spoiled by developing second-level authentication to enhance users' confidence levels (Zhang & Gupta, 2018).

Using Virtual Private Network (VPN) software, especially during public connection, is an effective way to encrypt traffic and prevent risks of social media (Zárate-Moedano et al., 2021) such as hijacking as one remains not only nameless on the internet but can hide one's IP address too. Also, a user can disable the 'Location' feature to prevent hackers from seeing their personal location details (Mousavi et al., 2020).

Nevertheless, experts attempt to prevent spamming in a variety of ways, but there was a limit to how successful earlier experiments using machine learning could be (Abdullahi & Kaya, 2021). For example, 'Blacklisting' is a technique that is being used to avoid spamming; however, this approach needs continuous updating in a specific order. Such a'behavioral analysis' approach is quite time-consuming in the sense that it rests on

gauging user account behaviors based on the URLs accessed (Ameen & Kaya, 2018). However, to identify spam more accurately on social media, Abdullahi & Kaya (2021) suggested a deep learning methodology called Dense Neural Network that is superior to traditional machine learning approaches. As the results of observing and controlling the performance of machine learning and deep learning classifiers on the SMS dataset, the results show that Dense Neural Network reasonably detects spam in both datasets than machine learning classifiers.

Since phishing and social engineering attacks exploit human weaknesses rather than technology flaws (Hadnagu, 2019), phishing attacks can best be tackled by 'machine learning' because this method may convert the difficulty of phishing attack detection into a classification task (Jupin et al., 2019). Anti-spamming tools can be employed to extend protection from a phishing attack that helps segregate genuine emails from fake ones (Gupta et al., 2016). There are several open-source websites that can determine whether a link, website, or webpage is genuine. In addition, there are numerous other algorithms that can be used to identify phishing attacks, such as the link guard algorithm and the surf detector (Gupta et al., 2016). However, the fact is that they are getting smarter with each passing day.

Many strategies have been developed to reduce the consequences of sybil attacks or fake accounts. For example, the 'Identity Deception Detection Model' (IDDM) attempts to capture the purpose behind the fake account on social media platforms. The model not only perceives deception but also differentiates between human and bot (Van Schaik et al., 2018). Khaled et al. (2018) proposed a new algorithm called SVM-NN to improve the identification of fake accounts on social media by utilizing fewer features reduction strategies to decrease the feature vector. More recently, Awan et al. (2022) suggested a solution to this problem named the Spark ML-based project with a higher degree of accuracy than existing methods of profile recognition.

As far as Malware attacks are concerned, research reveals that analysis is a successful approach for creating a defense against malware-attacks; malware analysis aims at discovering how malware communicates with the whole environment (Maglaras et al., 2018). For example, Yuan et al. (2019) offered a deep learning strategy that relies on LSTM and encoder-decoder neural network architectures. This method can detect and alert users to system errors that are probably caused by malware attacks.

According to Uzun et al. (2018) several publicly available facial/voice recognition technologies (such as Microsoft Cognitive Services or Amazon Rekognition) are vulnerable to even the most basic attacks.Therefore, they presented a Real-Time Captcha (rtCaptcha) system to address the shortcomings of current liveness/human detection methods and prevent 'impersonation'. As such, organizations need to employ some sophisticated software such as 'Social Mention' being used by Google. 'Social Mention' forwards email warning messages to users if their names have a mention on social media (Yang et al., 2019).

The following diagram in Figure.2.1 summarises the technical tools discussed for users in defense against cyberattacks on social media platforms.

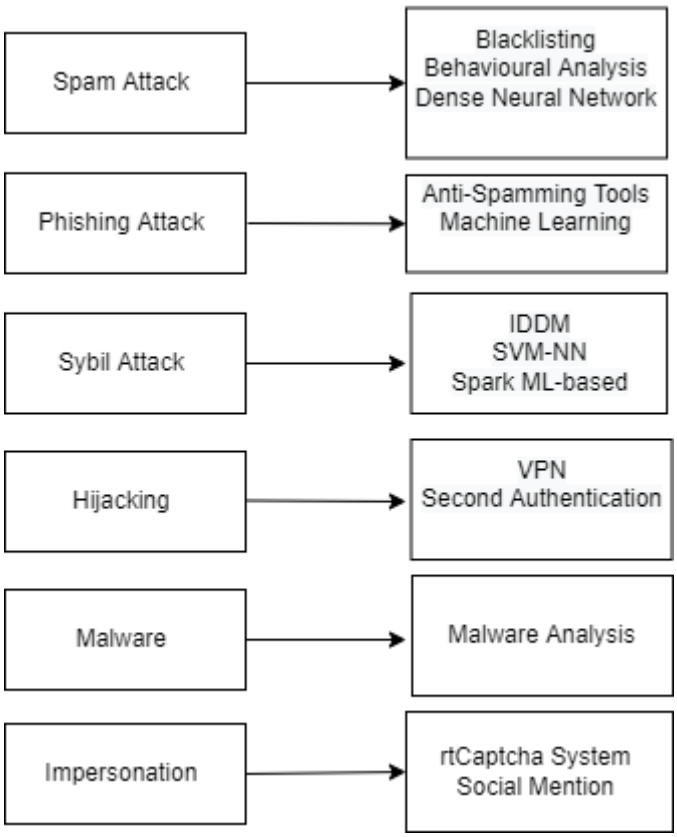


Figure 2.1: Technological defense tools

2.3.2 Non-technological defense tools

Even while attempts have been made to decrease the threats associated with social media, no system is completely resistant to hackers (Alshaikh et al., 2019). Threats on social media, including identity fraud, social engineering, image retrieval and analysis, necessitated that users be informed of proper online behavior and how to file reports of suspicious activity. Research indicated the value of combining technical skills with human and cognitive

abilities to improve a cybersecurity workforce (Brilingaitė et al., 2020).

Employees and organizations should be aware that using technical support systems could be one strategy to stop cyberattacks, but users need perform their responsibilities in defense against these threats adequately (Chowdhury & Gkioulos, 2021; Edgar & Manz, 2017). As such, employees need to realize that safeguarding the organization's IT assets is not their duty, but their survival is associated with it (Hovav & Putri, 2016).

While European Network and Information Security Agency (ENISA) (2010) asserts that technology can protect us from cyber incidents at certain times and not always because with the advancement of technology, hackers are likely to employ more evolved techniques for their operations; in other words, technology can never provide a fool proof solution always. However, well-informed individuals who are properly trained could help to successfully thwart cyber incidents.

Developing a defense mechanism against social media cyber-attacks is generally crucial. However, studies establish that if organizations can improve training for their staff and formulate effective policies then they can certainly minimize risks arising from social media hackers (Demek et al., 2018). Also, cybersecurity is not only about creating fencing to protect from hackers; in fact, it goes much farther than that to include many other important aspects such as setting cybersecurity policies, risk management, protocols, ethics, and so on (Lee, 2021). As per European Network and Information Security Agency (ENISA) (2019), raising cybersecurity awareness is a continuous process, and training is the first line of protection against hackers' maliciously inclined 'endeavors' (Aldawood & Skinner, 2019).

The non-technical measures adopted to reduce cybersecurity risk including social media are illustrated in the sections that follow.

Awareness Campaigns

A great example of a security awareness approach is the "campaigns"; some researchers describe the 'awareness campaign' as an intervention to alter user behaviour considerably (van der Kleij et al., 2020). The European Cyber Security Month (ECSM) is an EU campaign that concentrates on raising organization as well as user's security awareness, that deployed by ENISA and other associates every October of every year. As many researchers argue that awareness campaigns need to run throughout the year uninterruptedly as users need to remind again and again (Muhirwe & White, 2016). The campaign centers on

training, strategy summits, online quizzes, common presentations to individuals, and so forth. However, such campaigns must be concise and simple in their content so that users do not get confused. Also, all the warning messages should be developed by experts in the field because researchers discovered that people are inclined to rest their trust in professionals rather than others (Bada & Nurse, 2019).

Baker (2016) suggests that campaigns should have contents on cyber awareness that may attract a large number of people. At the same time, using a 'convincing' technique is considered a successful idea in 'campaigns' for changing user behaviours which are comprised of advising on technological change.

Policies

Liew (2021) argues that setting policies to guide the proper use of social media is not optional; in fact, social media policies (SMPs) specify certain rules for developing healthy social media practices. Stoessel (2016) suggests that SMPs include three key issues: first is the policy control meaning prescribing the proper behavioural guidelines for using social media platforms, the second deals with managing cookies, etc. including banning certain sites, and the last one is about the training of employees so that they can understand those policies clearly and practice them properly.

While employees tend to recognise what is the secure usage for them for social media practice, Bennett & Manoharan (2017) assert that employees need to develop their system in compliance with the company's SMPs that include social media security policy, information disclosure policy, social network passwords policy, Twitter policy, Facebook policy and so on. Ozkaya (2018) emphasizes that users must know the dark side of social media so that one does not fall into a trap while making use of it.

Wisniewski et al. (2017) argue that policies provided by social media platforms also serve the purpose of raising awareness by those sites; however, many users fail to understand how to make use of those features effectively. The fact remains that most of them avoid using it because of their inability in handling those features (Bhatnagar & Pry, 2020). Nyoni & Velempini (2018) assert that many of the users cannot understand SMPs because, at times, they are mentioned in technical language.

Additionally, there are many challenges to SMPs; that is so because technology has been evolving constantly and to keep pace with the technology SMPs need to evolve too. SMPs still do not have any standard international body, such as the IEEE, and as such, there is

no uniform format for developing it (Stoessel, 2016). Hiltz et al. (2014) discover that the second challenging issue is to develop clear policies for using social media.

While many organizations prefer to focus on technical issues rather than human factors (Bennett & Manoharan, 2017), a wide variance can be seen among the organizations as far as SMPs are concerned (Stoessel, 2016). In one revelations, Bennett & Manoharan (2017) find that while firms in 156 US cities make use of social media for work extensively, only 30 of them have well laid down formal policies for social media use; much of the social media misuse has happened because of this. Employees, in many such organizations, have got trapped in "bad experiences" for this reason. Moreover, in many organizations, people have lost their jobs for violating organizational SMPs.

Therefore, a formal policy is a must to guide employees in using social media platforms. As policy implementation enhances the amount of social media-related training and technological controls; however, the key issue is that organizations are adopting social media strategies and policies in a reactive approach, as opposed to practicing a formalized risk management rule (Demek et al., 2018).

Social Media Guidelines and Best Practices Recommended

The National Cyber Security Centre (NCSC) offers guidelines for interacting safely with other users. At this juncture, it will be appropriate to introduce key social media platforms.The purpose of presenting this data is to show how these platforms do explain appropriate behaviour while communicating with others through them, and that users should read and understand these rules. Finding out why some people do not comprehend and utilise this information is therefore one of the study's primary objectives.

Facebook

On the Facebook platform, one can make use of privacy setting tools for the safe handling of the operations. Even users can select their audience to share content with them. The audience selector option can be found at several places through which users can share their content such as posts, photos, and other information on Facebook through their profile. *'Change who it's shared with'* is an option at Facebook to modify things that any user has already shared with others. Facebook provides, without using any technical jargon, clear and straightforward recommendations in the chosen language; Moreover, users can choose from many options to secure their accounts. While reporting incidents such as accounts of impersonation, fake accounts, multiple profiles, and many others can

be done through simple steps such as clicking on the three dots under the cover photo or by selecting *Find support or report profile*.

Facebook also explains how users should deal with spam, how to recover an old Facebook account that one fails to log in, or what to do if the account is disabled, or if a friend's account has been hacked. Instructions are also available if the account has been compromised or is being used by someone else.

Facebook not only provides two-factor authentication (TFA) but also provides reasons for doing that. Facebook takes care in protecting the profile password and clearly instructs, in case of any incident, to reset passwords. They also conduct surveys by providing a link to users to have feedback for their experiences on Facebook.

Twitter

Similar to Facebook, Twitter also provides a help page for protecting the tweets of users. However, it is up to users to set their accounts public or private. In case a user wants to protect his or her tweets, Twitter provides full instruction for that.

In case of a hacking incident on Twitter, the help centre provides some guidance to manage the incident. A request for a password reset is the first necessity in such circumstances. A *support request* can be forwarded to them if one is unable to log in even after resetting the password. In short, if the account has been compromised one needs to contact the help centre as quickly as possible. Twitter also provides a set of security recommendations to stay safe on Twitter. They strongly recommend having a strong password with a combination of numbers, special characters, and alphabets.

Moreover, a user can report tweets, lists, and direct messages that violate the Twitter Rules, such as those containing abusive or harmful content, spam, impersonation, copyright, or trademark violations. In short, reporting incidents on Twitter is quite convenient.

YouTube

Like Facebook, Twitter, YouTube has also provided a *YouTube Help* page to stay safe online. They have explained likely phishing incidents on YouTube stating that they never ask for the email address, password, or other information related to the account. They advise their users to secure their accounts to prevent any kind of hacking; securing steps have been explained by providing a short video on their website.

They recommend reporting any questionable content on YouTube to the *YouTube team*,

such as spam or phishing. They also provide tips to follow in case a user account has been compromised. They provide a list of recommendations such as enabling the TFA, creating a unique and robust password, updating regularly for keeping user accounts safe; the importance of these aspects is explained at length.

The YouTube *Help page* can be used to report any incident. Reporting inappropriate content on YouTube is quite simple. For reporting a video on YouTube, one needs to select the *Report on the video player menu* giving a reason for this reporting, which is then acknowledged with a confirmation message. Users can report a video, a playlist, a thumbnail, a link, a comment, a live chat message, and an advertisement on YouTube.

Instagram

The *Help Centre* page on Instagram presents valuable information for their users to stay safe online. On Instagram, one can decide whether to set one's account private or public. Making the profile private means contents such as videos, photos, or location pages can be viewed by only those who have been approved by the account holder. Setting the account public means anyone on Instagram can see all the contents inserted by the account holder.

Instagram Help Centre also provides step-by-step guidance on how to set your profile private. Apart from providing some valuable tips, the FAQs provide answers to many general queries of users such as 'how to remove followers', 'how to remove Instagram images from Google search, 'how to turn comments on or off for Instagram posts, and so on. Moreover, under the *staying Safe* option, there are many security tips and guidance provided that include reporting any incident such as impersonation, bullying, or harassment on Instagram. The *'report it'* link given on their website helps report any phishing account quickly. Instagram takes impersonation seriously; one can also report impersonation incidents by filling out a form regardless of one is having an Instagram account or not. They provide valuable guidance to deal with these kinds of incidents.

To keep user accounts safe, Instagram has laid down a set of security warnings that users need to follow for safeguarding themselves from cybercriminals that including changing passwords regularly, creating a strong password, and what to do if the account is hacked. Explaining the concept of the TFA, they insist on enabling the TFA for keeping the account secured. On finding that account has been hacked, they recommend contacting them to reset the password immediately. Password can be reset using the email address, phone number, or even the Facebook account. Users can ask for additional support if they fail to

reset the password.

LinkedIn

LinkedIn has introduced an *In Help* page for its users to stay safe online while interacting with others. The page known as Settings & Privacy is organized into six sections to assist users in viewing and modifying their account information, privacy preferences, ads settings, and communication notifications quickly. The 'Settings & Privacy' page enables users to manage their account settings, update their privacy and security settings, and set their preferences for contacting their followers. At the top of this page, users can see an overview of their account details, including their profile headline, number of connections, and details about the premium accounts they currently have. If the user account has been compromised or hacked, their immediate recommendation is to change the password through the change password option available to the user within settings.

They also explain how phishing emails can put the account at risk. Usually, such phishing emails are not addressed directly to users but advise recipients of the mail to act in hurry, usually to open an attachment and act as directed. Reporting incidents on LinkedIn is not only simple but efficient too. The user can do this by going through the other person's profile and clicking on the More icon and then on Report. Various options such as suspicious or fake are available to choose from. In fact, with the help of this procedure, many different incidents can be reported on LinkedIn. They have also explained the TFA feature provided by them to access the account, which is known as Two-Step Verification. This provides an additional level of security to establish the legitimacy of the account. To prevent any malicious attempts to access their account, LinkedIn strongly recommends its users enable this feature. Usually, the two-step verification is done through the user's mobile phone.

TikTok

TikTok has also taken several steps to safeguard the accounts of its users; under the option Guides, users can find much information for protecting their data in TikTok. They also collect mobile numbers and emails from their users to provide the latest updates to them. This also helps when the account is compromised or hacked. Moreover, TikTok insists on creating a unique and robust password so that others cannot easily guess it. They also provide an example to create a strong password by using special characters, numbers, as well as alphabets. The two-step verification is mandatory for safeguarding the user's

account. Users can also verify the devices when they attempt to access from other devices, essentially to keep the account safe. TikTok also educates its account holders to thwart phishing attacks to garner sensitive data from users. They insist on verifying the link before accessing the page as phishers may lure the account holder by offering them some gifts. TikTok has a simple procedure to report any incidents via the Help Centre page; moreover, users can report videos by holding down on the content and tapping Report (NCSC, 2019).

Training

Having SMPs in place is not just enough to manage the security and development of employees' behaviors; the organizations need to communicate these policies through training (Demek et al., 2018). Training is crucial because employees must understand why these policies are important for safeguarding themselves and their organizations. Training is the key to changing people's behaviors and perspectives, which is necessary for reducing any cyberattacks (Löffler et al., 2021). According to Chowdhury & Gkioulos (2021), robust security training is an organization's biggest investment, it is a non-technical approach to protecting the system and users from cyber-attacks (Edgar & Manz, 2017). In a way, cybersecurity training is an effective approach, which helps in eliminating the usual mistakes of users – difficult to achieve by any technological solutions.

Users must be trained for using social media security settings to combat cyber threats. Updating on these aspects periodically is as necessary as original training itself. According to Wisniewski et al. (2017) almost 48% of Facebook users are not aware of how to use privacy settings provided by the Facebook platform. At the same time, Nyoni & Velempini (2018) suggest simplifying not only privacy settings provided by social media sites but users need to be trained adequately to take advantage of it.

Demek et al. (2018) indicate that organizations resort to training to ensure that employees follow set policies and plans. Subsequent training sessions may be organized as per the needs of the employees. It becomes necessary for an organization to train its staff members to apprise them about the risks involved in using social media platforms. Employee training should be extensive covering all major topics such as social engineering, strategies adopted by hackers, insecure software as well as a variety of cyber threats associated with social media.

Understanding malware behaviors, reporting potential security threats, supporting or-

ganizational IT policies, and complying with major regulations (HIPAA, GDPR, PCI DSS, and so on) fall under cybersecurity awareness training (CSAT). Researchers indicate that training helps employees not only to understand information security issues in the larger context but realise the consequences that arise due to a lack of security awareness (Stefaniuk et al., 2020).

Thus, the primary purpose of CSAT is to raise knowledge and empower employees to recognise, impair, and report any cyber-attacks (Aldawood & Skinner, 2019). CSAT relates to specific user learning that allows employees to know all essentials about cybersecurity and IT systems including regulatory compliance. CSAT and learning are imperative to enable end-users to make knowledgeable decisions and approach cyber threats (Tsokkis & Stavrou, 2018).

Training programmes that concentrate on raising the security awareness of employees make the firm stronger in responding to cyber incidents (Zwilling et al., 2019). Studies reveal that having sufficient training programmes for employees could be a significant factor in improving their compliance with the information security policies of organizations (Safa et al., 2016). In general, the main goal of security training programmes is to cultivate a positive culture of information security within the organizations (Glaspie & Karwowski, 2017).

There is no doubt that training is the first option for raising user awareness in many organizations. ENISA (European Union Agency for Cybersecurity, 2014) as shown in Figure 2.2, reveals that learners acquire only 20% of what they listen and read; however, they grasp almost 90% of what they have practiced. In short, training programmes apprise users of the techniques used by hackers in achieving their objectives (Alshaikh et al., 2018).

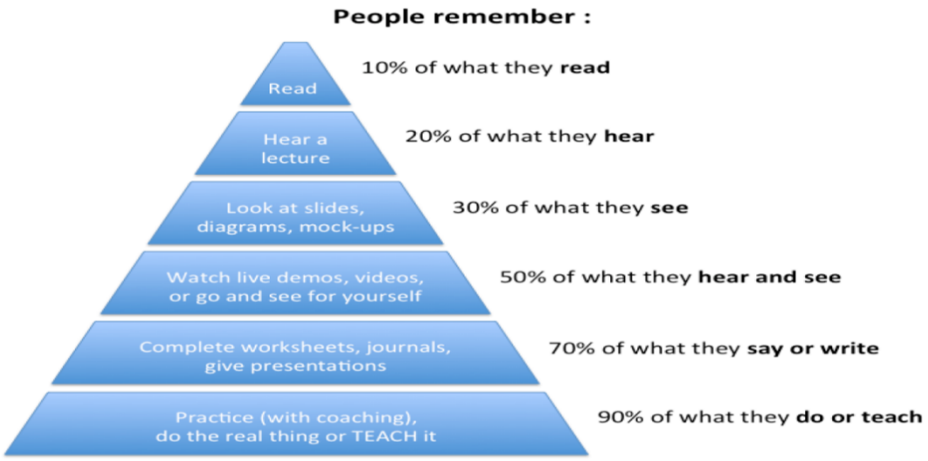


Figure 2.2: Learning pyramid (European Union Agency for Cybersecurity, 2014)

Also, CSAT programmes need to ensure users understand when and how they can be reached by the IT team. While the role of a CSAT programme is to tell people what to do in specific circumstances, they need to follow them even when an explanation is not available (Dugan, 2018). As such, a CSAT programme is organized for raising employees' security knowledge, and to create a generic awareness approach in an organization.

Cybersecurity Training Approaches

Whereas the focus of this study is on cybersecurity training as a defence against cyber risks, it is advantageous to comprehend the various training ideas and techniques.

Training methods and approaches are developed over time (Aldawood & Skinner, 2019). The ENISA has been working hard to make Europe cyber-secure since 2004, and it is active in the area of training and awareness, by using its expertise to support National Information Security (NIS) skills. Their training sessions combine lectures, education, guidance, exercise sessions, presentations, hands-on training, discussion, focused activities, etc. Also, they suggest a large number of training methods and tools that can be used as a medium in their training sessions as shown in Figure 2.3. In general, a security training approach should be such that organizations design a clear plan to train their employees, which leads to enhancing security awareness in them (Stefaniuk et al., 2020).

Figure 2.3: Training methods (European Union Agency for Cybersecurity, 2014)

Furnell & Vasileiou (2017) classify training approaches into two categories: Push and Pull. A 'Push approach' involves informing people what to do by using methods such as giveaways, penalties, and conviction. In contrast, the 'Pull approach' rests on motivating or encouraging people to do what is necessary. However, the success of security training depends on the methods being used to deliver information to the trainees (Edgar & Manz, 2017).

As shown in Figure 2.4 the ENISA classifies training approaches into three groups: Online, hybrid, and offline. Videos, online training sessions (Ghafir et al., 2018), social media, emails, games, webinars, , intranet, screensavers, video conferencing (Ghazvini & Shukur, 2016) are 'online approaches'. Conduct mock attack, run scenario, drills, war-gaming exercises, stories of good practice, rewards, tip sheets, FAQs are classified as 'hybrid approaches', and group training sessions, flyers, workshops, external expert lectures, posters, events, fall under 'offline approach' (European Union Agency for Cybersecurity, 2017). Moreover, presentations, regular meetings, reports, all form part of offline training approaches (Safa et al., 2016; European Network and Information Security Agency (ENISA), 2019). These information is compiled in Table 2.1.

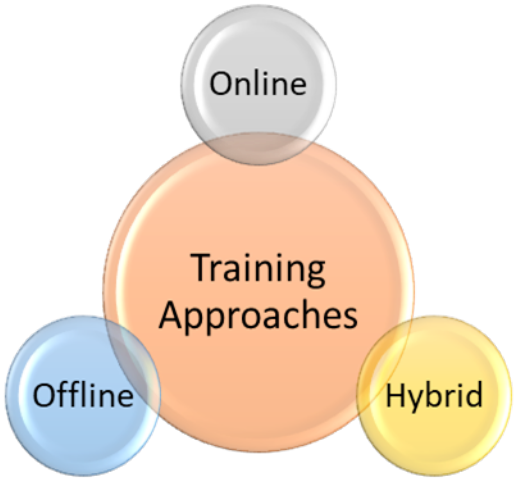


Figure 2.4: Training classification by ENISA

Table 2.1: Training classification by ENISA

Online	**Hybrid**	**Offline**
Social media	Conduct mock attacks	Flyers
Online games	Rewards	Workshops
Videos	Tip-sheets	External expert lectures
Webinars	Run scenarios	Posters
Online training sessions	Rehearsal	Events
Intranet	War-gaming exercises	Presentations
Screen saver	FQs	Reports
Emails	Stories of good practice	Meetings

Many people prefer the offline training method because it allows them to share insightful ideas, have fruitful conversations, and receive prompt feedback (Siami Namin et al., 2016). Pedley et al. (2020) reports that physical training is still frequently seen as the most effective method of luring trainees. However, the online system is used by many global companies for employee cybersecurity training, whereas others argue that a hybrid training approach blends online and offline approaches, and some organisations prefer it. However, despite a variety of training approaches available, the same mistakes are being repeated consistently (Furnell & Vasileiou, 2017). Existing methods do not cater to all different types of employees, their learning objectives, and learning styles (Caulkins et al., 2016; Christopher et al., 2017).

Thus, the following section aims to investigate the factors that lead employees to adapt more to cybersecurity training and learning, which might assist me in achieving the project's key goals.

2.4 Factors Supporting Adaptive Cybersecurity Training

2.4.1 Training Delivery Approaches

As per European Union Agency for Cybersecurity (2014), an effective training session on cybersecurity aspects should have several elements that include a brief introduction, real-life stories, videos, games, group activities, and competition between learners as well as analyzing real case studies along with discussing why certain policies on cyber issues have been enacted. A proper mix of training delivery approaches has been deemed to be not only advisable but indispensable (Alshaikh et al., 2018; Schürmann et al., 2020; Zhang et al., 2021). The authors of this project agreed on that, still, I will look further into why people favour one training method over another. As such, I will analyse these differences based on several aspects.

Ki-Aries & Faily (2017) shows that when cybersecurity training focuses on specific awareness topics such as password protection, it becomes more effective. At the same time, it is equally crucial how the training is delivered. Based on the experiment to discover the user preferences between three varied – namely video-based, game-based and text-based training approaches, Ki-Aries & Faily (2017) reveal that merging delivery methods produce much better outcomes than using a single way. However, they emphasize that each method must cover the same topic for achieving desired objectives. They further state that the game-based approach is the preferred way of learning IT security topics such as phishing.

It is obvious that people differ in their choices for the training approaches they receive. However, I will go beyond merely demonstrating that and proceed to explore how, why, and to what extent employees favour a particular training style.

2.4.2 Customising the Training

Numerous studies have found that customized cybersecurity training is preferable to a one-size-fits-all method, for example, it should be customized to fall in line with organizational goals and circumstances (Glaspie & Karwowski, 2017) such as business needs, budgets, organization vision, mission, culture (Bada & Nurse, 2019). On the other hand, mandatory and one-size-fits-all approaches routinely fail to encourage staff (Zhang et al., 2021).

Indeed, Furnell & Vasileiou (2017) claim that the training is more effective when employees feel that it is tailored to them.

It needs to be noted that there is no uniform training for cybersecurity. While cybersecurity training needs to be based on the roles or responsibilities borne by the person in an organisation (George et al., 2020), the training aspects vary as simple users' may need only basic knowledge but at the same time, intense users may need detailed hands-on training with a clear understanding of the gaps and vulnerabilities that exist in the system.

Zhang et al. (2021) suggest that organizations need to be more sensible in developing a clear strategy for funding cybersecurity programmes. They assert that the cybersecurity programme is a long-term investment and not an expense. Care needs to be exercised in that the cybersecurity programme does not become a generic version because every individual has a distinct job role to play and different responsibilities to discharge within the organization, and their awareness and knowledge levels vary too significantly.

It follows that customized cybersecurity training is superior to standard training. However, studies have not yet looked at how tailoring ACST should be concerning social media and human factors, including age, gender, work experience, educational level, and academic qualifications, as well as other online behavior patterns, which is what this study aims to accomplish.

2.4.3 Trainers

While factors contribute to developing a successful training programme, trainers have a huge role to play in increasing the enthusiasm towards the learning process (Brilingaitė et al., 2020). ENISA has been working on enhancing the network security by raising knowledge of users for which they mainly focus on "trainers" who are the backbone of the training sessions (European Network and Information Security Agency (ENISA), 2012). As per the ENISA, professional trainers are necessary for conducting effective training of the participants. At the same time, many researchers focus on 'trainees' to bring positive outcomes in terms of learning (Antonaci et al., 2017; Safa et al., 2016). While "trainers" are crucial for delivering productive training programmes, they are the masters who own the sessions for positive outcomes (Taniuchi et al., 2018). Researchers argue that having qualified and skilled trainers in the cybersecurity domain is a must for improving the situation dramatically; in fact, trainers influence learners' opinions significantly (Javidi

et al., 2019).

While comparing three training formats (computer-based, instructor-based, and text-based) Stockhardt et al. (2016) discover that instructor-based training is the most efficient way for increasing security awareness; however, it consumes more time than the other two methods.

Studies have shown that having skilled trainers is crucial for achieving training objectives. However, I will look at the qualities that make an excellent trainer to assist top management in choosing their trainers, whether inside or outside the organization. To find a solution that could underestimate the challenges those trainers experience at work, I will also investigate that by conducting interviews with some trainers and trainees.

2.4.4 Straightforward, uncomplicated, and simple Training

The key to practical cybersecurity training is to be short, periodic with regular breaks, and clear in meaning with no technical terms (Ghafir et al., 2018). As such, Bada & Nurse (2019) discuss the importance of having a training methods that are free of any complexity and easy in comprehension for all participants. It is clear that the training's simplicity may impact its success. I will investigate this aspect in more detail. Further, I pay close attention to social media cybersecurity.

As it is crucial to understand that security training programmes should be organised periodically and not as a one-time exercise because technology keeps on updating and so are the ways of hackers (Clark & Hakim, 2016). On this, the authors of this project were in agreement, but as I will see later, it is crucial to follow up with trainees on a regular basis. To illustrate this, I will examine trainee behaviour using a variety of evaluation techniques.

Demek et al. (2018) arugue that employees need to be trained throughly on cyber policy, and these policies need to be clear and easy to implement for enhancing their effectiveness. This is consistent with our study, as I will demonstrate later, our test's questions will be simple, free of ambiguity, and based on recommended SMPs and best practises.

2.5 Human Aspects in Cybersecurity Training

Given that there are differences in numerous demographic parameters, including age, gender, work type, and level of experience, I hypothesized that human factors played a major impact in the degree of adaptability in cybersecurity training. Their attitudes differ from one another as well.

Studies demonstrate that technical solutions and procedures cannot secure digital systems alone, and a human factors analysis is essential in cybersecurity (Jeong et al., 2019).The study of human factors examines how people behave physically and psychologically in connection to various situations, activities, and assets. As such, no training programme will elicit desired results unless it is designed uniquely to change the behavioral aspects of users; such behavior poses serious challenges for firms in tackling cybersecurity issues (Aldawood & Skinner, 2019).

When people are the most vulnerable link across the cybersecurity landscape, a human-centric approach to cybersecurity training, such as the one proposed by George et al. (2020), has greater chances to succeed. As such, the human factor needs to be strengthened in the cybersecurity domain compromising cybersecurity effectiveness; however, to minimize its adverse effects, it is required that security awareness is raised among users or employees as one of the topmost priorities by management (Ghazvini & Shukur, 2016).

The subsections below therefore concentrate on these human variables and how prior research takes them into account with cybersecurity.

2.5.1 Age

Furnell & Vasileiou (2017) argue that security training will be effective if the employee feels that the session or the course was tailored uniquely to them; generalization tends to give the impression that this is not their responsibility. The point is that strategies for young and old will differ due to their varying approaches and understanding of these aspects. Since younger users have weaker scores on measures of security awareness than older peers (Hadlington, 2018) they are more vulnerable to a phishing attack and could trick easily. At the same time, Hadlington (2018) and George et al. (2020) argue that taking on cybersecurity issues at an early age helps establish a strong foundation among users in tackling the menace effectively. However, Saridakis et al. (2016) and Blackwood-Brown

et al. (2021) asserted that cybersecurity training is more important for older people than younger ones as they are more prone to get trapped in cyber-attacks.

Furnell & Vasileiou (2017) have argued that security training must vary according to the age of the trainees, because different age groups have varying preferences and understanding of cybersecurity. However, Furnell & Vasileiou (2017) did not study the problem specifically within the context of organisations with a presence and operations on social media, which is what I intend to do.

Another age-related study carried out by Hadlington (2018) suggests that younger people are more vulnerable to phishing attacks than older ones, likewise, elderly individuals require greater cybersecurity training than younger individuals (Saridakis et al., 2016; Blackwood-Brown et al., 2021). As I will show later, this corroborates our findings. However, I have not limited our analysis to phishing attacks, and I will attempt to correlate different age ranges to other cybersecurity issues that are also part of social media.

2.5.2 Gender

So will be the case when strategies are devised specifically either for males or females. According to Anwar et al. (2017), 'gender' is, in general, an influential factor in deciding individual behaviors, and therefore, these factors need to be considered while designing the security training programmes. Researchers indicate that women and men are not comparable in their adoption of information technology and related security protocols (Lin & Wang, 2020). Studies show that women are not only more likely to comply with privacy policies but also more concerned about privacy than men (Anwar et al., 2017). Dhakal (2018) proposes that women are more conscious of information security awareness programmes and more excited toward security protocols than men. At the same time, they are more likely to be a victim of cyber-attacks than men. As such (Parker & Flowerday, 2020) found that women are more prone to phishing attacks on social media than men. While females have been observed to display weaker password creation behavior, they, therefore are more prone to a cyber-attack. Lin & Wang (2020) maintain that women engage more than men on social networks and form closer social bonding; distinct cultural and social norms and societal expectations also play a pivotal role in different behavior patterns of individuals on social media. However, studies have not adequately demonstrated why these variations in genders exist. Consequently, I plan to carry out that in our study.

2.5.3 Background and Expertise

Individual background and prior experience/expertise towards cybersecurity play a vital role for people while approaching security risks issues. For example, those with IT backgrounds are invariably interested in knowing how a cyber-attack can be executed. At the same time, people active in social sciences will attempt to focus more on behavioral aspects of the attackers (George et al., 2020). It needs to be noted that people, in general, tend to take security risks as only the side-effects of the incidents and tend to find the solution differently (George et al., 2020). Precisely for these reasons, cybersecurity training approaches need to be geared based on the background and expertise of the people involved in the tasks (Pedley et al., 2020).

Similarly, it is not appropriate to claim that a specific organization is having a higher level of security awareness than others (Ghazvini & Shukur, 2016), especially when user skills are not matching in cybersecurity concepts within the organization (Gratian et al., 2018). Studies reveal that employees possessing expertise in the IT field are more familiar with cyber threats than others (Jeske & Van Schaik, 2017). Raising awareness of cybersecurity among technical and non-technical personnel run differently. People with IT training perceive the performance of security software to thwart cybersecurity attacks quite differently when compared with people with a non-IT background as the latter view them only as a list to do or not-to-do or simple guidelines (Gasiba et al., 2021).

Therefore, a person's individual background and prior work experience play a vital role when addressing cyber risks, as stated by George et al. (2020). Thus, I have gathered information from different employees in various organisations working in different sectors and having diverse backgrounds. Our findings encourage the utilisation of training approaches geared towards the background and expertise of different employees, which is what Pedley et al. (2020) suggests too.

2.5.4 Job Roles and Sectors

Job roles and responsibilities do have their influence in dealing with cybersecurity risks. Technology, information systems and their applications have a different bearing on the people employed depending upon the roles or responsibilities they hold in the organization (Toth & Klein, 2014). For example, Nifakos et al. (2021) argue that healthcare

professionals such as doctors, nurses or medical support staff pose higher risks to their organizations when they interact with social media platforms providing hackers excellent opportunities to conduct cyber-attacks and extract sensitive details of the organization.

It is important to notice that CSAT is not equally widespread across all the sectors of the economy for the simple reason those cyber-attackers have their preferences while targeting these sectors. For example, the finance sector is the most preferred area (44%) for cyber-attacks followed by the information and communication sector (28%). The administration sector (3%) is the least preferred sector for cyber-attacks (Pedley et al., 2020).

While I agree with Nifakos et al.'s observations, I am also interested in learning about other sectors of the industry for example, the military, art, design, sport, and financial sectors. Thus, I have endeavoured to collect information from employees working on a wide range of organisations performing many different roles.

2.5.5 Attitudes and Behaviors

Human attitudes that include behaviors, values and preferences play a critical role in becoming vulnerable to cyber-attacks (Pattinson et al., 2018). According to Van Schaik et al. (2018), user attitude, habits such as time spent on social media, and perceived risk collectively decide their behavior on social media platforms. The users who use social media platforms for exchanging information are more likely to be victims of cyber-attacks. Hadlington (2018) suggests that the users who ignore security-related warnings have higher chances of victimization from cyber-attacks; this includes also those who are addicted to social media.

To further understand this, I have distributed an online survey, which features specific sections about attitudes and behaviours. In turn, the findings derived from these sections allow me to formulate a risk equation 7.1 to assist policymakers, cybersecurity formulators, and trainers to prioritise training for those who need it the most, and Chapter 7 will go into more detail about this formula.

2.6 Chapter Conclusion

This chapter examines how social media cybersecurity risks are real and so are the tools that are employed to thwart such threats. Threats have been identified to have many forms such as malware attacks, Sybil attacks, phishing attacks, impersonation, identity fraud, and so on to deal with. While technology alone cannot prevent social media cyber-attacks, non-technological tools could be handy to make users aware and equip them to be able to identify and thwart different kinds of cybersecurity threats for safeguarding themselves as well as organizations.

As such, mere technological solutions cannot prevent cyber incidents, but skillfully formulated training programmes are crucial for raising awareness of the employees towards cybersecurity threats. While training formats with mixed delivery approaches tend to provide superior outcomes, ENISA supports online, offline and hybrid approaches as well.

Therefore, cybersecurity awareness is a must for all levels of users so that they can recognise and report the incident as and when any threat is encountered. In the current times of the ever-developing era of technology, raising awareness is no more optional. Most experts now emphasize that user skills in the aspects of cybersecurity can be improved through training.

In conclusion, this chapter examines the previous studies and sets a tone for analyzing and using factors responsible for ever-increasing cyber incidents, and how users adapt to cybersecurity training differently based on many factors. These variables aid in offering more customized cybersecurity training based on valuable reviews and statistics.

The chapter shows how age, gender, employment type, and level of expertise are just a few examples of human aspects that significantly impact how adaptable cybersecurity training can be.

The following chapter will discuss the data collection process and methodologies used to investigate the challenges of cybersecurity training for social media. The investigation will examine different groups of social media users to understand their awareness level, needs, and objectives, as well as the current practice towards cybersecurity training for social media. The following chapter will involve the design of a survey and interviews process from key stakeholders, which will give me insight into the extent of the problem.

Chapter 3

Methodology

This chapter specifies the methodological strategy and procedures chosen to answer the questions of this study. The sample size is described, and the participants selection process is explained. The reliability, interview methods, coding procedures and interviews scenarios are discussed initially. The methods used for distribution and collection of the survey and interviews are discussed. Statistical treatments of the survey are outlined.

3.1 Introduction

In order to examine the proposed framework for this project, I employed a "theory of change approach". Theory of change as defined by Weiss et al. (1995) is how and why an initiative works. In this work, I analyze both quantitative and qualitative investigations, as well as theoretical literature, using a comprehensive systematic review (Aromataris & Pearson, 2014). The purpose of using this strategy is to shed light on how and why the adaptive cybersecurity training for social media is beneficial. This theory was selected for this project since it is straightforward and would produce both short-term and long-term results. To fulfil our intend, I moved forward through the following three stages: I am first developing a theory of change that attempts to improve people's social media cybersecurity behavior. Second, I evaluated the framework's tasks and desired effects, which will all be covered in Chapter 8. Eventually, I analyze and interpret the evaluation's findings, including how they may need to be modified in terms of the initiative's theory of change and resource allocation.

3.2 Research Approach

Our research design essentially consists of employing two research methods simultaneously that are popularly known as qualitative and quantitative research methods - often known as mixed methods (McKim, 2017). I applied a mixed approach to generalize the results and define a behavior or concept's meaning for different people (Creswell, 2003). In the qualitative study, I have decided to conduct in-depth interviews. This will help me enrich quantitative findings obtained by serving a questionnaire to participants for understanding the issues involved in adaptive cybersecurity training along with many other objectives as listed earlier. This kind of research methodology will also lead me to an in-depth understanding of cybersecurity training-related issues that users face on social media.

3.3 Survey

Based on the fact that the majority of organisations rely on social media to complete their work, the limitations of the studies that focus on social media users in the workplace, the rising number of social media-related incidents, and the indication from previous research that people have varying responses to cybersecurity training and cybersecurity awareness approaches, I came up with the questions for this survey.

This survey's questions were designed and structured with three primary concerns in mind: why is adaptive social media cybersecurity training so important, how could we conduct adaptive cybersecurity training for social media risk, and what does adaptive mean?

As such, the survey was arranged to take a broad view of the participants. The survey's design was based on the necessity to recognise employees' observations of cybersecurity threats and privacy matters with the use of social media.

I use the quantitative methodology for two purposes; first, to discover the correlation among different factors in the proposed framework and, second, to recognise the strength of analytical techniques such as relationship and group analysis. Furthermore, by this method, I can hold a foundation for comparing our analysis with others, and future studies can examine their results with our research.

I requested employees to engage in the online survey about their practices and experiences with the use of social media and their training backgrounds in this area. I asked questions about their thoughts on overall social media usage. MY questions aimed to recognise the participant's perceptions of the training in general and the cybersecurity training in particular (to review the survey questions, please see 9.3). I selected this approach because electronic surveys have the benefit of facilitating data collection and analysis (Castro, 2018).

The targeted participants were Kuwaiti employees who work in Kuwait industries, using social media, and are above 18 years old. I sent out our online survey to employees in numerous organisations.

Due to the sensitive nature of our work, I undertook the ethical review process required by the *University of Plymouth*, which is where I was based while conducting our investigation. The ethical review was recorded through the *Plymouth Ethics Online System* (PEOS) (University of Plymouth, 2022), and the approval was granted on 5 September 2020. Prior to distributing our survey, a pilot test was carried out among ten people to analyse the survey's feasibility and the adequacy of our questions. Abiding by the University of Plymouth's ethical approval policy, the survey was conducted in complete anonymity.

My Google Forms survey was sent to 55 management contacts at various Kuwaiti organisations. I requested that these contacts distribute the survey to employees who met the research criteria and were potentially willing to participate. The survey was available for 41 days, from 5 September 2020 to 17 February 2021, after I received ethical approval.

The survey was developed in English and consisted of 25 questions. The survey instrument was comprised of four sections.

The first section: Introduction and right to withdraw

This section consisted of a brief introduction about the project aims, the participant's eligibility, the time required to complete the survey, and their right to withdraw.

The second section: Focus on Demographics and attitudes

This section consisted of sixteen questions, started with questions about demographic details, and ends with training approaches preferences. Demographic questions were used as crucial variables and examined if awareness was distinctive for people of different backgrounds. Demographic items that were added as control variables include questions

on age, gender, academic status, job role, and work experience. Attitude to social media is crucial in this study, as these sections involved many questions that assess this area with different styles of questions.

The third section: Cybersecurity Training Feedback

The third section consists of four questions that focus on those who have had cybersecurity training. I need to identify more information about this cybersecurity training they attended, where they got this training or learning, how many times a year, what was the training approach, and if this training includes any social media references.

The fourth section: Cybersecurity Training Perception

This section consists of three questions and aims for those who never attended cybersecurity training; yet our objective is to identify the most cybersecurity struggling areas and their perception about cybersecurity training.

I used mixed types of questions for this purpose: multiple choice, checkboxes, short answers, and a five-point Likert Scale. Then the survey ended with a message asking for permission to pursue further investigations (interviews) and requesting their contact details if they approve (more details can be seen in Appendix 9.3).

3.3.1 Sample Size

Since this study essentially attempts to explore how far the staff members in the organisations in Kuwait are aware of matters of cybersecurity (especially when they interact with other people on social media), it becomes imperative to find out statistics about the organisations. As per the Central Statistical Bureau 2018, there were 401,057 employees in Kuwait's public sector (Kuwait Central Statistical Bureau, 2021). It is interesting to notice that there is a significant gender difference among employed staff in firms within Kuwait. To elaborate further, there are only 129,688 male employees against 185,228 female employees. The largest group of the employees (22%) belong to the 30-34 age group. While 45% of the employees hold a bachelor's degree, the lowest percentage (12%) have less than secondary school as their qualifications (Kuwait Central Statistical Bureau, 2021).

I used Excel to calculate our sample's confidence interval for population mean. The result of the z-values is from 2.76 to 2.92, which represents a 99% confidence level (Calculator.net, 2022). Accordingly, the recommended sample size is 542 participants, yet I reached 641

participants (the following chapter will cover details about the participants).

3.3.2 Survey Reliability

Reliability is the way to measure the quality and consistency of data obtained. It indicates the consistency of the results when several participants work under different circumstances. The internal consistency here is *good* as the overall reliability range is .888 (De Swert, 2012). Further details are given in Table 3.1.

Table 3.1: The initial reliability test results

Scale	**Items**	**Cronbach's Alpha Coefficients**
Attitudes	5	.384
Behaviors	5	.713
Preferences	13	.895
Perceptions	4	.920
Cybersecurity training	6	.886

3.4 Interviews

3.4.1 Interview Methods

In this study, I aim at filling the gap between literature review and practical experience to obtain a deep, holistic range of knowledge. Thus, I complemented the survey with in-depth interviews with relevant people who were policymakers, involved in training formation, and those who have attended cybersecurity training (pls refer to Appendix 9.3 for more details).

To capture thoughts on our research questions, I conducted in-depth, semi-structured interviews with individuals from different institutions in the state of Kuwait under conditions of strict anonymity. The subjects belonged to organisations of diverse activities and sizes. I conducted interviews using scenarios that helped to create an adaptive cybersecurity training system for social media.

Our interview questions were divided into three sections; each section has its unique questions that aim to a specific objective. At the beginning of the interview, I set ten items that can show me the participants' backgrounds, such as age, gender, etc. Then, the first

section targeted those who set policies in the organisations and training formation. I asked ten questions to policymakers, and five to training formation. The second section is for those who attended social media security training, I provided nine questions. Cybersecurity training does not necessarily include social media threats topics, and some people, especially those with IT backgrounds, attended technical cybersecurity courses that do not refer to social media, so that, the third section targeting those who attended cybersecurity training and did not necessarily include social media issues, and it was nine questions at all. At the end of the interview survey, I set ten general questions that targeted all the participants and asked general questions about cybersecurity and social media knowledge.

Three trial interviews were carried out for each part of the interview questions, one from policymakers, one for training formation/trainer, and the last was from cybersecurity trainees. Those interviews were not part of the 25 main participants, and they were aimed to test the research questions' cogency and possible replies from expected participants.

The interviews took place over Zoom and lasted approximately thirty to forty-five minutes. It should be noted that the interviews were in English, friendly, and progressed smoothly I started arranging our interviews at the time I received the ethical approval letter. As shown in Table 3.2 the first interview took place on the 12th of Sep 2020, and the last one was on the 15th of Oct 2020.

Table 3.2: Interviews data collection process

Timeline	**Data Collection**	**Data Analysis**	**Analysis Method**
June 2020	3 pilot study interviews		
12 Sep-15 Oct 2020	25 in-depth interviews	Initial codes Focused codes	NVivo software

3.4.2 Subject's Background

Since our study focuses on how an adaptive cybersecurity training approach can help enhance the security awareness of users, I decided to conduct interviews with a specific set of people that largely formulate social media policies in their organisations. At the same time, I realized that setting in-depth interviews with those who have undergone cybersecurity training is more likely to help me achieve the aims and objectives of our

research.

With the realization that many of the interviewees are experienced in cybersecurity training and these trainings were including social media issues, I split our trained interviewees into two groups or categories: one group of people with IT expertise, and the other group of people with a non-IT expertise. More details about these interviewees in terms of gender, academic qualification, and job roles can be seen in Table 3.3.

Overall, these interviewees can be divided into the following three categories:

-the first group: policy makers, and training providers (11),

-the second group: trainees with IT expertise (7),

-the third group: trainees with non-IT expertise (7),

Table 3.3: Interviewees' background details

Policymakers & Training Formation/Trainers				
ID	Age	Gender	Education	Years of experience
1	43	M	Master	4
2	29	M	Bachelor	2
3	35	M	PhD	10
4	44	F	PhD	21
5	54	M	Bachelor	4
6	56	M	PhD	6
7	53	M	Master	17
8	38	M	Bachelor	13
9	36	M	PhD	3
10	56	M	PhD	18
11	4	M	Master	16
Cyber Security Trainees (IT Backgrounds)				
12	39	F	Bachelor	16
13	31	F	Bachelor	1
14	35	F	Bachelor	10
15	45	M	Bachelor	15
16	38	M	Bachelor	17
17	31	M	Master	3
18	27	M	Bachelor	2
Cybersecurity Trainees (Non-IT Background)				
19	37	M	Bachelor	15
20	52	F	Bachelor	22
21	35	F	Master	10
22	25	M	Bachelor	2
23	36	F	College, but no degree	15
24	37	F	Bachelor	5
25	34	M	College, but no degree	4

3.4.3 Scenario-based Interviews

Before each scheduled interview, interviewees were informed about the outline of the interview by email, so that a semi-structured, exploratory interview could be conducted. For this purpose, I used the *Zoom* platform for recording the conversations. As the interviews developed into fruitful conversations, the participants professionally shared their experiences, referring to situations they faced related to cybersecurity. In line with the expectations, each of them had different and varied scenarios to share with me. After finishing the interviews, the recorded data was collected, transcribed, and analyzed thoroughly.

While all interviews began by asking about the participants' background, it is important to note that the four distinct groups of interviewees were served with different sets of questions. This is to facilitate the construction of different scenarios matching with their past experiences, as each group can help me to reach the objectives of this study. Every attempt was made to construct a unique scenario with these participants so that their insight based on their past experiences could be evoked in the best possible manner. A detailed conversation with them could also enlighten me about the current cybersecurity training practices followed and some key challenges faced by their organisations for effective outcomes.

While the questionnaire was classified by topics that include background, knowledge, attitudes, practices, history, challenges, and preferences, open-ended questions helped me to evoke wide-ranging responses from the participants. While 10 general questions were asked to all participants, specific groups, such as policymakers and training providers, were interviewed on as many as 25 items, and those who attended cybersecurity training related to social media before were interviewed on 14 items.

Background

All participants were asked some basic background questions – essentially these questions related to demographic information such as age, gender, educational level, work experience, and job role. The purpose of these questions was to identify the impact of these factors in cybersecurity awareness and its relationship with demographics. Moreover, this understanding is also likely to pave the way for designing an adaptive cybersecurity training system for social media users.

Knowledge

Users' knowledge of cybersecurity threats, mainly social media risks, has been one of the crucial determinants for exhibiting safe behavior when they remain active on social media. It is quite obvious that the ability to act safely on social media is diverse among people. In this sense, it is important to know if the chosen participants possess knowledge regarding matters related to cybersecurity and whether they exhibit safe behavior while using social media. Moreover, it is important to know if they conceive and enforce cybersecurity-related protocols in their day-to-day functioning. Further, I wanted to check if cybersecurity training undertaken by them has enhanced their knowledge and awareness in this field. I attempted to develop specific open-ended questions, intended at evoking participants' responses about their social media cybersecurity knowledge, and ascertain if these questions remain relevant to them.

Attitudes

Usually, it has been discovered that much of the security-related behavioral aspects of participants have much to do with their attitudes. It is interesting to know how people react or behave in certain security-related events, such as cyber-attacks by hackers. I also want to know if an adaptive cybersecurity training system can make them more effective in tackling social media security-related incidents, and whether attitudes lead to forming certain habits that put them at risk, especially when they tend to select weak passwords for their social media accounts, or when they tend to defy certain security protocols while using social media sites.

Practices

It is equally important to know how employees approach social media security-related issues in their day-to-day activities. The questions under this topic have been designed to analyze staff behavior on social media. For instance, I want to know if policy makers create and set certain policies for their staff. If so, I need to ascertain if these policies have been effective enough to achieve their security objectives in their organisations. The questions related to these aspects also helped me to know how managements implement training processes to raise the security awareness of their staff. With some specific questions, I was also able to identify some challenges in this area, and, how social media security-related training helps staff members in changing their online practices.

History

Given that information on how victims of cyber-attacks fight back is scarce (Tapanainen, 2017), thus, it is important to know how participants faced incidents such as phishing, hacking, or fraud due to their attitudes or lack of proper behavior while working on social media. Jeske & Van Schaik (2017) assert that any familiarity with security threats makes people more knowledgeable than those who have never faced any such threats. Thus, knowing history about the security-related incidents can shed some light on the changes in awareness and attitudes of participants while working online. Additionally, knowing about cybersecurity training and confirming if such training met the trainees' expectations could help me to meet our objectives.

Challenges

As usual, challenges are likely to be many and varied for all stakeholders in matters pertaining to cybersecurity. For example, it is important to understand the hurdles faced by policymakers while setting SMPs within the organisation. Similarly, trainers have their own set of issues and obstacles in imparting effective training for their staff members. At the same time, trainees may fail to grasp some typical vocabulary used in the cybersecurity domain or the training methods employed by trainers. At times, the training atmosphere is not found conducive for those attending the training, resulting in an overall failure of the training programme. The point is that I have made serious attempts to identify such challenges and issues to meet our objective of developing adaptive security training programmes.

Preferences

Understanding individual training preferences is crucial for the success of any training programme. While several training methods including workshops, webinars, mock attacks, interactive games, case studies, quizzes, posters, online, presentations, posters, etc. are available, the crucial aspect is to find out which one is the most effective to successfully train participants. Apart from the training approach, the frequency of training programmes is equally crucial and cannot be ignored. Similarly, the duration of training sessions is also important so that neither they are too short for effective learning nor too long to bring monotony in the sessions. In short, the emphasis is on making the programme effective not only from the organisational perspective but also from the viewpoint of participants.

3.4.4 NVivo Software

Codes are known as the labels for specifying blocks of sense to the narrative or probable data gathered through research (DeCuir-Gunby et al., 2011). In this study, I used the NVivo software to facilitate our coding approach. I started with a blank sheet, without making any assumptions about what I was going to find in the data gathered through our interviews. I was completely open to letting the data speak to me. All the data collected through interviews was categorized and further segmented through the coding process. The coding process helps not only to map the data but also to have an overview concerning our research questions. The NVivo software programme has been employed for organizing, analyzing, and finding insights in the qualitative data collected through interviews.

In total, 25 participants were interviewed, separated into different categories, such as cybersecurity trainees, policy makers, and training providers (refer to Table 3.3). The preparation of memos during each interview process was diligently followed to avoid misinterpretation or miscommunication while using those data for our research findings.

3.5 Codebook

While there is no universally accepted coding procedure, qualitative researchers suggest beginning with a codebook, which involves a set of codes, descriptions, and symbols, to assist in analysing interview data. Matching patterns are identified and segregated for clarity and further scrutiny. In a way, coding is an iterative process to arrive at a certain conclusion (DeCuir-Gunby et al., 2011).

For easy and clear understanding, the codename/label, definitions along an example of each code have been tabulated in Table 3.4 below.

Table 3.4: Codes, Description, and Example.

Code Name	Description	Example

Adaptation	This code covers how trainers modify their training to accomplish desired results, and how trainees feel more adaptive during the training.	*"We have to make more than one group, a group for the basics, and group for the little advance, and group for professionals or who have experience"*
Awareness	This code outlines the methods used to increase cybersecurity knowledge, including awareness sessions and adhering to certain processes,	*"Cyber awareness is a continuous activity. During the COVID-19 lockdown periods as well, we conducted awareness sessions for our employees".*
Challenges	The code contains all the challenges and issues that the selected categories have encountered.	*"The big challenge is some employees feel that this is not their responsibility to secure their App, they think that this is another field or sector responsibility"*
Evaluation	This code specifies how policymakers verify that staff members are adhering to SMPs and how trainers evaluate the effectiveness of their training.	*"at the end of each training, we usually run a survey, some sort of asking questions to evaluate the trainer, the content, the training itself,"*
Format	This code contains all information pertaining to a cybersecurity training session that participants attended, and that instructor delivered, including (format, content, period, and satisfaction rating),	*"It is one day workshop last for two hours, I tried to make it short to be more effective and attracting because people get bored"*
Methods	All of the delivery techniques used in cybersecurity training, are included in this code.	*"It was like uploading videos and you can always watch them but if you have a question, you can go back to them"*
Factors	This code contains the factors that lead to adaptive cybersecurity training.	*"First I attract by the trainer, second the topic"*

Incidents	This code comprises all information about incidents that happened to the interviewees while using social media and how they handled them.	*"I restore my password through the administration of Twitter, and they told me that I have to put TFA for resetting my password, then I put my passwords and my email and my mobile number,"*
Policies	This code outlines the organisation's cybersecurity policies and how they were communicated to employees.	*"We can do such as workshops, and we do seminars, and we do like sending flyers and brochures through emails on monthly basis and that is all"*
Preferences	This code incorporates the cybersecurity training methods that learners favor and enjoy the most.	*"In class is nice because there is interaction, face-to-face, and any question raise to my mind I can ask"*
Suggestions	The interviewers' suggestions and opinions for improving the cybersecurity training system are included in this code.	*"Keep it simple, because people especially in our region they want something very simple and easy of use, if they feel that it's just a little bit complex, they will give up, and they will say oh we will not use it!"*
Struggling	This code covers the social media topics that people are interested in learning more about, having difficulty with, or needing training in.	*"The most important was social engineering and mobile hacking"*

3.5.1 Inter-rater Reliability Test

The interview coding system facilitates an investigation of interviewees and their replies in a single response. A co-occurrence review of the issues resulted in 10 combinations of the codes. Overall, the coders accepted 83% of the individual responses, with a multi-value nominal alpha coefficient (mvna = 0.803), meaning that coder-evaluated individual interview responses befell in place over 80% of the time controlling for the possibility of the agreement due to chance.

3.6 Chapter Conclusion

In conclusion, the purpose behind having a mixed method research design (a combination of qualitative and quantitative research methods) is to have an in-depth understanding of cybersecurity related issues that are faced by a variety of stakeholders, such as policymakers, trainers, trainees and general staff across organisations. Personal interviews brought forth many unforeseen scenarios that were not possible to discover merely through a quantitative study. Separating interviewees into three distinct groups of people helped me not only to understand many aspects of cybersecurity but paved the way for developing adaptive cybersecurity training programmes for social media users. Knowing about the participants' background, history, previous knowledge, attitudes, practices, preferences, and the challenges faced became essential to understand cybersecurity-related issues thoroughly. Summing up, an appropriate research design is crucial for moving closer to developing an adaptive cybersecurity training system, which is the aim of this project.

Chapter 4

Preliminary Results and Findings

This chapter presents the quantitative and qualitative results of the data analysis procedures that I described in Chapter 4. The background of the research sample and their use and perceptions of social media were presented first, followed by the analysis of their cybersecurity awareness. The Chi-square test was chosen to examine the relationship between our variables. The associations between every two variables are provided in a table followed by each sub-section in this chapter.

4.1 Introduction

Responses to the questionnaire were collected online through a Google form (Castro, 2018). Data were then entered and processed using the SPSS software (Yockey, 2016). In total, 641 people were served with the questionnaire and all of them have returned their answers.

4.2 Background of Research Sample

Responses to items on the data form were used to describe the characteristics of the sample and to develop demographic variables for the study of relationships between demographic characteristics and cybersecurity. All respondents have been working as employees in organisations in Kuwait, they are 18 years of age or above, and using social media. The demographic study of all respondents is shown in Table 4.1 below.

4.2.1 Demographics

The largest percentage of respondents in the sample belongs to the 26-35 age group, constituting almost 36% of the total. The lowest percentage of respondents belongs to the 18-25 age group, constituting almost 6% of the total sample size. In terms of gender, female and male respondents constitute 59% and 41% respectively. When it comes to educational level, 63% of participants reported having a bachelor's degree, and 1% reports having less than a secondary school education. While 23% are working in the education sector, which includes learning and training fields. Respondents working in sports and media, including art and entertainment, are 4%.

Table 4.1: Demographics data

Variable (s)		**N (%)**
Gender	Male	263 (41)
	Female	377 (59)
Age	18-25	37 (6)
	26-35	229 (36)
	36-45	226 (35)
	46-55	93 (14)
	55+	54 (8)
Education	Less than secondary school	7 (1)
	Secondary school	13 (2)
	Some colleges, but no degree	60 (9)
	Bachelor's degree	408 (64)
	Postgraduate degree	150 (23)
Job role/Discipline	Education, training, and library	153 (24)
	Computer and technology	92 (29)
	Healthcare support	20 (5)
	Leadership and management	158 (53)
	Business and financial operations	104 (47)
	Art, design, entertainment, sport and media	36 (18)
	Office and administrative support	114 (65)
	Military	72 (55)
Years of experience	Less than 2	23 (4)
	2-5	96 (15)
	5-10	119 (19)
	10-15	116 (18)
	15-20	119 (19)
	20-25	79 (12)
	25+	70 (11)

4.2.2 Social media usage

Within the questions of my survey that focus on the employees' social media behaviours; I aimed to determine how concerned they are with the privacy and security of their

social media accounts. Where public means they care less about their privacy on social media, private means more privacy; however, I assume they may not know whether their accounts are public or private, so I provide "Do not know," option,and of course, they may not be using this social media platform at all if they select "Do not use it."

In this study, it has been discovered that almost 73% of respondents have kept their Instagram accounts private. At least, 54% of the respondents do not use Facebook; almost 65% of the respondents do not use LinkedIn. In the case of Snapchat, almost 75% of the participants have kept their accounts private; WhatsApp accounts have been kept private by almost 53% of the respondents. Only 47% of the Twitter account holders have kept their accounts public, as summarized in Table 4.2 below.

Table 4.2: Social media status

Variable (s)		**N (%)**
Instagram	Public	153 (24)
	Private	469 (73)
	Don't know	1 (.2)
	Don't use it	17 (3)
Twitter	Public	317 (49)
	Private	203 (32)
	Don't know	11 (2)
	Don't use it	109 (17)
Facebook	Public	96 (15)
	Private	183 (29)
	Don't know	12 (2)
	Don't use it	349 (54)
LinkedIn	Public	130 (20)
	Private	43 (7)
	Don't know	26 (4)
	Don't use it	441 (69)
Snapchat	Public	74 (12)
	Private	479 (75)
	Don't know	7 (1)
	Don't use it	80 (12)
WhatsApp	Public	287 (45)
	Private	340 (53)
	Don't know	13 (2)
	Don't use it	-

The amount of time employees spend daily on social media platforms, and the device used to access social media are other aspects of employee social media behaviour that I aimed to examine concerning cybersecurity-related issues.

While investigating usage patterns, it has been revealed that almost one-third of the questionnaire respondents keep themselves occupied with social media for at least 3 hours

a day, and only 4% of them use social media for less than 30 minutes daily.

It should be noted that close to 39% of the respondents use their smartphones to access social media sites; a large proportion 71% indicate that they do not use a tablet to access their social media accounts. Similarly, 65% of the participants do not use a laptop/desktop for this purpose, whether from home or work, as shown in Table 4.3.

Table 4.3: Social media usage

Variable (s)		**N (%)**
Social media usage in a day	Less than 30 min	26 (4)
	30-60 min	61 (9)
	1-2 hours	167 (26)
	2-3 hours	172 (27)
	3+ hours	214 (33)
Using mobile phone to access social media	0	7 (1)
	1-2 hours	193 (30)
	3-4 hours	249 (39)
	5-6 hours	116 (18)
	6+ hours	75 (12)
Using table to access social media	0	452 (71)
	1-2 hours	144 (22)
	3-4 hours	27 (4)
	5-6 hours	7 (1)
	6+ hours	2 (.3)
Using home desk/laptop to access social media	0	418 (65)
	1-2 hours	148 (23)
	3-4 hours	44 (7)
	5-6 hours	20 (3)
	6+ hours	3 (.5)
Using work desk/laptop to access social media	0	427 (67)
	1-2 hours	104 (16)
	3-4 hours	64 (10)
	5-6 hours	28 (4)
	6+ hours	9 (1)

4.2.3 Cybersecurity Awareness

To determine the level of cybersecurity awareness among employees, I have formulated a series of questions. First, I looked into as to whether they had been the target of cyberattacks, and then we posed an open-ended question to learn more about the nature of the incident and how it was handled.

As per Figure 4.1, 78% of the participants confirm that they have not been exposed to any kind of cyberattack or security breach, and 5% do not know whether they were a target before or not, including the privacy of their accounts being compromised.

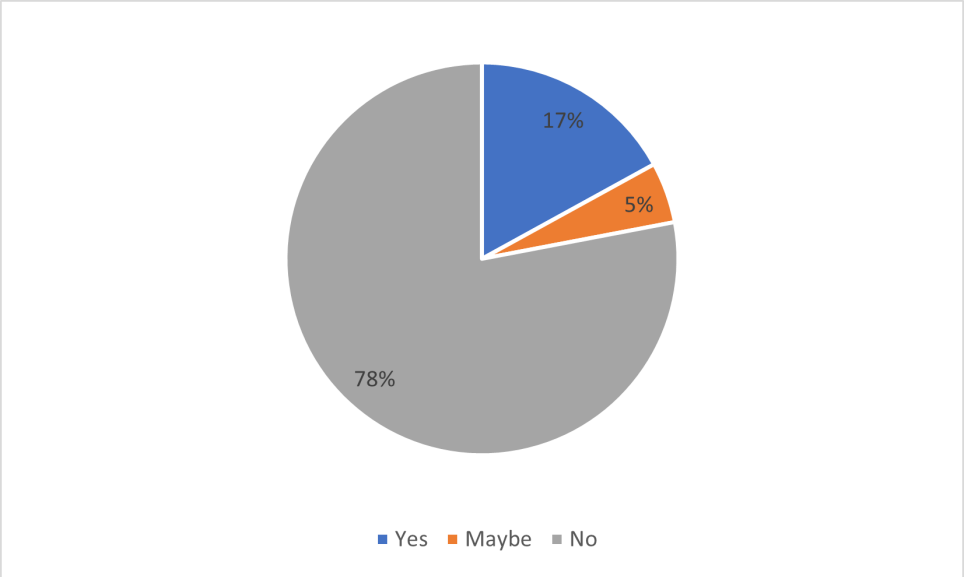


Figure 4.1: Being a victims to cyberattacks

The open-ended question: "If yes, please provide more details about the incident and how you combated this incident?" at the bottom of this question created qualitative datasets. This gave me more insight into employees' behaviours online.

The following are examples of responses received from 17% of respondents to this question: The majority of incidents involved finances; one respondent said, "My visa was stolen," while another said, "My bank card was stolen, but I refunded it immediately." Some participants were aware of the reason for this incident, yet they did it anyway, for example: "Yes, my credit card was stolen multiple times because I used an untrustworthy website for online shopping."

The impact of impersonation and identity fraud has also been demonstrated by this study; for instance, one respondent stated, "Hacker stole all my private pictures and

impersonated me to contact my followers." Another stated, "My Snapchat account has been compromised." Similar incidents occurred on other social media platforms, including Facebook, Twitter, Instagram, and WhatsApp.

This study's participants have also raised the issue of hacking for extortion; for example, one participant stated, "My email was hacked, and they threatened to delete everything on it if I do not pay them." "I was using public Wifi when I was attacked by a hacker who threatened that if I did not pay him, he would steal all my photos and data from my device," said an additional participant, indicating that she was aware of the incident's cause. Another stated, "My email account was compromised because I clicked on a link that was sent to me."

Those incidents served as a wake-up call to people that this is real and even if they survived this time, they may not survive the next. For example, one of the participants stated that he was unable to receive his money back from one of the Google accounts even after he stopped the credit card through the bank and raised the issue, which amounted to around 1,000 pounds, because the payment was made with the correct credentials. In response, the company requested that he submit a formal complaint. However, his money is not returned.

The survey posed five additional questions to gain a deeper understanding of the participants' general cybersecurity perceptions as shown in Table 4.4. At least 58% of the participants strongly agree that privacy and security are important to them. In total, 33% of the respondents strongly disagree with the phrase, "I am not responsible for my information security as it is the function of IT staff". At the same time, 31% of the participants disagree with the phrase. "Technology alone protection programmes can protect devices from being hacked". Close to one-third of respondents agree that they not only read but also understand social-media security policies. Accessing social media system settings and setting the available security options is a task clearly understood by 58% of the participants.

Table 4.4: Security perceptions

Variable (s)		N (%)
Privacy and security are important to me	Strongly disagree	6 (.9)
	Disagree	5 (.8)
	Neutral	29 (4.5)
	Agree	227 (35.5)
	Strongly agree	373 (58.3)
I am not responsible for my information security, as it is the function of IT staff	Strongly disagree	212 (33.1)
	Disagree	175 (27.3)
	Neutral	122 (19.1)
	Agree	116 (18.1)
	Strongly agree	15 (2.3)
Technology alone protection programs can protect devices from being hacked	Strongly disagree	99 (15.5)
	Disagree	200 (31.3)
	Neutral	158 (24.7)
	Agree	148 (23.1)
	Strongly agree	35 (5.5)
I read and understand security policies related to social media	Strongly disagree	60 (9.4)
	Disagree	112 (17.5)
	Neutral	201 (31.4)
	Agree	217 (33.9)
	Strongly agree	50 (7.8)
I know how to navigate the social media system setting and set the security options that are available	Strongly disagree	16 (2.5)
	Neutral	100 (15.6)
	Agree	374 (58.4)
	Strongly agree	150 (23.4)

In order to gain a deeper understanding of how employees react to phishing emails, the survey provided an invented email that could be phishing (as shown in Figure.4.2). This allowed me to gain a deeper understanding of how employees react to phishing emails. The survey provided respondents with the following four options:

1- I will click on the blue button to view the policy

2-I will ignore it

3-I will report it as spam

4-I will contact the HR department through a separate email thread asking about the new benefits

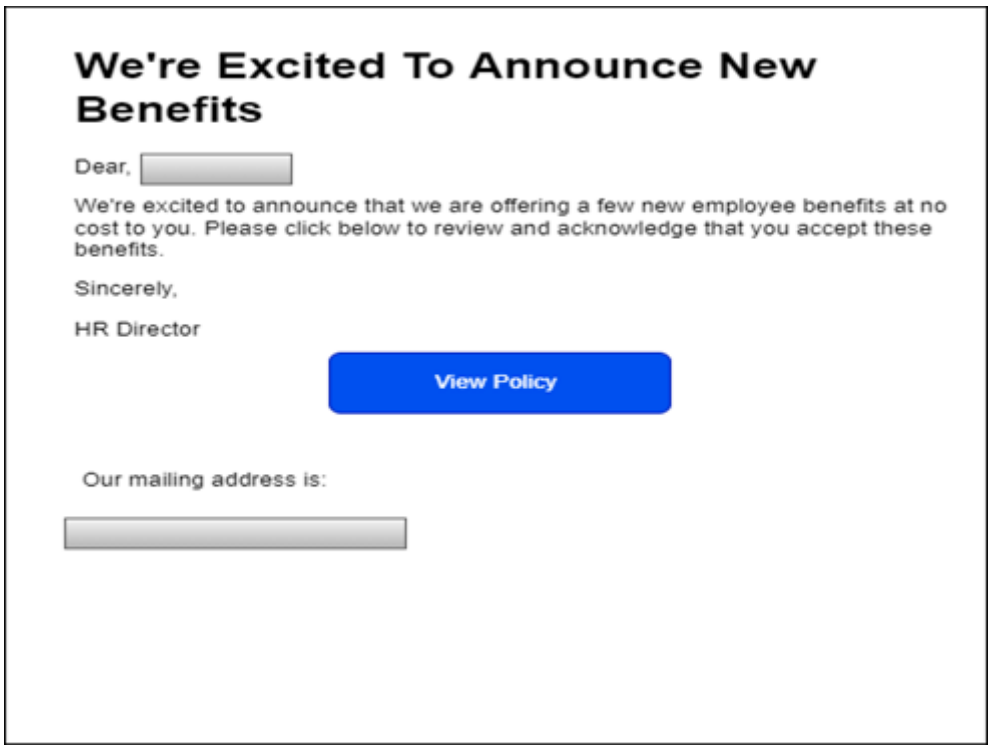


Figure 4.2: Phishing email

As per Figure 4.3, 72% of respondents claim they deliberately ignored suspicious emails. The same proportion of 6% selected the options to contact the HR department for clarifications and press the blue button for more information.

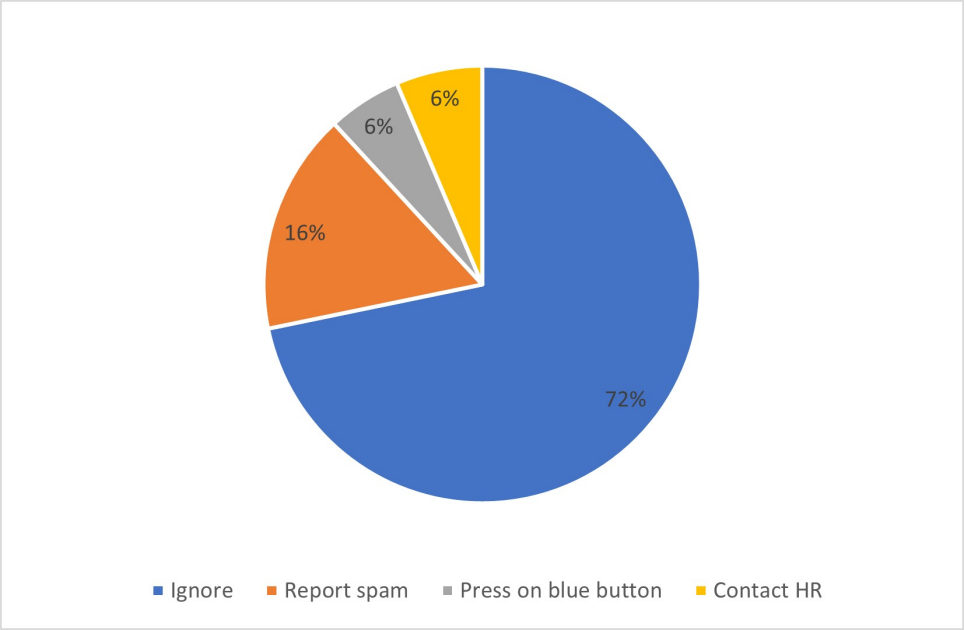


Figure 4.3: What do you do if you receive this email?

This question was followed by an optional question requesting the reason for selecting this

option, which provided me with a deeper understanding and insight into the employees' awareness of this issue. I received 442 brief comments, and the majority of them indicated that their ignorance is an automatic response; however, here are some examples of other participants who chose to neglect said, "to save time," and "fear of the unknown," respectively. Another said, "I dislike reading because it is easier for me."Many demonstrated their ignorance due to negligence.

Some of those who chose to press the blue button did so out of curiosity and desire to learn more. For example, "Maybe this is an opportunity for me!" Another stated, "I wish to verify the new offer."

Others who reported it as spam did so out of concern for others; one participant explained, "I don't want anyone else to experience the same problem." Another one stated, "to stop receiving such emails again." Those who selected spam want to halt these types of unwanted messages.

Respondents define Sensitive information differently, particularly when posted publicly on social media. As depicted in Figure 4.4, a large proportion of the participants 84% reveal that their phone numbers were considered the most sensitive information and should not be posted on social media, and posting the achievements was deemed sensitive to only 5% of them.

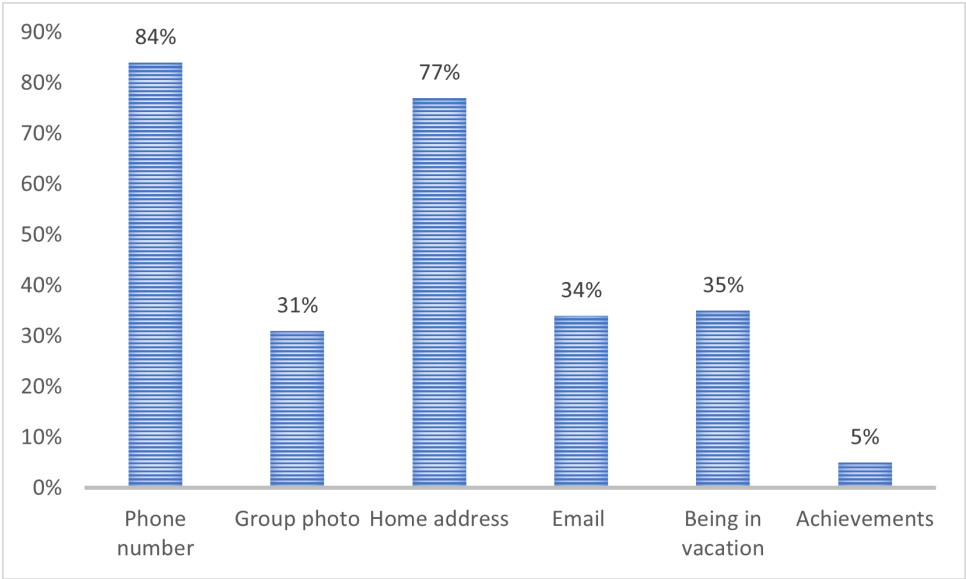


Figure 4.4: Sensitive details

In the process to understand the awareness of respondents in matters related to security aspects, at least 56% of the participants, as shown in Figure 4.5, define "phishing" correctly.

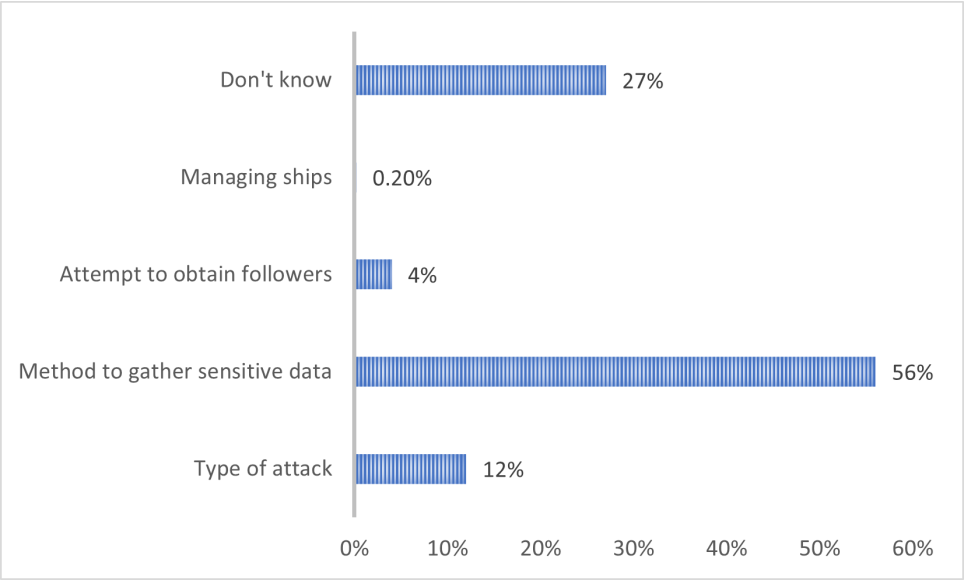


Figure 4.5: Phishing concepts

More questions are being added to the survey to better comprehend employee online behaviour. As shown in Table 4.5 a larger proportion of respondents (72%) clearly understand that *https* is more secure than *http*. At least 41% of participants confirm that they rarely use public networks that are available in airports, cafes, or other public places. As far as passwords are concerned, 43% of users confirm that they always make strong passwords combining letters, numbers, and special characters. At least, 28% of participants confirm that they use antivirus software to protect their devices – in fact, they update their antivirus software regularly. A similar percentage (28%) of participants confirm that they always check the spellings of the URLs in the given links, before entering any sensitive information there.

Table 4.5: Security practices

Variable(s)		N (%)
I use public networks, like those in cafes or airports	Never	136 (21
	Rarely	263 (41)
	Sometimes	188 (29)
	Often	40 (6)
	Always	13 (2)
I use a combination of letters, numbers and special characters when choosing a password	Never	20 (3)
	Rarely	44 (7)
	Sometimes	93 (14)
	Often	204 (32)
	Always	279 (44)
I use antivirus software to protect my devices	Never	76 (12)
	Rarely	103 (16)
	Sometimes	133 (21)
	Often	150 (23)
	Always	178 (28)
I regularly check the antivirus software update on my computer / laptop	Never	82 (13)
	Rarely	114 (18)
	Sometimes	145 (23)
	Often	147 (23)
	Always	152 (24)
I always check the spelling of the URLs in links before I click or enter sensitive information	Never	56 (9)
	Rarely	98 (15)
	Sometimes	141 (22)
	Often	181 (28)
	Always	164 (26)

4.2.4 Cybersecurity Training Preferences

Given that the primary objective of this study is to identify an adaptive cybersecurity training system for social media threats, it is crucial to learn more about employees' training preferences regarding cybersecurity topics.

As per Table 4.6, at least 44% of participants indicateed that conducting workshops or in-class training is a very useful approach, with 36% of them calling it moderately useful. At the same time, 37% of the respondents consider gaming for training purposes as a very useful approach. The approach based on stories has also been termed very useful by more than 35% of the respondents. An incentive approach of training has been considered very useful by at least 39% of them.

Table 4.6: Training preferences

Variable(s)		N (%)
Workshops	Not at all useful	14 (2)
	Extremely useful	134 (21)
Online training	Not at all useful	28 (4)
	Extremely useful	74 (12)
Posters	Not at all useful	41 (6)
	Extremely useful	60 (9)
Games	Not at all useful	34 (5)
	Extremely useful	79 (12)
Webinars	Not at all useful	29 (4)
	Extremely useful	73 (11)
Stories	Not at all useful	23 (4)
	Extremely useful	114 (18)
Social media	Not at all useful	18 (3)
	Extremely useful	103 (16)
Offer incentive	Not at all useful	22 (3)
	Extremely useful	128 (20)
Tip-sheets	Not at all useful	38 (6)
	Extremely useful	52 (8)
Conduct mock attack	Not at all useful	90 (14)
	Extremely useful	87 (14)
Awareness raising events	Not at all useful	37 (6)
	Extremely useful	77 (12)
Videos	Not at all useful	19 (3)
	Extremely useful	97 (15)
Emails	Not at all useful	98 (15)
	Extremely useful	71 (11)

In addition, I wanted to determine if these preferences were based on prior experience or merely an estimate, so I asked participants how many times they had received cybersecurity training or if they had never received such training before. As shown in Figure 4.6 the vast majority of participants, 72%, had never before received cybersecurity training.

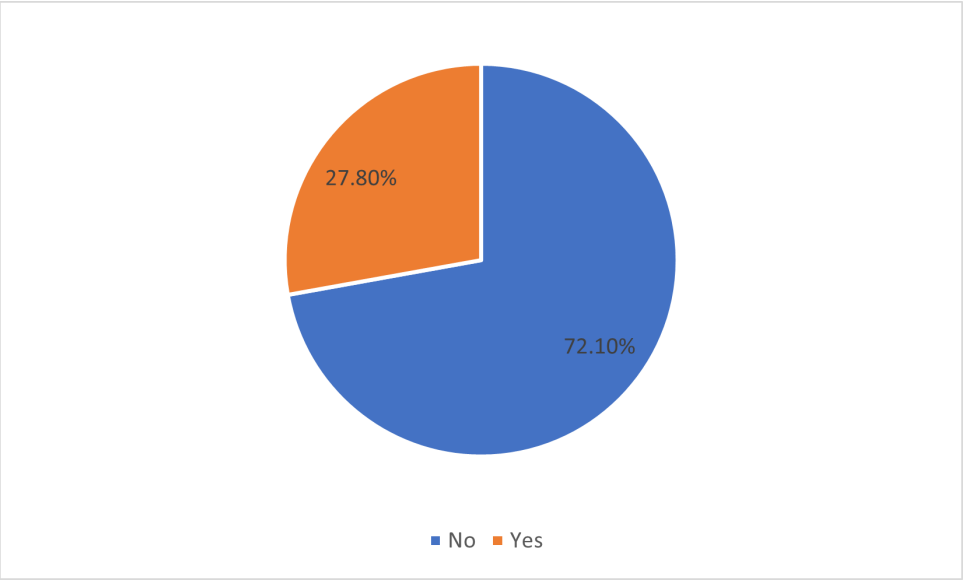


Figure 4.6: Have you ever been trained about cybersecurity?

In addition, as per Figure 4.7, 63% of those who have received cybersecurity training received it during their working hours, compared to less than 12% of those who received it during their university studies.

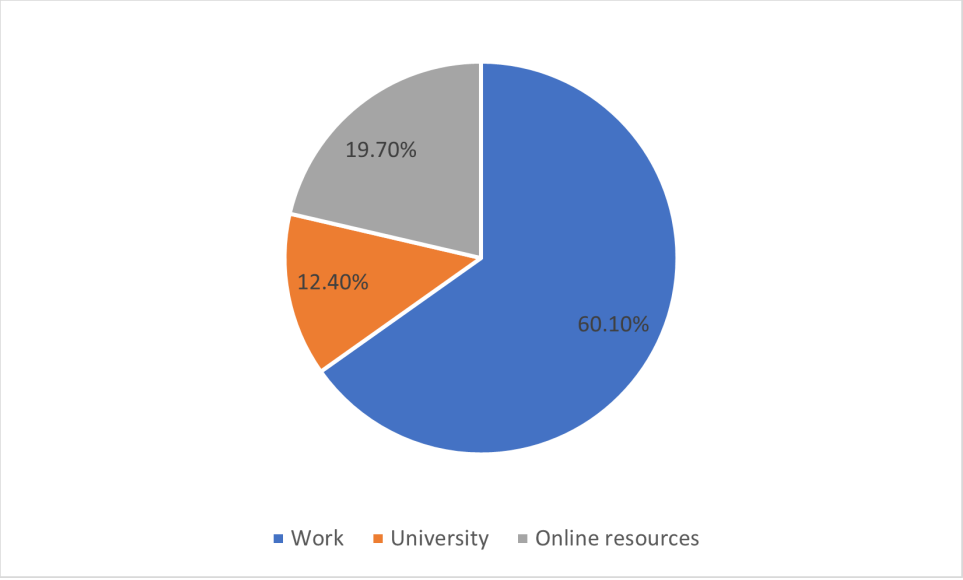


Figure 4.7: Where did you receive this training about cybersecurity?

At least 61% of those who trained before about cybersecurity reported that they have received such training once a year.

Numerous training methods have been utilised to impart training; no single method can be deemed indispensable for this purpose. Nonetheless, as shown in Figure 4.8,

workshops or in-class training with interaction was the most common method of training for participants, while mock attacks or phishing tests accounted for less than 2%.

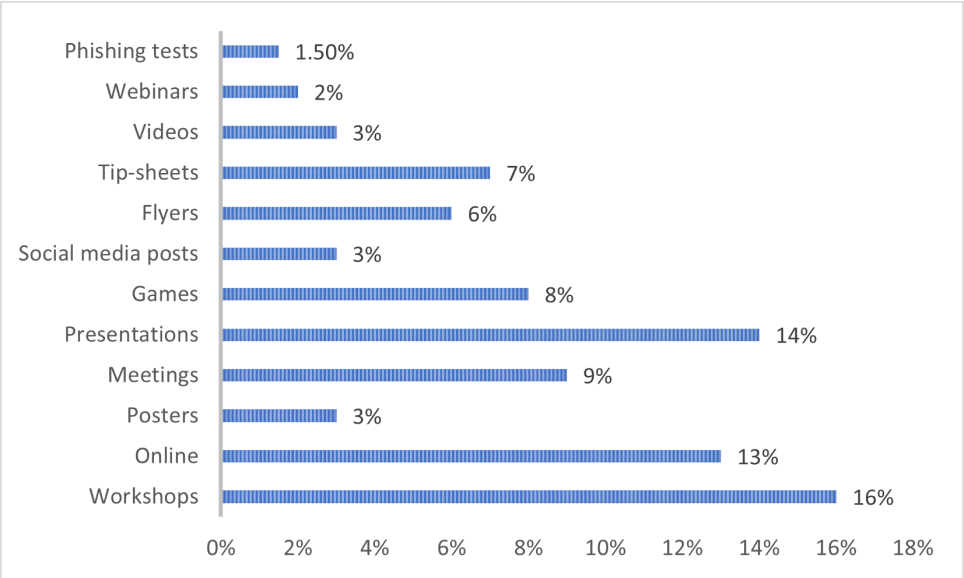


Figure 4.8: Training approaches received

On the aspect of whether participants should receive training or not on issues related to cybersecurity, at least 87% of them agree or strongly agree with the importance of such training. A large proportion (85%) of them are in favor (either agree or strongly agree) of having social media policies in place.

As such; I wanted to learn more about the areas that employees struggle with the most in terms of cybersecurity so that I could design the adaptive training system by filling in the gaps; one of the direct questions that have been posed to participants is to select the area that they struggle with the most from the options provided. As per Figure 4.9, hacking (49%) is described as the main one, and password protection as the least one (27%).

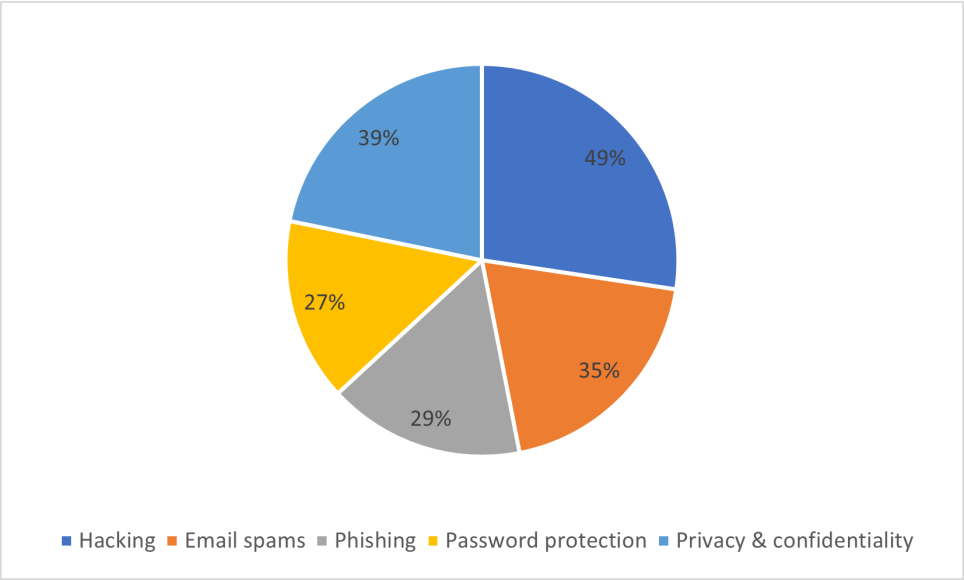


Figure 4.9: Struggling areas

4.2.5 Reasons why cybersecurity training is ineffective

It is essential for me to comprehend why trainees and employees consider cybersecurity training is ineffective. As a result, I included a question in the survey that could help me locate the answer.

In this study, cybersecurity training fails or becomes ineffective due to a variety of reasons. As many as 61% of the participants (those who either agree or strongly agree) consider boring and routine training sessions as the main cause for failure. As per 63% of the respondents (those who agree or strongly agree), the training tends to fail when it is difficult to follow or uses technical jargon. 35% of respondents acknowledge that customised training is superior to generic training. 37% pointed to the role of the training delivery methods, while 38% stated the role of the environment, including the locations and scheduling of the training. Lastly, 37% of the participants pointed out the crucial role of the trainer and the significance of having skill and experience. More details on the causes of failures of training sessions can be found in Table 4.7.

Table 4.7: Reasons for training to fail

Variable (s)		N (%)
It is boring and routine	Strongly disagree	24 (4)
	Disagree	33 (5)
	Neutral	190 (30)
	Agree	225 (35)
	Strongly agree	168 (26)
It is difficult and includes technical language	Strongly disagree	21 (3)
	Disagree	45 (7)
	Neutral	175 (27)
	Agree	229 (36)
	Strongly agree	170 (27)
It is provided in a one-size-fits-all	Strongly disagree	24 (4)
	Disagree	55 (9)
	Neutral	225 (35)
	Agree	217 (34)
	Strongly agree	118 (18)
The delivery training methods are poor	Strongly disagree	15 (2)
	Disagree	48 (7)
	Neutral	189 (29)
	Agree	239 (37)
	Strongly agree	149 (23)
The training environments are limited	Strongly disagree	17 (3)
	Disagree	38 (6)
	Neutral	238 (37)
	Agree	243 (38)
	Strongly agree	104 (16)
The trainers are unskillful	Strongly disagree	22 (3)
	Disagree	39 (6)
	Neutral	174 (27)
	Agree	171 (27)
	Strongly agree	234 (37)

4.3 Inferential Analysis

The Chi-square test examines the relationship between two categorical variables (McHugh, 2013). Also, it is a statistical test that compares observed and expected results. The chi-square test is designed to establish whether a variation between observed and predicted data is due to the relationship between the variables under consideration. As a result, this test is an ideal choice for enabling me better understand and comprehend the relationship between our two category variables (Southampton, 2022).

Statistical analysis to compare my variables was performed by Chi-square test. The confidence intervals have been set to 95% and 99% respectively. Hence, p-values between 0.01 and 0.05 were considered statistically significant.

4.3.1 Degrees of Freedom in the Chi-square Test

The most frequent definition of degree of freedom (df) is the number of values in a distribution that are free to fluctuate for any particular statistic, according to Healey (2014). Other authors have attempted to be more specific by defining degrees of freedom regarding sample size, the number of relationships in the data, and the difference in dimensionalities of the parameter spaces. Although the df is theoretically difficult to understand yet is required to report to understand statistical analysis, it is connected with statistical power (Pandey & Bright, 2008).

Degrees of freedom differ from one statistical test to the next as we progress from univariate to bivariate and multivariate statistical analysis, depending on the nature of the restrictions used, even when the sample size remains constant. However, as the number of parameters to be evaluated grows, the degrees of freedom decrease. As a result, degrees of freedom differ from one statistical test to the next.

In the chi-square statistic, the degree of freedom is calculated to test the hypothesis that the connection between two variables (row and column variables) is linear. The Chi-square test subtracts one from both the number of rows and columns to determine the degree of freedom since we can tell the values in the last cells for both rows and columns by knowing the values in other cells (Weiss, 1968).

4.3.2 Demographics and Training Preferences

Gender and Training Preferences

There are other factors also associated with people's preference, through to a lesser degree. In this study, the association between 'gender' and 'training preferences', as shown in Table 4.8, is also evident out of 13 variables, six variables are found to be associated with gender. The results of chi-square tests inform that female prefer *online training, posters, gaming, emails, and webinars* . At the same time, a *mock attack* as a training approach is preferred by male trainees. However, in this study, the Chi-square analysis revealed no statistical correlation between gender and the following training delivery methods:

- Workshops
- Storytelling approach
- Social media posts
- Offering incentives to encourage behaviors
- Distributing tip sheets
- Attending awareness-raising events
- Watching videos.

Table 4.8: Gender and training preferences

	Male Count/Expected	Female Count/Expected
1-ONLINE TRAINING (χ^2 = 11.302, df = 4, p- value <.05)		
Not-useful	13/11.5	15/16.5
Very-useful	23/30.4	51/34.6
2-POSTERS (χ^2=9.898, df = 4, p-value <.05)		
Not-useful	19/16.8	22/24.2
Very-useful	18/24.7	42/35.3
3-GAMES (χ^2 = 26.375 , df = 4, p-vale <.001)		
Not-useful	15/14	19/20
Very-useful	17/32.5	62/46.5
4- WEBINARS (χ^2 = 23.035, df = 4, p-value <.001)		
Not-useful	16/11.9	13/17.1
Very-useful	19/30	54/43
5- MOCK ATTACKS (χ^2 = 13.699, df = 4, p-value <.01)		
Not-useful	28/37	62/53
Very-useful	46/35.8	41/51.2
6- EMAILS (χ^2 = 13.699, df = 4, p-value <.01)		
Not-useful	35/40.3	63/57.7
Very-useful	22/29.2	49/41.8
7- VIDEOS (χ^2 = 6.853, df = 4, p-value .144)		
Not-useful	10/7.8	9/11.2
Very-useful	104/103.1	64/57.1/75
8- AWARENESS RAISING EVENTS (χ^2 = 4.322, df = 4, p-value .364)		
Not-useful	12/15.2	25/21.8
Very-useful	75/81	122/166
9- TIP SHEETS (χ^2 = 8.970, df = 4, p-value .062)		
Not-useful	17/15.6	21/22.4
Very-useful	63/70.3	108/100.7
10- OFFER INCENTIVES (χ^2 = 4.019, df = 4, p-value .403)		
Not-useful	10/9	12/13
Very-useful	96/103.1	155/148
11- SOCIAL MEDIA (χ^2 = 4.272, df = 3, p-value .234)		
Not-useful	11/7.4	7/10.6
Extremely-useful	37/42.3	66/60.7
12- STORYTELLING (χ^2 = 8.968, df = 4, p-value .062)		
Not-useful	12/9.5	77/92.5
Very-useful	11/13.5	148/132.5
13- WORKSHOPS (χ^2 = 2.248, df = 4, p-value .690)		
Not-useful	7/5.8	7/8.2
Very-useful	109/117.1	78/78.9

Age and Training Preferences

While the association between 'gender' and 'training preferences' is significant, a weaker

association has been noticed between age-group and 'training preferences'. As shown in Table 4.9 below, *posters* as an approach for delivering cybersecurity training are preferred mostly by the 46-55 age group, especially when compared with the 18-26 age group. Similarly, the *storytelling* approach is also preferred the most by those who fall in the 46-55 age group followed by those who are in the 18-25, and 36-45 age group. The chi-square results also reveal that *emails* delivering cybersecurity content are preferred by the older age-group over their younger peers.

However, the Chi-square results in this study found no statistical correlation between the age of employees and their preferences for the following training methods:

- Workshops or in-class training
- Gaming approach
- Webinars
- Social media posts
- Offering an incentives
- Distributing tip sheets
- Mock attacks or phishing tests
- Attending awareness raising events
- Watching videos (pls, refer to Table 4.9)

Table 4.9: Age and training preferences

	18-25 Count/Exp	26-35 Count/Exp	36-45 Count/Exp	46-55 Count/Exp	>55 Count/Exp
1-POSTERS (χ^2 = 31.821, df = 20, p- value <.05)					
Not-useful	1/2.4	14/14.7	1/14.5	3/6	7/3.5
Very-useful	6/10	67/63	29/62.5	29/25.7	10/14.9
2-STORYTELLING (χ^2=38.752, df = 20, p-value <.01)					
Not-useful	1/1.3	7/8.2	9/8	2/3	4/1.9
Very-useful	10/13	74/80.5	77/79.5	46/33	18/19
3-EMAILS (χ^2= 35.106 , df = 20, p-vale <.05)					
Not-useful	14/5.7	38/35	35/34.6	7/14	4/8
Very-useful	6/8	44/52	54/52	23/21	18/12
4- WORKSHOPS (χ^2 = 19.808, df = 20, p-value .470)					
Not-useful	0/.8	7/5	6/4.9	0/2	1/1.2
Very-useful	16/16.5	101/102	95/100	51/41.4	21/24
5- ONLINE TRAINING (χ^2 = 22.364, df = 20, p-value .321)					
Slightly-useful	1/1.6	8/10	13/9.9	3/4.1	3/2.4
Very-useful	11/12.3	77/75.9	69/74.9	38/30.8	17/17.9
6- GAMES (χ^2 = 19.376, df = 20, p-value .498)					
Not-useful	0/2	11/12.2	11/12	7/4.9	5/2.9
Very-useful	10/13.6	86/84	84/83	40/34	14/19.8
7- WEBINARS (χ^2 = 20.189, df = 20, p-value .446)					
Not-useful	0/1.7	9/10.4	18/10.2	1/4.2	1/2.4
Very-useful	13/12	76/75	70/74.2	37/30.5	13/17.7
8- SOCIAL MEDIA (χ^2 = 11.568, df = 15, p-value .711)					
Not-useful	0/1	8/6.4	8/6.4	1/2.6	1/1.5
Very-useful	5/6	37/37	40/36.4	16/15	5/8.7
9- OFFER INCENTIVES (χ^2 = 20.426, df = 20, p-value .432)					
Not-useful	0/1.3	10/7.9	10/7.8	1/3.2	1/1.9
Very-useful	11/14.5	93/90	79/88.6	44/35.5	23/21.3
10- TIP SHEETS (χ^2 = 14.581, df = 20, p-value .800)					
Not-useful	3/2.2	12/13.6	11/13.4	6/5.5	6/3.2
Very-useful	13/10	62/61.2	53/60.4	28/24.8	14/14.4
11- SOCIAL MEDIA (χ^2 = 26.653, df = 21, p-value .183)					
Not-useful	0/.6	4/2.7	5/3.3	2/3.3	5/3.3
Very-useful	7/3.7	13/15	14/19	25/18.7	27/19
12- MOCK ATTACKS (χ^2 = 13.006, df = 20, p-value .877)					
Not-useful	8/5.2	30/32.2	32/32	11/13.1	9/7.6
Very-useful	7/9.2	57/57	59/56	26/23	10/13.4
13- EVENTS (χ^2 = 24.559, df = 20, p-value .219)					
Not-useful	3/2.1	14/13.2	12/13	4/5.4	4/3.1
Very-useful	13/11.4	64/70.5	74/70	35/28.6	11/16.6

Work Experience and Training Preferences

Moreover, the chi-square test reveals nine significant associations regarding training preferences and experience of the participants (in years). Referring to Table 4.10, the chi-square test results inform that people with 15-20 years of experience are the ones who most value *workshops/physical* presence for cybersecurity training. Against this, the people with 10-15 years of experience consider *workshops and webinars* their least preferred method of training; they tend to prefer *Online* training instead. The people with 2-5 years of experience prefer *webinars* and *posters* as the training methods. However, the same training methods are given least preference by the people with 15-20 years of experience. The chi-square test results also reveal that people with 10-15 years of experience consider *gaming* as the most preferred way of training; yet that goes down slightly with the people having over 15 years of experience. Similarly, most of the participants prefer *incentive* as the preferred method of training; however, that decreases slightly with people with a higher level of experience.

Mock attacks as a training method is a preferred approach by new employees; yet those with 5-15 years of experience consider them less important. However, people with 15-25 years of experience prefer *videos* as the training method for cybersecurity. In addition, the most experienced people (25+ years) give the highest weight to *email* learning and training.

The Chi-square analysis, however, revealed no statistical correlation between the years of experience of employees and their preferences for the following training methods:

- Gaming approach
- Social media posts
- Learning through stories
- Distributing tip sheets
- Attending awareness raising events
- Viewing videos, Table 4.10 for more details.

Table 4.10: Work Experience and training preferences

	<2	2-5	5-10	10-15	15-20	20-25	>25
	Count/Exp	Count/Exp	Count/Exp	Count/Exp	Count/Exp	Count/Exp	Count/Exp
1-WORKSHOPS (χ^2 = 44.773, df = 28, p- value <.05)							
Not-useful	0/.5	0/2	7/2.6	3/2.5	2/2.6	1/1.7	1/1.5
Very-useful	9/10	47/43	47/53	59/52	54/53	36/35	25/31
2-ONLINE TRAINING (χ^2=51.169, df = 28, p-value <.01)							
Not-useful	5/3.5	10/14.4	21/18	22/17	21/18	8/12	3/10.5
Very-useful	7/7.6	39/32	39/39.4	34/38	33/39	30/26	26/32
3-POSTERS (χ^2= 41.338 , df = 28, p-vale <.05)							
Not-useful	9/5.4	22/23	27/28	20/27	36/28	15/19	13/16.5
Very-useful	5/6.4	37/26.6	30/33	32/32	30/33	19/22	21/19
4- GAMING (χ^2 = 61.612, df = 28, p-value <.01)							
Not-useful	2/0	2/5	10/6	5/6	2/6	6/4	7/4
Very-useful	8/8.4	22/35	54/44	48/43	50/44	32/29	15/26
5- WEBINARS (χ^2 = 54.965, df = 28, p-value <.01)							
Slightly-useful	4/4	8/18	20/22	30/22	26/22	13/15	11/13
Very-useful	8/7.5	48/31.5	37/39	37/38	31/39	22/26	23/23
6- OFFER INCENTIVES (χ^2 = 70.034, df = 28, p-value <.01)							
Not-useful	0/2.4	3/10	16/12	6/12	17/12	9/8	7/7.2
Very-useful	8/9	44/38	52/47	43/45.5	42/47	31/31	26/27.5
7- VIDEOS (χ^2 = 60.263, df = 28, p-value <.01)							
Not-useful	0/1	3/3	6/3.5	6/3.4	2/3.5	1/2	1/2
Very-useful	11/9	37/38	51/47	40/45.5	41/48	36/31	29/27.5
8- MOCK ATTACKS (χ^2 = 51.751, df = 28, p-value<.01)							
Not-useful	4/3	8/13.5	19/17	16/16	19/17	10/11	11/10
Very-useful	4/6	31/24	27/30	27/29	26/30	26/20	16/17
9- EMAILS (χ^2 = 52.831, df = 28, p-value <.01)							
Not-useful	3/3.5	28/15	14/18	13/18	22/18	6/12	7/11
Very-useful	7/5	20/22	26/27	24/26.5	17/27	26/18	24/16
10- STORIYTELLING (χ^2 = 33.884, df = 28, p-value .205)							
Not-useful	1/.8	1/3.4	7/5.3	3/4.2	4/4.3	3/2.8	3/2.5
Very-useful	9/8	37/33.8	45/41.8	37/40.8	36/41.8	31/27.8	25/25
11- SOCIAL MEDIA (χ^2 = 26.653, df = 21, p-value .183)							
Not-useful	0/.6	4/2.7	5/3.3	2/3.3	5/3.3	1/2.2	0/2
Very-useful	7/3.7	13/15	14/19	25/18.7	27/19	9/12.7	8/11.3
12- TIP SHEETS (χ^2 = 32.537, df = 28, p-value .253)							
Not-useful	0/1.4	7/5.7	7/7.1	4/6.9	7/7.1	3/4.7	8/4.2
Very-useful	12/6.1	29/25.7	33/31.8	27/31	27/31.8	22/21.1	16/18.7
13- EVENTS (χ^2 = 41.334, df = 28, p-value .050)							
Not-useful	1/1.3	6/5.6	8/6.9	8/6.7	4/6.9	4/4.6	3/4
Very-useful	7/7.1	34/29.5	31/36.6	32/35.7	39/14.3	34/24.3	16/21.5

Educational level and Training Preferences

It may be interesting to notice that those with a bachelors or postgraduate level of education give preference to *mock attacks*, *incentives*, *videos*, *awareness events*, *and emails*. Postgraduates favour *videos* as the most preferred method for receiving information and taking training regarding cybersecurity-related topics followed by those who had some courses but without any degree

Statistically, this study revealed no correlation between the education level of employees and their training preferences for the following training approaches:

- Workshops or in-class training
- Online training courses
- Viewing posters
- Gaming approach
- Attending webinars
- Social media posts
- Storytelling approach
- and, reading tip sheets, (More details in Table 4.11 below).

Table 4.11: Educational level and training preferences

	<Secondary Count/Exp	Secondary Count/Exp	Colleges Count/Exp	Bachelor Count/Exp	Postgraduate Count/Exp
1-OFFER INCENTIVES (χ^2 = 34.289, df = 20, p- value <.05)					
Not-useful	0/.2	1/.4	3/2.1	9/14	9/5.2
Very-useful	1/2.7	6/5.1	12/23.5	168/160	63/59
2-MOCK ATTACKS (χ^2=43.996, df = 20, p-value <.01)					
Not-useful	0/1	1/1.8	8/8	52/57	29/21
Very-useful	3/2	5/3	9/15	106/101	36/37
3-EVENTS (χ^2= 36.842 , df = 20, p-vale <.05)					
Not-useful	1/0	1/1	7/3.5	21/24	7/9
Very-useful	5/2.2	6/4	6/18.5	135/126	50/46
4- VIDEOS (χ^2 = 42.842, df = 20, p-value <.01)					
Not-useful	0/0	1/0	4/2	12/12	2/4.5
Very-useful	1/3	6/5	11/23.5	159/160	73/59
5- EMAILS (χ^2 = 33.034, df = 20, p-value <.05)					
Slightly-useful	1/1	2/2	6/9	63/62.5	25/23
Very-useful	0/2	5/3	5/14	97/93	39/34
6- Workshops (χ^2 = 16.465, df = 20, p-value .687)					
Not-useful	0/.2	0/.3	2/1.3	9/8.9	3/3.3
Very-useful	3/3	6/5.8	30/26.7	179/181	67/67
7- ONLINE TRAINING (χ^2 = 17.566, df = 20, p-value .616)					
Not-useful	0/.3	0/.6	4/2.6	9/6.6	0/.1
Very-useful	2/2.3	6/4.3	20/20	48/49	0/.7
8- POSTERS (χ^2 = 22.295, df = 20, p-value .325)					
Not-useful	0/.4	0/.8	3/3.8	26/26	12/9.6
Very-useful	2/2	5/3.6	19/16.6	117/113	34/41.5
9- GAMED (χ^2 = 29.117, df = 20, p-value .085)					
Not-useful	0/.4	1/.7	3/3.2	19/21.7	11/8
Very-useful	0/2.6	8/4.8	18/22	151/150	57/55
10- WEBINARS (χ^2 = 24.386, df = 20, p-value .226)					
Not-useful	0/.3	1/.6	3/2.7	13/18.5	12/7
Very-useful	2/2.3	6/4.3	15/20	135/134	52/49.2
11- STORIES (χ^2 = 26.731, df = 20, p-value .143)					
Not-useful	1/.3	1/.5	4/2.2	11/14.7	6/5.4
Very-useful	0/2.5	7/4.6	17/21	146/143	55/52.7
12- SOCIAL MEDIA (χ^2 = 17.195, df = 15, p-value .307)					
Not-useful	1/.2	1/.4	2/1.7	9/11.5	5/4.2
Very-useful	3/1.1	4/2.1	10/9.7	60/65.7	26/24
13- TIP SHEETS (χ^2 = 18.956, df = 20, p-value .525)					
Not-useful	1/.4	1/.8	3/3.6	25/24.2	8/9
Very-useful	1/2	6/3.5	10/16	111/109	43/40

Job Roles and Training Preferences

The training preferences of the participants largely depend on the job roles they do. The chi-square test results reveal that out of 13 training approaches, 12 are significantly associated with the participants' job role or discipline (Table 4.12 for more details).

Table 4.12: Job role and training preferences

	Edu Co\Ex	IT Co\Ex	Health Co/Ex	Leader Co/Ex	Business Co/Ex	Art.. Co\Ex	Office Co\Ex	Military Co\Ex
1-WORKSHPS (x2 = 54.3888, df = 32, p-value <.01)								
Not-useful	**1/3.3**	**0/1.6**	**0/0.4**	**8/2.9**	**2/1.8**	0/0.5	2/1.9	1/1.1
Useful	**37/32**	**26/15.7**	**2/3.8**	**29/27.8**	**12/14.7**	4/5.2	13/17.8	11/10.9
2-ONLINE TRAINING (x2 = 67.590, df = 32, p-value <.01)								
Not-useful	5/6.7	1/3.3	1/0.8	11/5.8	5/3.6	0/1.1	4/3.7	1/2.3
Useful	23/17.7	17/11.3	4/2.1	10/15.4	8/9.6	3/2.9	3/9.8	5/6
3-POSTERS (x2 = 41.666, df = 20, p-value <.01)								
Not-useful	13/9.8	3/4.8	0/1.2	9/8.5	7/5.3	0/1.6	3/5.4	6/3.3
Useful	15/14.3	12/7	5/1.7	13/12.5	4/7.8	4/2.3	4/8	1/4.9
4-GAMES (x2 = 53.582, df = 32, p-value <.01)								
Not-useful	7/8.1	2/4	1/1	8/7.1	7/4.4	3/1.3	3/4.5	3/2.8
Usful	25/14.3	15/9.3	0/2.2	16/16.4	9/10.2	3/3.1	8/10.5	2/6.4
5-WEBINARS (x2 = 67.987, df = 32, p-value <.01)								
Not-useful	2/6.9	1/3.4	2/.8	9/6	5/3.8	1/1.1	2/3.9	6/2.4
Useful	18/17.5	13/8.6	1/2.1	18/15.2	11/9.5	1/2.9	6/9.7	3/5.9
6-STORIES (x2= 70.034, df = 28, p-value <.01)								
Not-useful	5/5.5	1/2.7	1/.6	8/4.8	2/3	2/.9	3/3.1	1/1.9
Useful	28/27.3	21/13.4	7/3.2	19/23.7	18/14.8	5/4.5	11/15.1	3/9.3
7- SOCIAL MEDIA (x2 = 22.345, df = 24, p-value <.05)								
Not-useful	5/4.3	0/2.1	1/.5	6/3.7	3/2.3	0/.7	1/2.4	2/1.5
Useful	23/24.6	19/12.1	6/2.9	16/21.4	16/13.4	3/4	10/13.7	8/8.4
8- OFFER INCENTIVES (x2 = 62.216, df = 32, p-value <.01)								
Not-useful	5/5.3	0/2.6	1/.6	10/4.6	3/2.9	0/.9	2/2.9	1/1.8
Useful	30/30.6	24/15	2/3.6	28/26.6	12/16.6	5/5	13/17	10/10.4
9- TIP SHEETS (x2= 62.577, df = 32, p-value <.01)								
Not-useful	7/9.1	3/4.5	1/1.1	9/7.9	10/4.9	2/1.5	4/5	1/3.1
Useful	16/12.4	12/6.1	1/1.5	8/10.8	6/6.7	2/2	2/6.9	2/4.2
10- MOCK ATTACKS (x2 = 64.730, df = 32, p-value <.01)								
Not-useful	28/21.5	1/10.5	2/2.5	9/7.9	10/11.7	0/3.5	17/12	8/7.3
Useful	17/20.8	16/10.2	2/2.4	8/10.8	16/11.3	1/3.4	8/11.6	7/7.1
11- EVENTS (x2= 64.730, df = 32, p-value <.01)								
Not-useful	6/8.8	2/4.3	1/1	17/7.7	8/4.8	0/1.4	2/4.9	1/3
Useful	23/18.4	15/9	2/2.2	15/16	1/10	5/3	7/10.2	4/6.3
12- EMAILS (x2 = 64.730, df = 32, p-value <.01)								
Not-useful	22/23.4	13/11.5	7/2.8	20/20.4	18/12.7	3/3.8	10/13	5/8
Useful	14/17	9/8.3	1/2	23/14.8	4/9.2	3/2.8	9/9.4	5/5.8
13- VIDEOS (x2 = 532.648, df = 32, p-value .181)								
Not-useful	0/3.2	16/16.3	6/4.8	18/26.5	28/22.6	0/.5	26/27.7	14/16
Useful	2/1	15/18.7	7/5.5	45/30.5	20/26	7/6.2	40/31.9	6/18.4

Videos

While the chi-square test results reveal no statistically significant correlation between people's job roles and videos for cybersecurity training, it can be inferred that video occupies a prominent place in online cybersecurity training. Several of the interviewees were asked questions on their preference for videos as one of the methods for cybersecurity training.

Watching videos as one of the methods of training is preferred by some interviewees because videos can be played and stopped at the convenience of the participants. With training through videos, the advantage is that they need not visit any specific venue. Videos are more convenient when explanations are lengthy involving several steps. One can rewind the video and see the part of it again when something is not clear. "I have learned about cybersecurity largely through videos available on YouTube, and I always enjoy watching those videos," said one of the interviewees.

Trainers/instructors also use videos for illustration purposes because "It is easy to explain complex things through visuals," said one of the trainer interviewees. "The more visuals for training, the more clarity to learners," said another expert trainer who participated in the interview. "Videos explain the different kinds of cyber-attacks with more clarity," said the Chief of Security of a medium-sized organisation.

Workshops

On the other hand, the chi-square test results reveal that those who work on IT tend to favor the workshops for cybersecurity training followed by the people working in education and related fields. In-class training is preferred by many IT employees interviewed for several reasons. One of them is that the training can be finished within a fixed time frame. Contrary to this, people holding management and leadership positions do not seem to like classes in person.

A large proportion of the interviewees prefer interaction to strengthen their conceptual understanding. However, because of the COVID-19 pandemic, virtual training has become a necessity at most places, and many of the interviewees called it not only "convenient" but also "exciting." It is convenient in the sense that one can record the lecture and listen to it at their convenience. In other words, virtual training provides enough flexibility to the participants.

Nevertheless, virtual training lacks the close interaction, which is only possible in classrooms with a face-to-face attendance.

Online

The chi-square test result reveal that people working in IT take the online training approach as the most practical one, whereas people in military and defense like online training only moderately. People holding leadership and management positions do not favor the online training approach. As such, job roles play a pivotal role in choosing the kind of training. "Being an HR professional, I always prefer online training as it allows me to discharge my other urgent assignments," said a middle-aged executive in a large company.

As far as the technical part of cybersecurity training is concerned, offline classes with an expert trainer are preferred over online classes. "One can raise many technical queries and find answers, which is somewhat cumbersome in any online classes; it does not lead to any strong interactive feelings too," said one of the technical persons serving in an IT department of a medium-sized company. "Another weakness with online training is that you need some kind of enforcement to make the training mandatory," one expert in training formation added.

Posters

According to the chi-square test results, IT employees consider posters extremely valuable for raising cybersecurity awareness, but they are only slightly valuable for people from the financial and business fields. People from education, training, learning, and military/defence establishments do not consider the posters important.

Webinars

Office and administrative personnel consider webinars highly helpful as one of the ways to deliver cybersecurity training. People from financial and business operations consider webinars moderately helpful, but people from IT consider webinars less valuable. People from military and defence organisations do not consider this approach of training at all useful.

Storytelling

The chi-square test results reveal that the storytelling approach to raising cybersecurity awareness has been found extremely valuable by those who work in the IT field. People from military and defense services find this approach only slightly useful. At the same

time, people involved with the education, learning, and training field as well as those working in arts, sports, and entertainment positions find the approach moderately useful. One of the trainees with IT role asserted that she liked listening to real stories related to cyber-attacks, she said: “I like to attend conferences with real people that have real stories.” Another interviewee working in the IT field, who attended a cybersecurity training programme in London, informed me about her experiences. As one hacker narrated his part of the story to the audience as to how he took advantage of the carelessness of internet users, she said: “I learned a lot from the stories and incidents narrated by the speakers or trainers in my previous training programme; the story session was immediately followed by a question-answer session from the audience”. Another interviewee from education, learning, and training field said: "I have listened to many stories on cybersecurity from my colleagues, which has made me conscious of such issues!" and someone from military roles added: “Listening to real stories on cybersecurity excites me.”

Social Media

The chi-square test results reveal that those who work in IT fields find social media as a tool to impart cybersecurity information extremely valuable, and moderately suitable for those working in the healthcare sector; it has been found slightly valuable by those who are involved in administrative and office jobs.

Offering Incentives

People working in IT fields strongly agree that offering incentives to raise cybersecurity awareness is extremely beneficial followed by those working in administrative and office jobs. At the same time, those who work in financial services and businesses find incentive offerings only moderately beneficial. Against this, people working in management and leadership positions do not find incentives at all useful for raising cybersecurity awareness.

Tip-sheets

Tip sheets are considered an extremely helpful approach for those working in IT fields, and somewhat useful for those working in management and leadership positions. On the other hand, people involved in businesses and financial services consider this method of training as ‘not useful’. Interviewees spoke differently in reply to this question. Some people said: “Tip Sheets” for gaining understanding about SMPs is a good way, many others said, “It is not the best way of learning about SMPs protocols.”

Mock Attacks

Conducting mock attacks as part of the training is highly supported by the people working in IT fields followed by those who are involved in administrative and office functions. This approach of training is approved moderately by those who discharge their services in business and financial fields. Management and leadership personnel find this approach of training not useful at all. The interview shows that phishing emails are used by many firms to check and arouse the awareness of their employees. This also filters out those who require training. One of the participants informed that her organisation runs "Email Campaigns" to raise awareness on the matters of cybersecurity. On certain days such as national day, phishing emails are forwarded to see if their employees fall into the trap. This exercise also acts as a filtering method to pick and send them for training. Usually, newcomers are found to be trapped in such kind of exercise.

Events

Raising awareness through holding events appears to be extremely valuable for those who serve in IT fields followed by those working in administrative and office jobs. On the other hand, people working in the finance and business sector support event holding only moderately; however, people occupying management and leadership positions do not consider such a training approach useful at all.

Emails

Raising cybersecurity awareness through emails is the most preferred way for people serving in management and leadership positions. Even the people serving in administrative and office jobs consider this approach of raising cybersecurity awareness quite useful; however, people attached with defense establishments/military along with the business and financial services do not consider this approach much pragmatic. The chief of the cybersecurity cell of one of the organisations I interviewed said: "Even within the network users help each other to avoid potential attacks, and emails help them to thwart certain cyber-attacks." Emails are used for giving guidelines and tips for using the internet. Many organisations have resorted to using emails in the time of COVID-19. One of the security experts from the medium-sized organisation argued that emails could be enough for apprising employees with some level of awareness; however, she said: "I am not sure if this is sufficient or not."

Gaming

The Chi-square test results reveal that from trainers' perspectives the gaming approach of cybersecurity training is highly useful. One of the trainers interviewed conveyed: "Games can teach people faster than mere words because it is a practical experience that people do not easily forget". However, many involved with IT fields or in office or administrative roles find it moderately helpful.

Sometimes, the gaming cum competition approach among participants accelerates the learning process. One of the female interviewees working in the IT sector said: "The gaming approach is the best approach I have experienced ever as I am fully involved in my learning." When the gaming approach is added with the competition it becomes more effective. In this process, "Trainees are divided into two groups and made to compete with each other in gaming," said one of the interviewees. At the same time, people involved in leadership positions or management functions, or military establishments consider gaming only slightly beneficial. Moreover, people attached with businesses or doing financial services view the gaming approach as an ineffective method for enhancing awareness related to cybersecurity. Figure 4.10 here below depicts the training preferences of users holding different positions in an organisation.

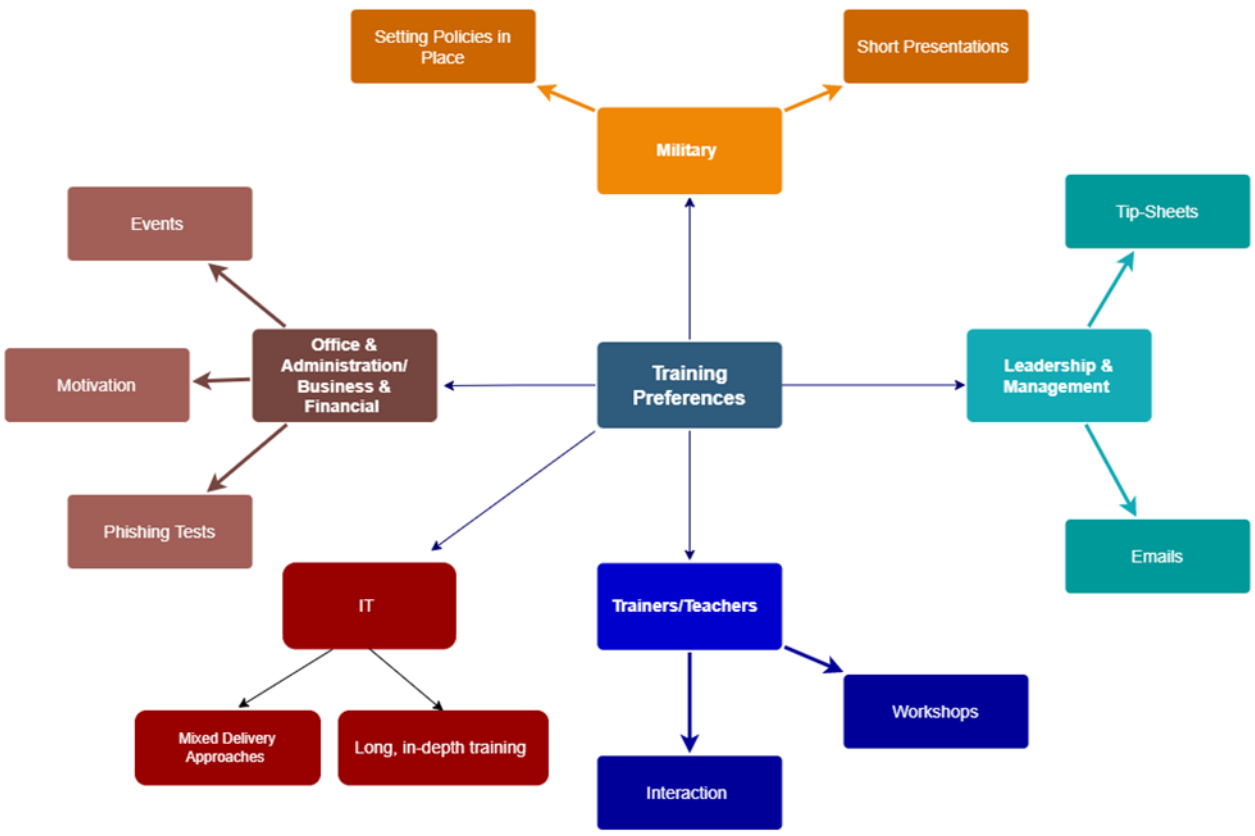


Figure 4.10: Job roles and training preferences

4.4 Factors Leading to Adaptive Training

In this study, I have analysed not only the factors that make employees adaptable to training, but also the influence of human factors on these areas. The following information refers to both significant and insignificant factors.

4.4.1 Job role and training adaptability factors

Concerning the factor of job role, the chi-square results were significant for all variables asked in the survey, beginning with motivation and concluding with the role of the trainer. From the survey and interview analysis, additional information will be presented.

Motivation

The chi-square test results (see Table 4.13) inform that people involved with education, training, and learning as well as defence personnel, in comparison to other groups, strongly agree that cybersecurity training sessions with routine lessons may not serve the real purpose of training. On the other hand, people from the IT fields did not agree with this notion. Trainees dislike the training session when they already know the information that is being imparted to them. This can be gathered from the remarks: “They still repeat the information that we know for several years!” Another said: “When they repeat the sessions, I stop giving the attention!".

Short training vs. long training is the aspect that I wanted to have some clue from the participants. One of the interviewed from military roles said: “I do not like long presentations, or long chatting or talking long about small issues.” Another interviewee from a management role said: “Our time and energy are precious, so it is better to keep the training programme short and brief.” A person with the business role uttered, “I prefer the quick training.” One of the candidates made a scathing remark, “I did not like it because it was a long presentation.” In contrast, many of the IT-educated participants clearly said: “We want a long in-depth study on security aspects; we have no objections to the longer sessions.”

On adaptation, someone from military roles said, "I can adapt more if there are interactions, learning with practical training, and also if there are small tests that make me improve my understanding of cybersecurity". As per one of the participants, adaptation becomes

possible when he feels good with the trainer who understands not only his questions but can also act as a good guide for him.

One expert in the field of training from a large organisation said: "Motivation is the key to success, and interaction facilitates practicing something by ourselves." Interaction enhances the involvement of participants: "Higher the interaction between instructor and participant, the higher are the chances of involvement of participant" said one of the young participants. Many of the participants suggested, "Trainers need to strengthen their training process with some hard facts such as data or numbers, real-life case studies and so on; people tend to follow when they see that they are likely to be affected."

Simplicity

The chi-square test results in Table 4.13 indicate that those who hold leadership and management positions, as well as those involved with defence establishments, strongly agree with the notion that using technical terms in cybersecurity training may be inadequate. One of the management personnel stated: "I will give more importance to using simple language, which is free of technical jargon so that people can understand easily." Another cybersecurity expert and trainer said: "I organise short seminars for the general public keeping in mind not to use any technical jargon." While demonstrating how hackers can access mobiles and how to keep devices safe from them, he makes the use of technical-free language that everyone can easily understand.

When things go too technical then trainees face difficulty in comprehending. One of the trainees from office and administrative roles trainees said: "I cannot understand because it's too technical." She also remarked: "I struggle a lot with privacy settings." On cybersecurity training, someone retorted, "They just want to pass the information, and they think that they are talking with someone professional." He meant it was challenging to understand the content.

Customizing

The chi-square test results in Table 4.13 also disclose that people involved in management or leadership responsibilities strongly agree that one-size-to-fit-all kind of training may not succeed in its purpose. At the same time, people involved in IT fields as well as in education, training, and learning functions moderately agree with this notion. Many interviewees opined that customizing the training was crucial to achieving the desired outcome as can be gathered from the remarks of one trainer I interviewed said: "I think

customizing is better; it might take more time and wasteful for organisations, but if you want effective results, then yes, customizing the training is better!" In other words, customized cybersecurity training programmes are needed which are based on prior experience and knowledge of cybersecurity. According to one of the participants from the IT field, customizing is beneficial for all as it would fill the gaps that they have.

Another participant said, "We have to make many groups – for beginners, for professionals and separate for those who are a little advanced in their cybersecurity awareness and knowledge". Someone said, "For me if it is applicable, I will favor the customization." One of the participants added, "Generalized training gives me a feeling that I am not a targeted member of this training process."

One of the chief managers with a non-IT background working in a medium-sized company became a victim of a phishing attack in early 2019; however, he came out unscathed from this incident. But when the IT office came to know about the incident, they immediately realized the necessity of training their staff, especially those working in the non-IT departments. With this incident, the IT team realized the importance of customizing the training based on the job roles/ responsibilities instead of offering generic training for all.

When the question was asked to cybersecurity trainers regarding the ways to make training sessions more adaptive, most of them supported customization of the training based on the audience. Their quick reply was: "It depends on the audience. To make training adaptive, it needs to focus and support trainees that are in the audience." Trainers also opined that imparting the training transparently made the trainees feel at home. For this, a variety of techniques need to be employed for delivering the information to trainees. One of the trainers said: "People learn differently, some learn more via lectures and presentation, some via practical training, so resorting to a single approach does not serve the purpose!"

One of the trainers that I interviewed revealed that he always made it a point to study his audience carefully before commencing any training session, especially their educational level, job roles, etc. It is equally important to know their expectations from the training so that the entire training session can be molded to go beyond their expectations. Many trainers suggested that: "Training should be tied up with the job requirements; the more the customization of the training, the more adaptive it will become."

Delivery Training Methods

The chi-square test results indicate that people working in education, training, and learning fields strongly assert that inferior training methods may lead to unsuccessful training related to cybersecurity. A method that is employed by the trainer or instructor for delivering the information and knowledge is considered crucial by our interviewees. The instructor may simply deliver a lecture before the audience without any interaction. In such cases, the audience may lose its focus in a short time. Contrary to this, when the trainer incorporates case studies, assignments, quizzes, or competition, etc. people get attached to the programme and learn more. One interviewee said, “When you listen to real stories or experiences, you are more inclined to be attentive and that helps.” Many preferred more than one training method for successful adaptation. One of the IT field candidates said: “I think blending all these approaches is interesting.” When it comes to adaptation with the cybersecurity training, the perceived difference is quite evident between the participants with an IT background and those with a non-IT background. One of the participants with an IT background said, "Being a technical person, I will take a technical approach for cybersecurity".

When it comes to cybersecurity training challenges, many interviewees from the administrative and office category find it difficult to adapt to cybersecurity training if the delivery approach of training is not conducive.

Environments

Also, as shown in Table 4.13 the chi-square test results reveal that people working in education, training, and learning fields strongly consider that the training environment is a crucial factor for the success of cybersecurity training. One of the experts in the field of training considers the training environment as the most vital factor. He says, “The environment is important, the training should be in the morning time, and the maximum period of training should be restricted to five days.” One of the participants described her experience with two cybersecurity conferences that she attended in Kuwait and London. She found the conference held in London as more adaptive because it was well organized in the sense that it covered many aspects related to cybersecurity including non-technical.

Trainers

The chi-square test results disclose that people involved with education, training, and learning fields strongly adopt the view that trainers play a significant role in the success of cybersecurity training programmes (More details in Table 4.13).

Most interviewed agreed on that as many of them said: "Trainer always occupies the most crucial place for the success of the programme." Even if the content is excellent but its delivery is not smooth or effective then the entire programme might fail. One of the participants said: "Trainer can always sharpen the content even if it lacks teeth, but it cannot happen otherwise." In short, he wanted to emphasize that an expert trainer could make the programme resilient and exciting. One of the trainers asserted: "The programme becomes a success when the instructor makes it exciting and entertaining"; he or she can simulate or create scenarios that one is likely to face in the days ahead.

In a way, a trainer can create situations when every member in the audience starts listening to them attentively. Someone said, "If the trainer is boring, I would not like to listen to them; in the training related to cybersecurity, we should be allowed to choose our instructor, especially when it is more technical."

It was universally accepted by most people that I interviewed that to make the training programme a success, a trainer is the most important factor – beyond all other factors. According to an expert in the field of training, it is the trainer's responsibility to make the training adaptive because only the trainer can ensure that everyone in the audience is involved and participates fully. Active participation is itself the clue of understanding the subject and that is why one of the experts in the field of training said: "You don't leave anyone sitting quiet and just enjoying the ride without any participation.

Table 4.13: Job roles and reasons for cybersecurity training to fail

	Education Co/Exp	**IT Co/Exp**	**Health Co/Exp**	**Leader Co/Exp**	**Business Co/Exp**	**Art Co/Exp**	**Office Co/Exp**	**Military Co/Exp**
Cybersecurity training fails if it is boring and routine (χ^2 =57.341, df = 32, p-value <.01)								
Disagree	2/8	10/4	0/1	6/7	9/4	0/1	3/4	1/3
Agree	58/54	27/26	7/6	42/47	22/29	14/9	30/30	22/18
Cybersecurity training fails if it is difficult and includes technical language (χ^2 =60.799, df = 32, p-value <.01)								
Disagree	5/11	11/5	0/1	8/9	14/6	0/2	4/6	1/4
Agree	64/55	25/27	5/6	43/48	21/30	16/9	37/30	13/19
Cybersecurity training fails if it is provided in one-size-fits-all (χ^2 =66.135, df = 32, p-value <.001)								
Disagree	8/13	16/6.5	0/1.5	6/11	9/7	1/2.2	7/7	5/4.5
Agree	60/52	31/25.5	4/6	33/45	25/28	11/8.5	32/29	17/18
Cybersecurity training fails if the delivery training methods are poor (χ^2 =48.874, df = 32, p-value <.05)								
Disagree	6/11.5	7/6	0/1	11/10	7/6	0/2	6/6	7/4
Agree	63/57	23/28	6/6.7	38/50	33/31	14/9	41/32	11/15
Cybersecurity training fails if the training environments are limited (χ^2 =68.520, df = 32, p-value <.001)								
Disagree	6/9	12/4.5	0/1	4/8	4/5	0/1.5	4/5	4/3
Agree	60/58	26/28.5	4/7	47/50.5	27/31.5	16/9.5	41/32	19/20
Cybersecurity training fails if the trainers are unskillful (χ^2 =50.560, df = 32, p-value <.05)								
Disagree	3/9	10/5	1/1	9/8	3/5	1/1.5	4/5	4/3
Agree	42/41	25/20	5/5	27/35.5	23/22	9/7	24/23	12/14

4.4.2 Education level and training adaptability factors

The education level factor was also significant, though to a lesser degree than the job role regarding the trainer; as disclosed by my Chi-square analysis in this study, all education levels agreed that having a skilled trainer was important.

However, the Chi-square results test found that postgraduate degree holders, over people with lesser educational levels, have the same opinion about the importance of customising

the training for better outcomes. *Motivation* factor avoiding boring and routine sessions is also holds for persons with higher degrees, such as postgraduate or bachelor's degrees, moreover, as revealed by the chi-square test results *simplicity* factor also strongly supported by bachelor's and postgraduate degree holders who they assert that simple language needs to be used to deliver cybersecurity content. As such, through the chi-square test results, it has been found that postgraduates extend utmost importance to the training method for its success followed by those who hold bachelor's degrees. As such, the higher the educational level (postgraduates), the higher the inclination is seen towards the training environment for its success (more details in Table 4.14).

Table 4.14: Educational level and reasons for cybersecuriy training to fail

	<Secondary Count\Exp	Secondary Count\Exp	Colleges Count/Exp	Bachelor Count/Exp	Postgraduate Count/Exp
Cybersecurity training fails if it is difficult and includes technical language (x2 = 40.409, df = 20, p-value <.001)					
Disagree	**0/.5**	**1/.9**	**4/4.2**	**35/28.7**	**4/10.5**
Agree	**0/2.5**	**4/4.7**	**20/21.5**	**156/146**	**48/53.7**
Cybersecurity training fails if it is provided in one-size-fits all (x2 = 38.200, df = 20, p-value <.01)					
Disagree	**0/.6**	**0/1.1**	**3/5.2**	**39/135**	**12/12.9**
Agree	**0/2.4**	**7/4.4**	**17/20.4**	**148/138.2**	**45/50.9**
Cybersecurity training fails if it is boring and routine (x2 = 41.666, df = 20, p-value <.01)					
Disagree	**0/.4**	**2/.7**	**4/3.1**	**20/21**	**6/7.7**
Agree	**2/2.5**	**1/4.6**	**12/21.1**	**152/143.4**	**57/52.7**
Cybersecurity training fails if it the delivery training methods are poor (x2 = 46.049, df = 20, p-value <.001)					
Disagree	**0/.5**	**2/1**	**0/4.5**	**4/30.6**	**5/11.3**
Agree	**2/2.6**	**7/4.9**	**13/22.4**	**157/152.4**	**60/56**
Cybersecurity training fails if the training environments are limited (x2 = 35.424, df = 20, p-value <.05)					
Disagree	**0/.4**	**0/.8**	**0/3.6**	**34/24.2**	**4/8.9**
Agree	**1/2.7**	**7/4.9**	**18/22.8**	**153/154.9**	**63/57**
Cybersecurity training fails if the trainers are unskillful (x2= 31.426, df = 20, p-value = .050)					
Disagree	0/.4	2/.8	6/3.7	28/24.9	3/9.1
Agree	1/1.9	3/3.5	10/16	121/109	36/40.1

4.4.3 Work experience and training adaptability factors

In this study, the chi-square test reveals only two variations in the factors that contribute to adaptive training and work experience: avoiding technical terms or simplicity and the significance of customising training. To clarify more, the Chi-square results indicated that

employees with 2–15 years of experience insisted on the simplicity of cybersecurity training when compared with other groups. This also holds for lesser experienced (2-5 years) people on customizing the training followed by those having 5-15 years of experience. However, other factors, such as motivation among learners, training techniques, the training environment, and the trainer, were insignificant. (More details in Table 4.15).

Table 4.15: Years of experience and reasons for cybersecurity training to fail

	<2 Co\Ex	2-5 Co\Ex	5-10 Co/Ex	10-15 Co/Ex	15-20 Co/Ex	20-25 Co/Ex	>25 Co/Ep
Cybersecurity training fails if it is difficult and includes technical language (x2 = 59.360, df = 28, p-value <.001)							
Disagree **Agree**	**0/2** **7/8**	**11/7** **45/34**	**11/8** **41/43**	**7/8** **51/41.5**	**4/8** **37/43**	**3/6** **31/28**	**5/5** **10/25**
Cybersecurity training fails if it is provided in one-size-fits all (x2 = 57.647, df = 28, p-value <.01)							
Disagree **Agree**	**2/2** **10/8**	**12/8** **41/33**	**12/10** **37/40.4**	**10/10** **44/39.4**	**8/10** **42/40.1**	**5/7** **29/26.8**	**2/6** **14/24**
Cybersecurity training fails if it is boring and routine (x2 = 20.626, df = 28, p-value =.841)							
Disagree Agree	0/1.2 11/8.1	7/5 39/33.8	7/6.1 39/41.8	7/6 44/40.8	3/6 38/41.8	4/4.1 29/27.8	4/3.6 20/24.6
Cybersecurity training fails if it the delivery training methods are poor (x2 = 25.994, df = 28, p-value = .573)							
Disagree Agree	2/1.7 10/8.6	5/7.2 44/35.9	10/8.9 47/44.4	12/8.7 48/43.3	2/4.6 14/18.3	5/5.9 26/29.5	6/5.3 20/26.1
Cybersecurity training fails if the training environments are limited (x2 = 34.014, df = 28, p-value = .200)							
Strongly disagree Strongly agree	2/1.4 9/8.7	4/5.7 44/36.4	4/7.1 56/45.2	8/6.9 46/44	10/7.1 32/45.2	7/4.7 28/30	3/4.2 24/26.6
Cybersecurity training fails if the trainers are unskillful (x2= 30.218, df = 28, p-value = .353)							
Strongly disagree Strongly agree	1/1.4 4/6.1	4/5.9 33/25.7	8/7.3 35/31.8	10/7.1 33/31	5/7.3 27/31.8	6/4.8 18/21.1	5/4.3 16/18.7

4.4.4 Gender and training adaptability factors

As far as gender perception is concerned, the chi-square test results reveal that females, contrasting their counterparts, are more inclined towards having customized training. However, training may be ineffective for both genders if it is boring and routine, challenging, and includes technical terms; the training methods are poor; the environment is not conducive to learning; or the trainer is insufficiently skilled, as our study found no statistical correlation between gender differences and those reasons for cybersecurity training failure. (more details in Table 4.16).

Table 4.16: Gender and reason for cybersecurity training to fail

	Male Count\Expected	Female Count\Expected
Cybersecurity training fails if it is provided in one-size-fits all (x2 = 12.635, df = 4, p-value <.05		
Strongly disagree **Strongly agree**	**18/9.8** **45/48.4**	**6/14.2** **73/69**
Cybersecurity training fails if it is boring and routine (x2 = 1.707, df = 4, p-value .789)		
Strongly disagree Strongly agree	10/9.9 76/69	14/14.1 92/99
Cybersecurity training fails if it is difficult and includes technical language (x2 = 8.340, df = 4, p-value =.080)		
Strongly disagree Strongly agree	8/8.6 74/69.9	13/12 96/100.1
Cybersecurity training fails if the delivery training methods are poor (x2 = 6.081, df = 4, p-value = .193)		
Strongly disagree Strongly agree	8/6.2 70/61.2	7/8.8 79/87.8
Cybersecurity training fails if the environment are limited (x2 = 5.306, df = 4, p-value = .257)		
Strongly disagree Strongly agree	10/7 50/42.7	7/10 54/61.3
Cybersecurity training fails if the trainers are unskillful (x2= 3.733, df = 4, p-value = .443)		
Strongly disagree Strongly agree	12/9 22/22	101/96.2 133/137.8

4.4.5 Age and training adaptability factors

This study found that the training environment is crucial for employees of varying ages. For instance, those between the ages of 26 and 35 recognise the significance of the environment the most, followed by those between the ages of 36 and 45. As my study reveals,

there was no correlation between age and other factors that create adaptive training, such as customising, avoiding technical terms, the training methods, motivations, and the trainer; therefore, It is widely acknowledged that these factors are necessary for enduring the training (More details in Table 4.17.

Table 4.17: Age and reason for cybersecurity training to fail

	18-25 Count\Exp	26-35 Count\Exp	36-45 Count/Exp	46-55 Count/Exp	>55 Count/Exp
Cybersecurity training fails if the training environment are limited (x2 = 35.462, df = 20, p-value <.05)					
Disagree	2/2.2	10/13.6	**21/13.4**	**4/5.5**	**1/3.2**
Agree	11/6	105/86.9	**69/85.8**	**38/35.3**	**24/20.5**
Cybersecurity training fails if it is boring and routine (x2 = 23.414, df = 20, p-value .269)					
Disagree	0/1.9	15/11.8	9/11.7	8/4.8	1/2.8
Agree	10/13	88/80.5	82/79.5	23/32.7	12/14.2
Cybersecurity training fails if it is difficult and includes technical language (x2 = 16.473, df = 20, p-value =.687)					
Strongly disagree	5/2.6	20/16.1	10/15.9	6/6.5	0/.1
Strongly agree	12/13.2	92/81.9	81/80.9	27/19.3	0/.4
Cybersecurity training fails if it is provided in one-size-fits all (x2 = 22.197, df = 20, p-value = .330)					
Strongly disagree	4/3.2	27/19.7	17/19.4	5/8	2/4.6
Strongly agree	8/12.6	81/77.8	80/76.4	34/31.6	14/18.3
Cybersecurity training fails if the delivery training methods are poor (x2 = 23.727, df = 20, p-value = .255)					
Strongly disagree	0/2.8	21/17.2	18/17	7/7	2/4.1
Strongly agree	15/13.8	101/85.5	75/84.4	28/34.7	20.20.2
Cybersecurity training fails if the trainers are unskillful (x2= 24.175, df = 20, p-value = .235)					
Strongly disagree	1/2.3	16/14	12/13.8	9/5.7	1/3.3
Strongly agree	6/9.9	74/61.2	54/60.4	24/24.8	13/14.4

Figure 4.11 summarises the study's findings about the factors that contribute to adaptive

cybersecurity training.

Figure 4.11: Factors leading to adaptive cybersecurity training

4.5 Chapter Conclusion

In this chapter, I have found through a qualitative and quantitative analysis that the most important factor associated with people's cybersecurity training preferences is their job roles. Participants do have their preferences towards offline and online training, depending upon whether they are new in the field or have been exposed to cybersecurity for a while. It is no surprise that, often, they are found to have been insisting on customized training rather than generalized one, because they have already undertaken some kind of training in the past. Participants do have numerous other questions that they look forward to answering by appropriate training programmes.

My interview results have revealed many things. Most of the participants are found to be in favor of having an adaptive cybersecurity training (ACST) programme. To fulfil the objective of developing an adaptive cybersecurity training programme, each training programme needs to be customized. Short training sessions are preferred over long ones by a large proportion of participants. Trainers need to adjust to the requirements of the trainees. At the same time, non-technical vocabulary is a must for creating interest and involvement in training. Training content should be relevant, interactive, and engaging. Although organisations can undertake various activities to raise security awareness among

their employees, trainers can also do a lot through their training programmes. The point to be noted is that cybersecurity awareness is an ongoing process that should not only be limited to times of crisis.

In conclusion, cybersecurity training must take into account the job roles of trainees along with factors such as gender, age, educational level, and work experience. In other words, preferences, backgrounds, and perceptions of trainees are important considerations for developing a robust training programme, which makes the trainees feel that the programme is unique to them. To put it succinctly, matching delivery approaches with trainees' preferences will make the training programme more adaptive, and that is how organisations are likely to succeed in their endeavors to create an effective ACST programme. The findings of this chapter give us insight into the development of an ACST framework to enable employees to thwart cyber-attacks that are often encountered by many on social media platforms. The visibility of developing adaptable cybersecurity training will be further explored in the subsequent chapter by highlighting the differences in knowledge and awareness of social media risks and threats.

Chapter 5

Evaluating the Challenges and Risks Associated with Social Media Cybersecurity

This chapter considers the quantitative and qualitative data covered in Chapter 3 and examines at the challenges that cybersecurity trainers and policymakers have when adjusting SMPs in place as well as the human risk factors associated with participant backgrounds and behaviors. A risk management strategy utilizing the tool risk matrix concludes the chapter.

5.1 Introduction

I define cyber risk as any risk of financial loss, disruption, or damage to the reputation of a person or organisation from some sort of failure associated with information technology systems. As such, risk management encourages the implementation of countermeasures to mitigate risks that adversely affect security requirements (Barrett, 2018; Chapple et al., 2021). Periodic risk management is indispensables (Rajamäki et al., 2018). To this effect, the National Institute of Standards and Technology (NIST) has introduced a cybersecurity risk assessment framework to help develop secure software and hardware (Nurse et al., 2017). However, such a framework ignores human factors that often causes security lapses (Nurse et al., 2017). Risk management approaches that consider the effects of human factors while developing mitigation strategies to prevent cybersecurity risks are scarce (King et al., 2018). Emphasis needs to be made to consider human factors that play a role in getting trapped into security incidents.

The importance of this chapter lies precisely in identifying SMPs communication chal-

lenges and the human factors that are responsible for aggravating cyber risks while using social media. Additionally, this chapter helps me to propose an approach to quantify risk (that is covered in chapter 7), so that organisations can establish countermeasures for resolving cybersecurity issues.

5.2 Social Media Policies' communications challenges

As far as security policies are concerned, most organisations do have those policies in place. However, when the question is asked about SMPs many employees do not have any clue about the significance of these policies, or why they are necessary for their security and the safety of their organisation. One of the interviewees in this study said: "Staff in my organisation is totally in the dark." One of the policymakers said, "We are cautious about the secure use of the internet, but hardly any policy is in place for social media." Someone else said, "We do not have any policy as such, but we train staff for this." He further added: "We train our employees in using the features that are provided to secure them on social media – for example, the two-way authentication." Another interviewee said: "They have SMPs in place; however, it is for those who are authorized to use the company's official social media platform, and any Tom, Dick, and Harry cannot access the account and post on behalf of the company".

A large proportion of the participants agreed that these policies are communicated to them at some workshops and then updated by emails, or tip sheets. The point is that most of the users confirmed that they were trained at least once in their sojourn at their organisations; however, only a few had an opportunity to update subsequently. Usually, companies tend to focus on new employees for security or SMPs as one of the participants confirmed, "We have different things for new hires"; "Old staff needs to take phishing test or some other test at least once a year to ascertain that they are maintaining their awareness on security issues at the required level", added another interviewee.

When organisations want to go securer, they block websites, emails, and social media sites without any security protocols in place. Moreover, they refrain from communicating security policies to their employees; this keeps their employees confused. One of the employees from such an organisation said, "I think they do something with the system so that we cannot access or open anything!" Someone said: "At the beginning, I thought there was a problem with networking!" When he asked one IT personnel, he got a terse

reply: “It is so because of security reasons”. When I interviewed an IT manager serving in a large public sector unit, he gave a similar reply: “Our employees are not allowed to access any social media sites or other sites on the internet for strict security and privacy reasons.”

It is important to explore how stringent are the policymakers and management in implementing the security or SMPs in their organisations. One of the policymakers replied that their organisation takes strict disciplinary action when someone is found violating the security policies. She said, “Policy violations are taken seriously for non-compliance.” These policies are mandatory for everyone and are mentioned in their appointment letters. Another policymaker argued, “By having such policies in place organisational risk is reduced significantly, especially when they are enforced strictly without any exception.”

Another security personnel uttered: “Our IT staff cannot share their solutions online such as in LinkedIn, essentially to prevent cybercriminals to assess our internal setup and infrastructure.”

“SMPs cannot be treated just like other policies,” said one of the policymakers. According to him, "It needs to be updated periodically because we have new kinds of threats and social engineering by cyber-attackers."

5.2.1 Policymakers and Cybersecurity Trainers Challenges

At times, many interviewed from training and education category in cybersecurity field said that explaining the technical terms to non-technical people is a challenging task for them. One of the trainers said, “For this reason, I feel a little bit difficult to conduct this workshop.” Another trainer said it is difficult to convince people to formulate a strong password as they feel that this will make their life complicated. Those who do not use their devices regularly find it challenging to remember their passwords and that makes their life miserable. He further stated, “It is a tough task for trainers to convince users to follow password policy as laid down by the policymakers”.

Finding the right time and venue both pose a real challenge for any trainer to conduct the training. “Garnering a minimum batch size of people who have not only similar preferences but are ready to take training at the given time and venue becomes a challenging task,” explained one of the trainers to whom I interviewed. Something similar was uttered by some other trainee on the environment and the training venue when she spoke, “I

don't like the venue. It was depressing!" She spoke negatively about the lighting and the colour of the walls in the room.

Another challenging task explained by many trainers is how to find a training method that is foolproof in achieving its objectives. Each organisation has different kinds of people with different needs and many of them are reluctant to undergo any training at all. "You have to try everything to get them on board", informed one of the security compliance's officers in an organisation. While trainers prefer an extended period of training, trainees want to finish the session as quickly as possible. One of the trainers said: "It is equally challenging to get everyone involved." At times, it becomes challenging to find the right trainer in line with the training content as pointed out by one of the training officers who were also in charge of training material.

In Kuwait, language becomes a big challenge for trainers as most of the people follow Arabic, it will definitely be the same in every other country where English is not the native tongue. All social media platforms mostly use English that many of the residents do not understand thoroughly. For a better grasp, all security policies and related content need to be furnished in Arabic to make users adaptive to training. Some of the participants proposed adding Arabic subtitles to the videos as many people struggle with the English language.

When cybersecurity trainers are policymakers, they face challenges as well when management is not supportive of investing in cybersecurity technology improvement. That is why they suggest that awareness campaigns should have a top-to-down approach; one of them indicated, "It takes time and a lot of effort; it can be described as the carelessness of management." Another interviewee said: "They (management) always think that they are fine and in a good standard of security!" "Top management's support is crucial to have security policies in place." This is what one of the policymakers said. When they blocked social media in their organisation to prevent access, employees made complaints to the top management and requested to allow them to access YouTube. When the top management becomes lenient on such issues then security policies suffer, and their implementation becomes challenging.

Policymakers responsible for putting security policies in place have been found to struggle with the mindsets of users of social media or the internet. "Putting policies in place is itself a daunting task" which is what is described by one of the senior security officers.

Changing people's attitudes while using social media or the internet is a tough task because people do not take security policies seriously. The responsibility of securing data is left solely on the shoulders of IT professionals. "We have a problem with mindsets", was the terse remark by the security officer. Calling it "a global issue" one cannot shirk one's responsibility, he further added. In other words, altering the mindsets of the people is a challenging task for those who formulate training programmes in cybersecurity, especially, when people tend to learn differently, and therefore, formulating a single kind of learning approach is an inefficient way of training. One of them discreetly said: "You cannot offer one platform or one education for all!".

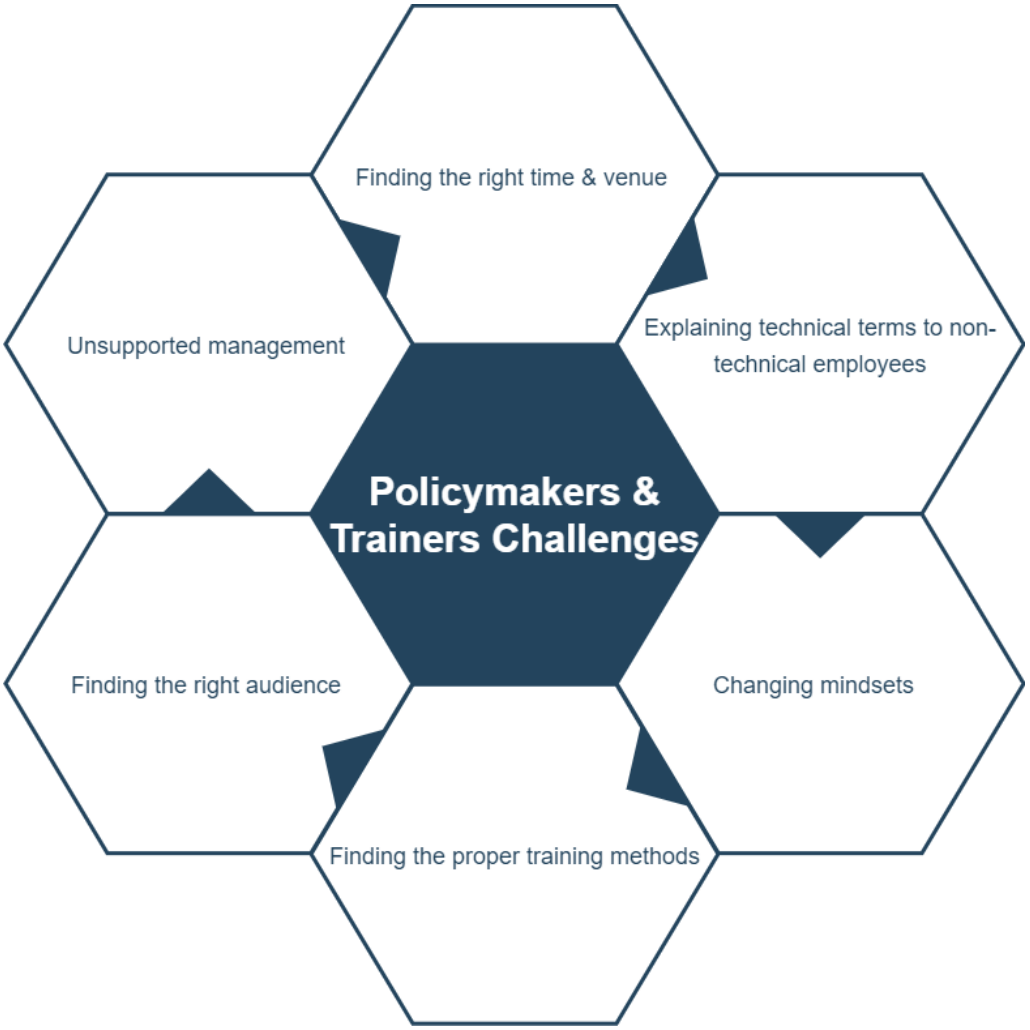


Figure 5.1: Policymakers and cybersecurity trainers' challenges

5.3 Risks Associated with Human Factors

The importance of this section lies precisely in identifying the human factors that are largely responsible for aggravating cyber risks. This is to state that this analysis will help us in formulating an effective cybersecurity risk assessment equation for policymakers and training formations in organisations leading to countermeasures for resolving cybersecurity risk issues (see Equation 7.1 in Chapter 7 for details).

5.3.1 Risk Associated with Job Roles

To assess the security awareness of the participants, I invited their actions on phishing email presented to them. The chi-square test results reveal that depending upon job roles people vary in their security awareness. Those working in administrative and office responsibilities are more vulnerable to phishing attacks as a large proportion of them pressed the blue button (view policy button). The people working in computer and technology fields have more awareness of the aspects of social engineering as they classified the email as a security incident. At the same time, those working in the education, training, and learning sector chose to contact the HR department for further clarifications (more details in Table 5.1).

Table 5.1: Risks associated with job roles' attitudes

What do you do if you receive this email? (χ^2**=36.644,** $df = 24$**,** p**-value <.05)**								
	Education Co/Exp	**IT Co/Ex**	**Health Co/Ex**	**Leader Co/Ex**	**Business Co/Ex**	**Art Co/Ex**	**Office Co/Ex**	**Military Co/Exp**
Click on	10/8	3/4	1/1	6/7	3/4	0/1	9/4.5	0/.9
Ignore	111/110	45/54	11/13	89/96	22/18	62/61	43/37.5	14/11.5
Report	19/25	22/12	6/3	28/22	11/13.5	3/4	9/14	5/8.5
HR	13/10	5/5	0/1	10/9	6/5	0/2	5/6	2/3.4

Regarding the concept of phishing, the chi-square test results reveal that people associated with technology and computer fields are more aware of this; the participants who hold leadership and management positions are least aware of the concept (more details in Table 5.2).

Table 5.2: Risk associated with job roles' knowledge

Which of the following options describe phishing? (χ^2 =53.598, df = 32, p-value <.01)								
	Education	**IT**	**Health**	**Leader**	**Business**	**Art**	**Office**	**Military**
Attack	16/19	7/9	2/2	17/17	12/10	3/3	10/11	9/2
Data	89/86	61/42	9/10	68/75	48/47	10/14	41/48	24/29.3
Followers	7/6	2/3	0/1	5/5	3/3	0/1	8/3	1/2.1
Technical	0/.2	0/.1	0/0	0/.2	0/.1	0/0	1/.1	0/.1
Don't know	41/41	5/20	7/5	43/36	20/22	12/7	25/23	18/14.1

As far as the association between the job roles and online attitudes is concerned, the Chi-square results test reveals many significant correlations. Public Wi-Fi available in cafes, restaurants, or airports is least used by the people involved with learning and training job roles followed by the people associated with computer and technology fields, the participants who hold office and administrative roles are more used to it.

Regarding the question, 'Which kind of people refrain from using anti-virus software programmes to protect their devices', the chi-square test reveals that most people associated with business and financial operations refrain from using any anti-virus software programme. At the same time, the test also reveals that most people associated with technology and computer fields, in comparison to the people from other fields, tend to use more software programmes to protect their devices or assets.

While it is essential to use some kind of anti-virus programme regularly, it is equally important to update those programmes regularly. It is important to know if any correlation exists between 'job roles' and 'updating the anti-virus programme.' The chi-square test results reveal that people in technology and computer fields almost always update their anti-virus programmes; in contrast, people in education, learning, and training jobs as well as people with business and financial operations rarely care about updating these programmes. Checking any link for spelling or veracity of the URLs is crucial before clicking or entering any sensitive data, the Chi-square test results reveal that people from business and financial operations rarely check the authenticity of the URLs before taking any action on the same. Conversely, the people from the computer and technology field do take the most care about ensuring the link's authenticity.

The chi-square test results reveal that people involved with office and business operations do not read and understand security policies related to social media – as opposed to those holding IT, training, learning, or education roles (more details available in Table 5.3 below).

Table 5.3: Risk associated with job roles' online behaviors

	Education	**IT**	**Health**	**Leader**	**Business**	**Art**	**Office**	**Military**
I use public network like those in the cafes or airports (χ^2 =47.562, df = 32, p-value <.05)								
Never	39/32.5	10/16	3/4	32/28	16/18	2/5	18/18	13/11
Often	12/10	0/5	2/1	7/8	3/5	3/2	7/5	6/3.3
I use antivirus software to protect my devices (χ^2 =62.167, df = 32, p-value <.01)								
Never	19/18	3/9	2/2	15/16	18/10	0/3	9/10	6/6.2
Always	45/43	32/21	3/5	38/37	18/23	2/7	22/24	12/14.5
I regularly check the antivirus software update on my computer/laptop (χ^2 =70.973, df = 32, p-value <.001)								
Never	27/20	3/10	2/2	16/17	17/11	0/3	10/11	4/6.7
Always	31/36	30/18	3/4	32/32	14/20	1/6	20/20	13/12.4
I always check the spelling of the URLs before clicking or entering sensitive data (χ^2 =51.749, df = 32, p-value <.05)								
Never	16/13	2/7	3/2	11/12	13/7	1/2	6/7	2/4.6
Always	44/39	33/19	3/5	29/34	13/21	6/6	19/22	11/13.3
Technology alone can protect devices from being hacked (χ^2 =69.876, df = 32, p-value <.001)								
Strongly Disagree	19/24	14/12	0/3	18/21	21/13	1/4	5/13	16/8
Agree	35/35	12/17	11/4	32/31	16/19	3/6	22/20	13/12
I read and understand SMPs (χ^2 =50.327, df = 32, p-value <.05)								
Disagree	18/27	14/13	2/3	20/23	24/14.5	7/4	15/15	9/9.1
Agree	58/52	33/25	5/6	39/45	24/28	10/8.5	28/29	13/17.6

Job Roles and Struggling Areas

It is important to explore if there is any correlation between people with different jobs roles and struggling areas while dealing with cybersecurity issues. The Chi-square test reveals that people operating in administrative and office functions struggle most with 'privacy and confidentiality issues. Protecting privacy is one of the crucial topics that people in this category want to understand and learn as one of them said: "Privacy is the major issue; the most important topic is privacy!" Another participant said, "We are confused on how much information we should provide on social media because we do not know what novel techniques are being employed or can be employed by hackers to hack their accounts?" In other words, they want to know how much data they can share on social media without being at risk. One of the lady participants had a different question about her privacy. She said: "Usually, I am wearing Hijab (scarf to cover the hair); however, sometimes I post my pictures without wearing it because my account is private." She was wondering if keeping the account private is the only option to stay safe online.

According to interview results, those working in office and administrative roles consider passwords an important topic; they have many and varied questions on this. For example, why they should change their passwords every 90 days. How one can assure that chosen password is a strong password. Someone asked: "When we have not disclosed our password to anyone then how come hackers can steal the same and hijack my account." As per the security policy norms, changing the passwords every three months and remembering them later has also been considered a major challenge by some of them. "It is very challenging to choose another new password. Our memory is not helping us every time!"

A considerable amount of confusion exists among the same category (Office and Administration) regarding phishing. Many of the participants had heard about phishing attacks in their life sometimes in the past. They said: "While phishing has been the most effective tool that hackers are employing to hijack organisations' security; however, no one among us is sure how phishing attacks take place or how anyone including our organisation can become a victim of hackers." They wanted to understand all pros and cons of these kinds of attacks in their every form thoroughly including future implications for the organisations. The chi-square test reveals that those who work in the education, learning and training field struggle most to protect their passwords and safeguard themselves from phishing-related issues.

At the same time, the chi-square results test shows that people working with healthcare

support systems and computer fields struggle with spam messages and emails that they receive. Those working in defense or military establishments, in comparison to other field groups, feel challenged by hackers (more details in Table 5.4 below). Many interviewees associated with military or defense establishments wanted to discuss and know more about hackers and their activities. One of them asked: "Why hackers have been able to prove themselves time and again when, on the other side of the table, many experts and qualified people are running and maintaining social media sites." The point is that the participant wanted to know why hackers cannot be defeated in their games once and for all. It was also noticed that those who were without any IT background had different questions in their mind.

Table 5.4: Job roles and struggling areas

	Education	**IT**	**Health**	**Leader**	**Business**	**Art**	**Office**	**Military**
Where do you struggle more? (χ^2 **=127.477,** df $= 64$**,** p**-value <.001)**								
Privacy	59/60	21/29	8/7	49/52	34/32	15/10	43/33	13/20.3
Password	20/13	0/7	2/2	12/12	4/7	1/2	8/7	7/4.6
Phishing	19/13	7/7	2/2	8/12	7/7	0/2	10/7	3/4.6
Email	12/11	8/5	4/1	11/9	5/6	0/2	5/6	0/3.7
Hacking	13/12	0/6	2/1	12/11	7/7	5/2	3/7	8/4.1

5.3.2 Risks Associated with Age

The chi-square test results have revealed significant correlations between age-group and their level of security awareness. Younger employees are found to be less informed than their older colleagues until age 55. Awareness decreases with the increase in age beyond the age of 55. In brief, people in the age group 18-36 and those older than age 55 pose the highest risks for cybersecurity-related incidents (more details in Table 5.5).

Table 5.5: Age and online behavior

	18-25 **Count\Exp**	**26-35** **Count\Exp**	**36-45** **Count\Exp**	**46-55** **Count\Exp**	**55+** **Count\Exp**
I use a strong password **(χ^2 =55.207, df = 20, p-value <.01)**					
Never	0/1	7/7	11/17	1/3	1/1.7
Always	19/16	85/98.5	113/98.5	40/40.5	22/23.5
I use antivirus software to protect my devices **(χ^2 =55.259, df = 20, p-value <.01)**					
Never	14/4	30/24	22/27	3/11	7/6.4
Always	6/.3	53/64	66/63	38/26	15/15
I regularly check the antivirus software update on my devices **(χ^2 =66.235, df = 20, p-value <.01)**					
Never	16/5	33/29	21/29	4/12	8/7
Always	3/9	46/54	55/52	36/22	12/13
I always check the spelling of the URLs before clicking or enter sensitive info **(χ^2 =51.654, df = 20, p-value <.01)**					
Never	12/3	18/20	16/20	7/8	3/5
Always	12/9.5	53/59	60/58	29/24	10/13
Privacy and security are important to me **(χ^2 =37.244, df = 20, p-value <.01)**					
Strongly Disagree	0/.3	0/2	3/2	3/1	0/.5
Strongly Agree	27/22	140/133.5	128/132	53/54	24/31.5
I can read and understand SMPs **(χ^2 =32.499, df = 29, p-value <.05)**					
Strongly Disagree	10/3.5	18/21.5	20/21	6/9	6/5.1
Strongly Agree	2/3	16/18	20/18	12/7	0/.1

I also attempted to investigate the relationship between age-group and their behavior towards suspicious emails presented to them. In this instance, the chi-square test results indicate that the employees in the age group 18–25 are the riskiest compared to the others because they were always ready to click the link in the emails. Those over 55 years of age need more training for they displayed their ignorance to take any action when confronted with such incidents (more details in Table 5.6).

Table 5.6: Age and phishing email

	18-25 Count/Exp	**26-35 Count/Exp**	**36-45 Count/Exp**	**46-55 Count/Exp**	**55+ Count/Exp**
What do you do if you receive this email? (χ^2 =28.496, df = 15, p-value <.05)					
Click on blue button	7/2	10/12	12/12	2/5	3/2.9
Ignore it	25/27	167/165	159/162	65/67	43/38.8
Report it as spam	3/6	35/37	40/37	23/15	3/8.8
Contact HR	2/2	17/15	15/15	3/6	5/3.5

The chi-square test also reveals that employees from different age groups struggle differently when they come across phishing, email spam, and hacking. While the young age-group employee (18-25) have been found to struggle with phishing and hacking more, email spam is posing a challenge to the employee in the age group (36-45). In comparison, the employees above age 46 are found to be struggling more with phishing incidents (more details in Table 5.7).

Table 5.7: Age and struggling areas

	18-25 Count/Exp	**26-35 Count/Exp**	**36-45 Count/Exp**	**46-55 Count/Exp**	**55+ Count/Exp**
Which cybersecurity areas do you struggle with the most? (χ^2 =39.289, df = 15, p-value <.01)					
Phishing	7/4	26/27	18/26.5	15/11	9/6.3
Email spams	1/3	10/16	23/16	7/6.5	3/3.8
Hacking	11/5	25/30	29/30	13/12	6/7.1

5.3.3 Risk Associated with Gender

While attempting to find the association between gender and their online behavior as well as attitudes, the chi-square test results reveal that females are more prone to cyber-attacks than males, and they are found to be less informed in cyber security concepts and controls (more details in Table 5.8).

Table 5.8: Gender and online behavior

	Male **Count/Expected**	**Female** **Count/Expected**
Technology alone can protect devices from being hacked **(χ^2 =87.392, df = 4, p-value <.01)**		
Strongly disagree	79/40	20/58
Disagree	88/82	112/118
Neutral	46/65	112/93
Agree	37/61	111/87
Strongly agree	13/14	22/21
I regularly check the antivirus software update on my computer/laptop **(χ^2 =20.513, df = 4, p-value <.01)**		
Strongly disagree	33/34	49/48
Disagree	40/47	47/67
Neutral	42/60	103/85
Agree	68/60	79/87
Strongly agree	80/62.5	72/89.5

To assess the security awareness of the participants, I invited their actions on a phishing email presented to them. On this, more females clicked the (View Policy) button in contrast to the males displaying their lack of awareness; contrary to this, a majority of the males indicated that they would report the email as spam and send a separate email to the sender to ensure if this was a legit action by them (more details in Table 5.9).

Table 5.9: Gender and phishing email

	Male **Count/Expected**	**Female** **Count/Expected**
What do you do if you receive this email? **(χ^2 =8.559, df = 3, p-value <.05)**		
Click on the blue button	12/14	22/20
Ignore it	178/189	282/271
Report it as spam	48/43	56/61
Contact HR in a separate email	25/17	17/25

Moreover, employees struggle differently based on their genders. Females have been found to struggle more in the areas such as privacy, password protection, phishing, and email spam; however, our test result findings reveal that males struggle more with hacking incidents than females (more details in Table 5.10).

Table 5.10: Gender and struggling areas

	Male **Count/Expected**	**Female** **Count/Expected**
Which cybersecurity areas do you struggle with the most? (χ^2 =23.196, $df = 8$, p-value <.01)		
Privacy and confidentiality	97/103	153/147
Password protection	16/23	40/33
Phishing	15/23	41/33
Emails' spams	16/18.5	29/26.5
Hacking	26/21	25/30

5.3.4 Risk Associated with Educational Level and Academic Qualifications

The chi-square test results also reveal that a significant correlation exists between employees' educational level and their attitudes online. Employees with a secondary or some college education but without any degree are the people found using Wi-Fi networks in public places without giving any due regard to the security and the same goes for password policies. In short, the higher the education of the user, the higher the compliance with security and password policies (more details in Table 5.11).

Table 5.11: Educational level and online behavior

	<Secondary **Count/Exp**	**Secondary** **Count/Exp**	**Colleges** **Count/Exp**	**Bachelor** **Count/Exp**	**Postgraduate** **Count/Exp**
I use public network like those in cafes and airports **(χ^2 =37.215, df = 20, p-value <.01)**					
Never	5/1.5	0/3	14/13	83/87	33/31.9
Often	0/.4	1/.8	5/4	22/25.5	12/9.4
I use a combination of letters, numbers etc. when chosing a password **(χ^2 =48.458, df = 20, p-value <.001)**					
Never	2/2	1/.4	3/2	10/13	4/4.7
Always	4/3	6/6	22/26	181/178	65/65.4
Technology alone can protect devices from being hacked **(χ^2 =39.357, df = 20, p-value <.01)**					
Disagree	3/1	2/2	1/9	66/63	26/23.2
Agree	2/2	4/3	20/14	91/94	31/34.7
I read and understand SMPs **(χ^2 =34.493, df = 20, p-value <.05)**					
Disagree	0/2	0/2	6/10.5	74/71	31/26.3
Agree	2/2	6/4	24/20	152/138	32/50.9

As such, the educational level of users and their security awareness has a direct positive correlation, as revealed by the chi-square test. Employees with more college degrees are, in general, more conscious about cybersecurity concepts or guidelines to remain safe (more details in Table 5.12 and 5.13).

Table 5.12: Educational level and phishing concept

	<Secondary Count/Exp	**Secondary Count/Exp**	**Colleges Count/Exp**	**Bachelor Count/Exp**	**Postgraduate Count/Exp**
Which of the following best describe 'phishing'? (χ^2 =40.684, df = 20, p-value <.001)					
Attack	2/1	3/2	9/7.5	52/51	13/19
Gather data	1/4	5/7	23/34	232/229	98/48
More followers	0/.3	0/.5	7/2	14/17	5/6
Technical skill	0/0	0/0	1/1	0/.6	0/0
Don't know	4/2	5/3.5	20/16	110/110.3	34/40.5

Table 5.13: Educational level and distinguishing the more secure link

	<Secondary Count/Exp	**Secondary Count/Exp**	**Colleges Count/Exp**	**Bachelor Count/Exp**	**Postgraduate Count/Exp**
Which of the following consider more secure link? (χ^2 =24.217, df = 5, p-value <.01)					
Http	4/2	6/4	30/17	107/114	32/42
Https	3/5	7/9	30/43	301/294	118/109

5.3.5 Risks Associated with Work experience

How is users' working experience in years associated with their cybersecurity awareness? The chi-square test results inform those employees with fewer years of experience are the riskiest group. They were less aware of cybersecurity matters, such as they were always eager to press the blue button in case of any email presented to them. At the same time, employees with over 25 years of experience need more training to deal with such emails, as most of them indicated that they would prefer to ignore such emails; in other words, they do not't have a clear understanding of how to react and deal with such security matters (more details in Table 5.14 below).

Table 5.14: Work experiece and phishing email

	<2	**2-5**	**5-10**	**10-15**	**15-20**	**20-25**	**25+**
What do you do if you receive this email? (χ^2 =34.406, df = 21, p-value <.05)							
Click on button	4/1	7/5	5/6	9/6	6/6	3/4	3/3.7
Ignore it	13/16.5	67/69	91/85.5	82/83	83/85.5	50/57	57/50.3
Report it	3/4	15/16	17/19	18/19	28/19	18/12	5/11.4
Contact HR	1/1.5	7/6	6/8	7/8	6/8	8/5	5/4.6

It has been found that given to their years of work experience employees struggle differently. Users with 10-20 years of experience attempt to struggle most in protecting their privacy and confidentiality. Employees with 2-5 years of experience struggle most with spam emails dispatched to their accounts. Phishing posed a challenge to those with less than 2 years of work experience (more details in Table 5.15 below).

Table 5.15: Work experience and struggling areas

	<2	**2-5**	**5-10**	**10-15**	**15-20**	**20-25**	**25+**
Where do you struggle more? (χ^2 =104.958, df = 56, p-value <.01)							
Privacy	6/9	27/37.5	45/46.5	51/45	55/46.5	29/31	27/27.3
Password protection	1/2	10/8	7/10	18/10	12/10	4/7	4/6.1
Phishing	7/2	10/8	14/10	11/10	4/10	5/7	3/6.1
Email spams	0/2	17/7	5/8	3/8	4/8	4/6	10/4.9
Hacking	2/2	3/8	8/9.5	8/9	13/9.5	8/6	7/5.6

The chi-square test demonstrates that, compared to other employees, new hires and those with more experience than 20 years were more concerned about their security and privacy. Although they still believe that their privacy is not their duty and place this on the shoulders of the IT team, new employees with 2–5 years of experience do not believe that technology is capable of offering comprehensive protection. They have grown more mature in their cybersecurity roles, though, as a result of their expanded experience.

As such, understanding the policies relating to social media is challenging for individuals with less expertise, and an employee's understanding of them has grown with experience

(more details in Table 5.16).

Table 5.16: Work experience and knowledge

	<2	**2-5**	**5-10**	**10-15**	**15-20**	**20-25**	**25+**
Privacy and security are important to me (χ^2 =49.519, df = 28, p-value <.01)							
Disagree	1/.2	0/.8	0/.9	1/.9	0/.9	0/.6	2/.5
Agree	3/8	36/34	42/42	39/41	35/42	32/28	30/24.8
I am not responsible for my IS as it is the function of IT employees (χ^2 =49.519, df = 28, p-value <.01)							
Disagree	5/6	34/26	28/32.5	29/32	37/32.5	17/22	23/19.1
Agree	1/4	17/17	35/22	23/21	11/22	11/14	11/12.7
Technology alone protection programmes can protect devices from being hacked (χ^2 =61.707, df = 28, p-value <.001)							
Disagree	11/7	37/30	30/37	30/36	34/37	25/25	19/21.9
Agree	2/5	20/22	19/27.5	33/27	24/27.5	27/18	21/16.2
I read and understan security policies related to social media (χ^2 =50.513, df = 28, p-value <.01)							
Disagree	9/4	24/17	20/21	10/20	16/21	13/14	12/12.3
Agree	7/8	27/32	41/40	45/39	38/40	29/27	27/23.7

5.3.6 Risk associated with time spent on social media

Does the time spent by users on social media have any association with their understanding of cybersecurity-related issues? The chi-square test results indicate that the time spent on social media has a positive correlation to their understanding of cybersecurity concepts. It has been discovered that the users who spend two hours a day on social media have more clarity on the definition of phishing (more details in Table 5.17).

Table 5.17: Time spent on social media and phishing concept

	<30 min Count/Exp	**30-60 min Count/Exp**	**1-2 hours count/Exp**	**2-3 hours Count/Exp**	**3+ hours Count/Exp**
Which of the following options best describes 'phishing'? (χ^2 =38.866, df = 16, p-value <.01)					
Attack	8/303	6/8	22/21	26/21.5	18/26.8
Gather details	12/15	37/34	87/94	102/97	122/120.4
More followers	0/1	8/2.5	6/7	1/7	11/8.7
Technical skill	0/0	0/1	1/.3	0/.3	0/.3
Don't know	6/7	10/16.5	51/45	43/46.5	63/57.8

Similarly, a significant positive correlation has been noticed between the time spent by users on social media and their level of security awareness. For example, in the matter of understanding a secure link and navigating security settings, the chi-square test results indicate that those who spend less than 30 minutes a day on social media, along with those who exceed three hours a day, are less knowledgeable than those who use it moderately (refer to Table 5.18).

Table 5.18: Time spent on social media and the more secure link

	<30 min Count/Exp	**30-60 min Count/Exp**	**1-2 hours count/Exp**	**2-3 hours Count/Exp**	**3+ hours Count/Exp**
Which of the following is considered a more secure link? (χ^2 =38.866, df = 16, p-value <.01)					
HTTP	12/7.3	10/17.1	45/46.7	42/48.1	70/59.9
HTTPS	14/18.7	51/43.9	122/120.3	130/123.9	144/154.1

On the other hand, people who spend more between 1-3 hours a day are more knowledgeable of cybersecurity concepts; they are more capable of protecting themselves. In a way, they reveal that privacy and security are essential to them.

At the same time, those who spend less than 30 minutes a day on social media and those who exceed three hours a day is unable to read and understand security policies provided on those platforms.

It is important to notice here that the people who spend more than 3 hours a day on social

media might cause more risk to themselves and their companies. That is so because they are more reliant on the capabilities of technologies to keep them safe from cyber-attacks; moreover, they also reveal that they make the use of WIFI in public places (more details in Table 5.19).

Table 5.19: Time spent on social media and online behavior

	<30 min Count/Exp	**30-60 min Count/Exp**	**1-2 hours Count/Exp**	**2-3 hours Count/Exp**	**3+ hours Count/Exp**
I am not responsible for my security as it is the IT staff role (χ^2 =38.866, df = 16, p-value <.01)					
Disagree	10/7	15/17	32/46	53/47	65/85.5
Agree	3/5	11/11	36/30	33/31	33/38.8
Privacy and security are important to me (χ^2 =55.589, df = 16, p-value <.01)					
Disagree	1/.2	1/.5	3/1	0/1	0/1.7
Strongly agree	8/15	32/36	99/97	105/100	129/124.7
Technology alone can protect devices from being hacked (χ^2 =27.863, df = 16, p-value <.05)					
Disagree	5/8	24/19	56/52	55/54	60/66.9
Agree	5/6	10/14	44/39	36/40	53/49.5
I read and understand security policies related to social media (χ^2 =28.896, df = 16, p-value <.05)					
Disagree	6/2	6/6	16/16	9/16	23/20.1
Agree	8/9	26/21	50/57	61/58	72/72.6
I know how to navigate the social media settings and set the security options (χ^2 =32.235, df = 12, p-value <.01)					
Strongly disagree	4/1	4/1.5	3/4	2/4	3/5.4
Strongly agree	3/6	20/14	40/39	39/40	48/50.2
I use public networks, like those in the cafes and airports (χ^2 =51.666, df = 16, p-value <.01)					
Never	16/5.5	17/13	38/35.5	26/37	39/45.5
Often	0/2	3/4	15/10	4/11	18/13.4

5.4 Risk Matrix

The 'risk matrix' which is the most widely used technique for tracking and managing risks (Markowski & Mannan, 2008; Duan et al., 2016; Smith et al., 2009);it was used in this study to develop a *graphical representation* that could categorize risk factors and their likelihood of occurring. Our below risk matrix charts were made using Excel. Each calculated risk subfactor in this study is given a probability and an impact value (Qazi & Akhtar, 2020). These risks are then represented on a risk matrix in order to prioritize them (risk analysis) and choose risk mitigation strategies (training).

In Chapter 7, I will go through each of those human factors connected to social media cybersecurity risk and how I weight them individually. However, I estimate that job role and age have the most significant weights, with 40% and 30% respectively, followed by gender and educational level with 10% apiece. Finally, years of experience and time spent on social media have equal weighting calculations with 5% for each.

5.4.1 Job roles risk estimation

I might categorize individuals working in the business and financial sector, as well as those in office and administration, as posing the highest risk, followed by those in education, learning, healthcare, leadership, the military, and the arts, who pose a medium risk. IT professionals, however, are less at risk than other careers. As a result, the possibility of cybersecurity risk because of social media use based on job roles is depicted in Figure 5.2 and illustrated in Table 5.20 below.

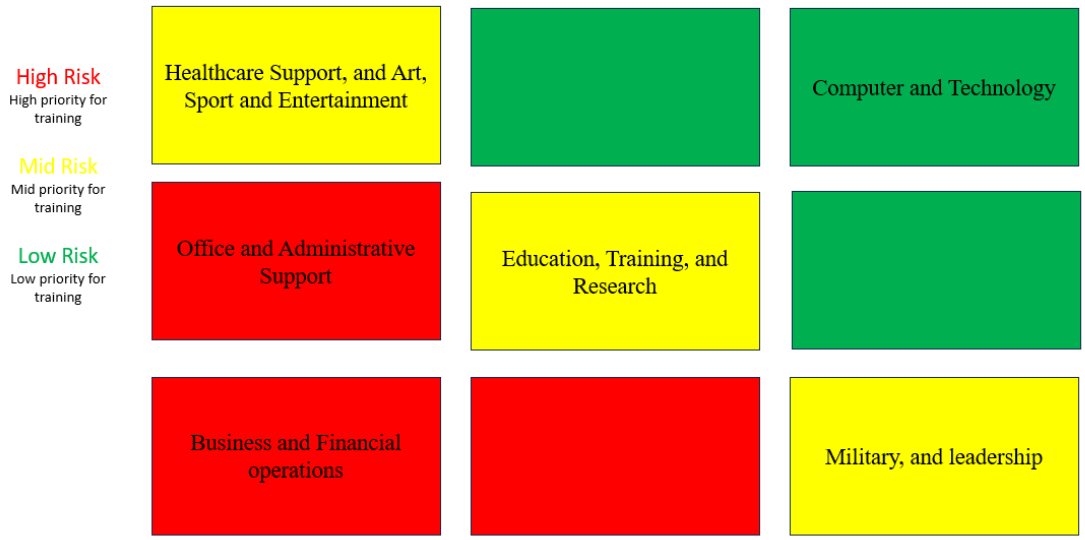


Figure 5.2: Job roles' risk

Table 5.20: Job roles risk estimation

Risk factor (s)	**Impact**	**Probability**
Job role 40%		
Education, training, and research	0.4	0.3
Computer and Technology	0.4	0.0
Healthcare support	0.4	0.2
Leadership and Management	0.4	0.1
Business and Financial Operations	0.4	0.4
Arts, Sport, and Entertainment	0.4	0.1
Office and Administrative support	0.4	0.4
Military such as police and army	0.4	0.2

5.4.2 Age risk estimation

Age, which I considered to be the second most important factor in this study and gave a 30% weight, can be represented as follows: those who are younger, between the ages of 18 and 35, pose the largest risk due to using social media, while those between the ages of 36 and 55 are at medium risk. However, when people become older and reach the age of 55, the risk goes up once more. This factor, "age", is illustrated in Table 5.21 (and Figure 5.3).

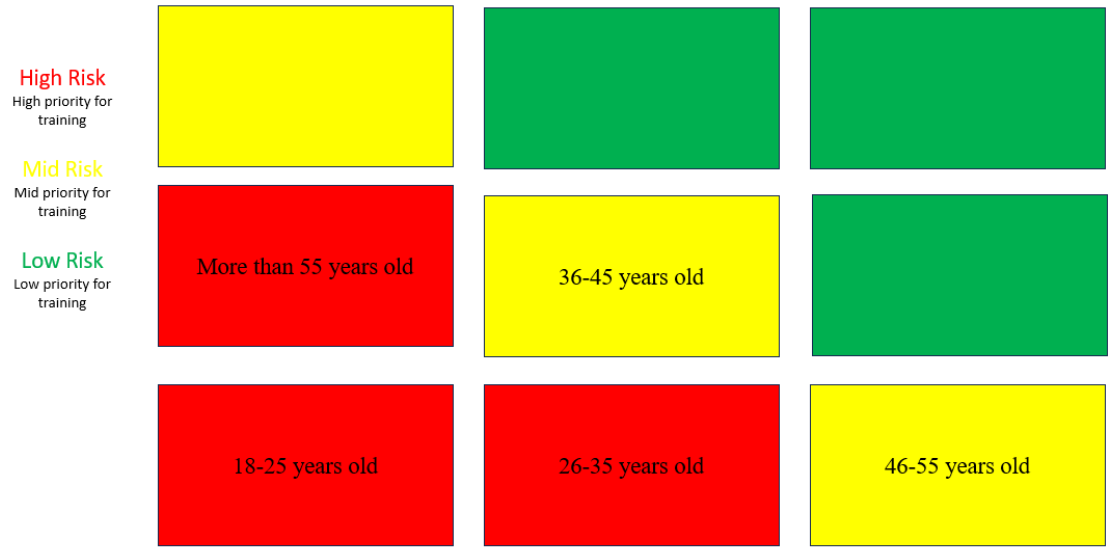


Figure 5.3: Ages' risk

Table 5.21: Age risk estimation

Risk factor (s)	**Impact**	**Probability**
Age 30%		
18-25 years old	0.3	0.3
26-35 years old	0.3	0.3
36-45 years old	0.3	0.1
46-55 years old	0.3	0.1
More than 55 years old	0.3	0.3

5.4.3 Gender risk estimation

Our calculations estimated that gender would contribute 10% of the total weight. Females are more susceptible to cyberattacks than males, according to our data and those from past studies. As a result, I suggested that the female might pose 0.1 risk, which is high risk, and that the male might pose 0.0 risk, which is low risk. These estimations are illustrated in Table 5.22 (and Figure 5.4).

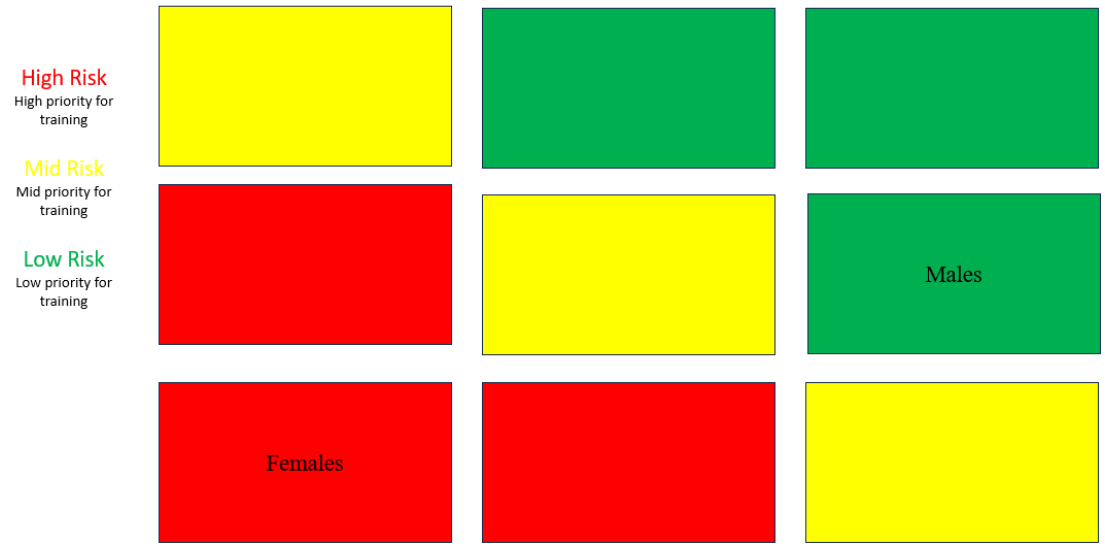


Figure 5.4: Education's risk

Table 5.22: Gender risk estimation

Risk factor (s)	**Impact**	**Probability**
Gender 10%		
Male	0.1	0.0
Female	0.1	0.1

5.4.4 Educational level and academic qualifications risk estimation

According to our calculations, educational level and academic qualifications would account for 10% of the total weight. Using our analysis of our data, I calculated the risk associated with each level of education as follows: people with higher degrees, such as bachelor's and postgraduate degrees, are at low risk with 0.0 estimates. However, social media use puts people with less education at greater risk, Figure 5.5 and Table 5.23 provide illustrations of these estimations.

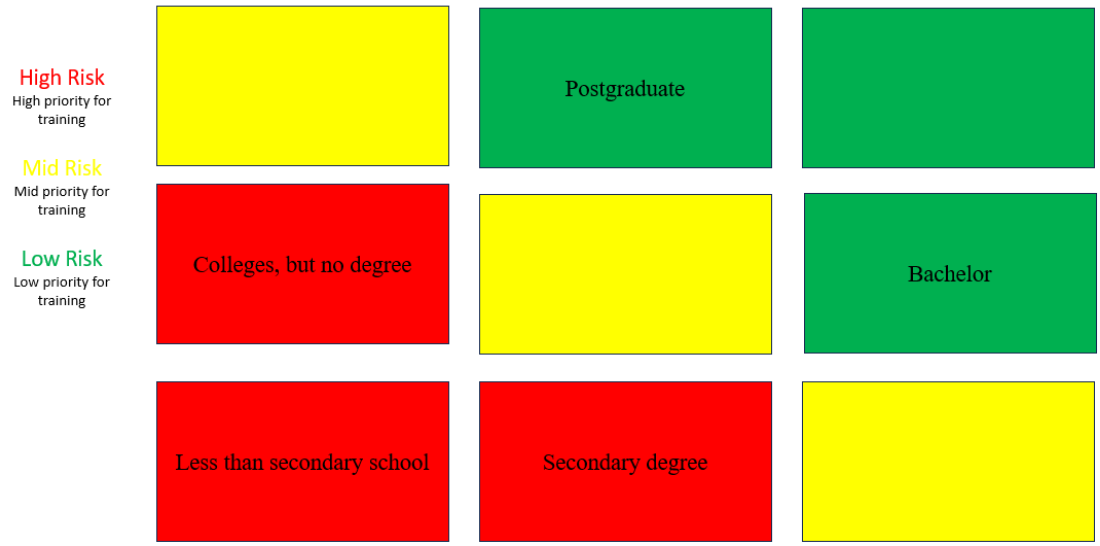


Figure 5.5: Education's risk

Table 5.23: Education risk estimation

Risk factor (s)	**Impact**	**Probability**
Educational Level and Academic Qualification 10%		
Less than secondary degree	0.1	0.1
Secondary degree	0.1	0.1
Colleges, but no degree	0.1	0.1
Bachelor's degree	0.1	0.0
Postgraduate degree	0.1	0.0

5.4.5 Work experience risk estimation

Based on the data I have acquired; I predict that years of experience may entail a 5% risk in comparison to our other factors. In order to quantify the potential risks that users of social media may bring based on their work expertise (in years), Table 5.24 and Figure 5.6 below illustrate those estimations.

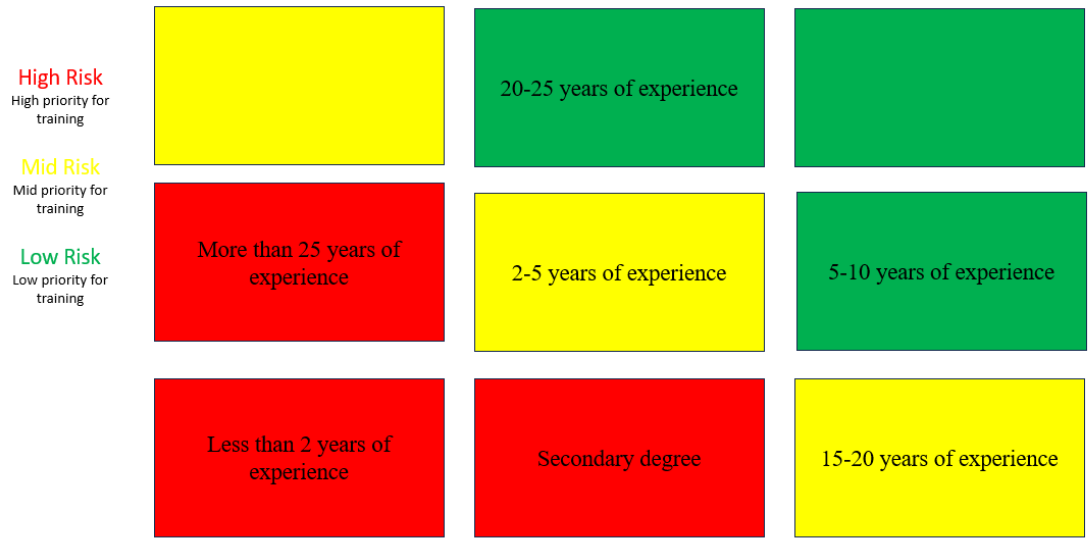


Figure 5.6: Work experiences' risk

Table 5.24: Work experience risk estimation

Risk factor (s)	**Impact**	**Probability**
Years of Experience 5%		
Less than 2 years of experience	0.05	0.05
2-5 years of experience	0.05	0.02
5-10 years of experience	0.05	0.00
10-15 years of experience	0.05	0.02
15-20 years of experience	0.05	0.02
20 - 25 years of experience	0.05	0.00
More the 25 years of experience	0.05	0.05

5.4.6 Time spent on social media risk estimation

The length of time spent using social media is taken into account in this study as a crucial behaviour influencing social media's level of risk. Thus, I discovered that people who use social media for less than 30 minutes per day and those who use it for more than three hours per day pose the most significant threat due to the lower understanding extracted from their answers. As a result, I calculated the risk associated with this factor, depicted in Table 5.25 and Figure 5.7 below.

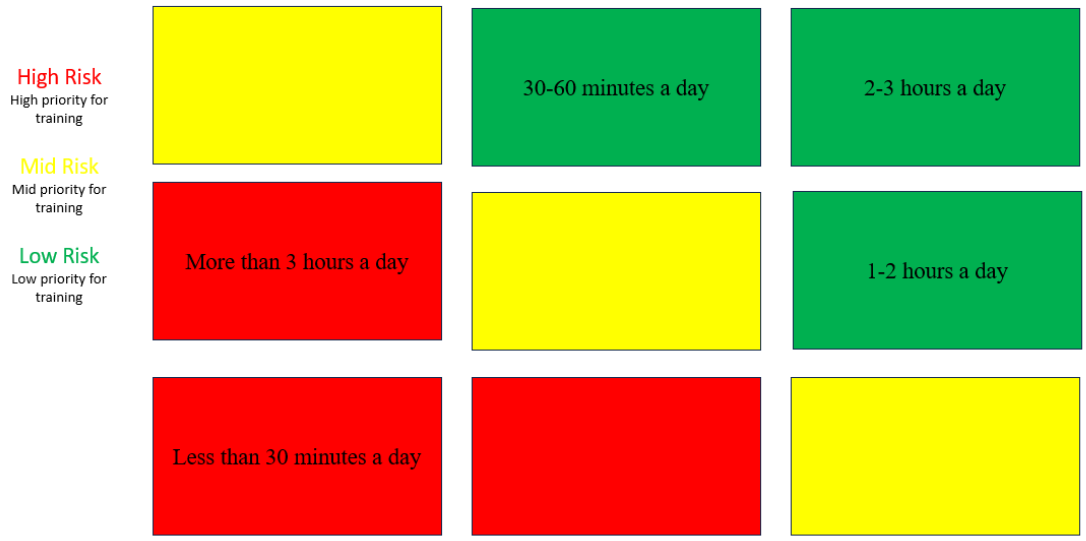


Figure 5.7: Time spent on social media's risk

Table 5.25: Time spent on social media risk estimation

Risk factor (s)	**Impact**	**Probability**
Time spent on social media 5%		
Less than 30 minute a day	0.05	0.05
30- 60 minute a day	0.05	0.00
1-2 hours a day	0.05	0.00
2-3 hours a day	0.05	0.00
More that 3 hours a day	0.05	0.05

As a result, by means of quantitative and qualitative content analysis of the data in this chapter I could sum up the description and preferred response for each risk factor in Table 5.26 below.

Table 5.26: Risk score groups

Risk name	Description	Preferred response
Jo role	The duties an employee is responsible for inside his organisation, and the nature of his work.	These risks are extremely significant, and require a lot of attention. Do not begin designing the training without taking this into account.
Age	The age expressed in years.	
Gender	What gender are they?	These risks are moderately significant, and you can cope with them. However, they will have an impact on how adaptable the training session is.
Educational level	The degree in education presently possesses.	
Years of experience	How long someone has been an employee.	Although these risks can be accepted, you should nonetheless be aware of them.
Time spent on social media	The daily average amount of time spent on social media	

5.5 Chapter Conclusion

The chapter discusses in detail the challenges faced by policymakers and cybersecurity trainers when they attempt to communicate SMPs to the entire staff, especially when human factors have been found to play a pivotal role in blowing away ever-increasing cyber risks on social media platforms.

Using a risk matrix tool to analyze and prioritize the significant factors in this study, I could estimate that the most crucial elements in cybersecurity risks are job roles and the age of users interacting on social media. While people need to be trained based on their

job roles, people handling business and financial operations need to be prioritized for cybersecurity training as they have fallen in the category of the riskiest employees in the company followed by those who work in office and administrative departments and then those who handle leadership and management operations. The experience of the employees and their age are other important parameters to be considered while giving training to them. The lesser the job experience, the higher the cyber risk associated with such employees meaning a fresher faces higher risks while interacting with social media and they must be given priority for cybersecurity training. With the increase in age, users are likely to exhibit more maturity towards cybersecurity policies; however, as our study reveals, people over age 55 needs to be prioritized for training.

As revealed in this study, and which also corresponds well with the findings of many previous studies, females are more prone to cyber-attacks than males for they are less proficient in cybersecurity concepts and therefore, they need to be prioritized for the training. The lesser the educational level, the lesser the clarity with cybersecurity concepts and vice versa. Accordingly, employees with no college degrees need to be prioritized for training. Employees spending less time on the internet and social media and exceeded the average time are likely to be less aware of cybersecurity concepts and therefore, they need to be prioritized for training.

The finding of this chapter leads us to create an equation ,7.1, that helps us to calculate the amount of risk that an organisation might face when their employees interact through social media, and that would be discussed in detail in Chapter 7. In other words, policy-makers and training formulators can make use of this equation to have some assessment of the risks involved with a typical group of employees working with them. As such, the result in this chapter provides me a detailed insight for developing a meaningful and adaptive cybersecurity training framework that can tackle myriads of challenges and risks encountered besides fulfilling the needs of users, the following chapter will present our theoretical framework by analyzing the gaps and limitations that exist in the relevant works.

Chapter 6

Human Factors in Cybersecurity: A systematic literature review

This chapter discusses a systematic literature review using seven journals, two conference proceedings, Hofstede's cultural dimensions theory, the framework proposed by ENISA that considers human aspects concerning cybersecurity issues, and NIST for risk management in cybersecurity. The search was carried out on Google Scholar. Several frameworks are reviewed critically and analysed in this chapter to develop our comprehensive framework to meet our objectives, as listed earlier.

6.1 Introduction

The ultimate objective of this research is to build an adaptive social media cybersecurity training framework to develop the staff of the organisation in full cybersecurity awareness. A systematic literature review (SLR) has been conducted in this research to know as much as possible about the state of the art on this topic and to collect evidence on the evolving nature of social media cybersecurity risks faced by organisations. In this SLR, two compounded collections of search terms were used: 'cybersecurity training, methodologies, framework, and awareness' and 'social media risks, best practices, standards, and policies'. The selection of these phrases has its roots in locating a reasonable variety of material about this topic. The objective is to comprehend how prior research has identified human behavioral weaknesses and vulnerabilities in cybersecurity, particularly in relation to social media, and how organisations have educated their personnel to improve social media cybersecurity.

As with this approach, I started with a deliberate and intentional selection of the information to be reviewed (Aromataris & Pearson, 2014), including journal papers, book chapters, logs, and publications related to our research objectives. Based on the five key stages listed by Duff (1996) and depicted in Figure 6.1 below, I created a list of search terms for our systemic literature investigation.

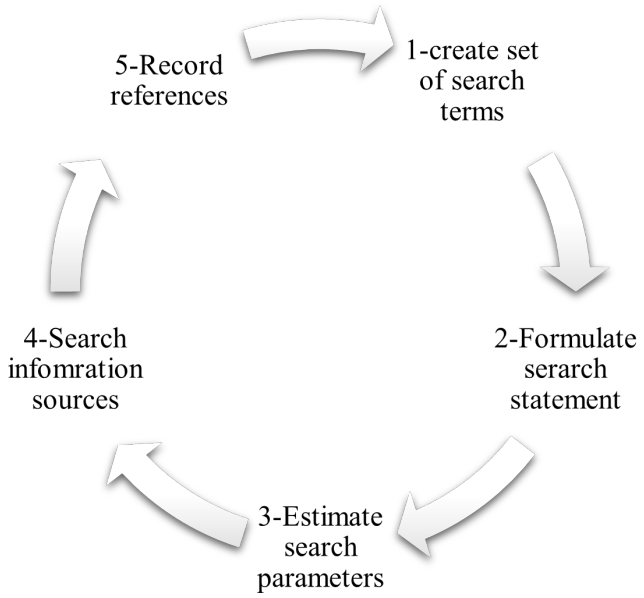


Figure 6.1: Systematic literature search (Duff, 1996)

As a result, exclusion criteria are created to ensure that all works evaluated are founded in sound concepts. If the discovered works do not take into account human variables, they are excluded. Additionally, the study excluded non-English studies, and those published in 2018 and after, I will make sure to only include pertinent literature.

I have chosen the frameworks that meet our objectives for developing the most appropriate framework to develop an adaptive training programme. Due to the limited availability of literature on social media cybersecurity, and further omitting literature that does not consider human aspects in cybersecurity, only a small number of cybersecurity training models can be enlisted here. Based on the SLR, the following frameworks are being reviewed to eventually have our framework for the purpose. Accordingly, I split these frameworks and methodologies into the following eleven major heads as follows.

6.2 Framework for Designing Interventions for the Human Aspect of Cybersecurity

As per the European Network and Information Security Agency (ENISA) (2019), raising cybersecurity awareness is a continuous process (as described in Figure 6.2). Accordingly, the ENISA suggests enhancing user awareness followed by analyzing gaps and vulnerabilities. Then a strategic plan is set to defend against cyber threats where success or failure of the entire process is evaluated keeping in sight the objectives of the security process.

The framework proposed by the ENISA aims at suggesting the ways and processes of raising cybersecurity awareness of users taking into consideration human aspects. It goes without saying that in the process of developing our framework some key aspects of the ENISA framework can be adopted and incorporated. While the ENISA aims at identifying gaps and vulnerabilities of people, I propose to start with identifying the background of our target audience by serving them a quiz to assess their preferences and understanding of the broader aspects of cyber security. This is based on the basic premise that understanding their background is crucial for developing an adaptive training programme.

Figure 6.2: Framework for designing interventions for human aspects of cybersecurity (European Network and Information Security Agency (ENISA), 2019)

The ENISA's framework then focuses on 'analysis'. It offers many methodologies to accomplish this aspect. They support 'surveys' as a valuable tool for having deeper insights on user behaviour and understanding. Surveys in form of a quiz help find gaps and

vulnerabilities of users interacting through social media. The third stage with the ENISA framework is all about the planning process and the fourth stage is its implementation. In our case, this part comprises of designing an adaptive training matching needs and preferences of users, which is based on the information gathered from stages one and three. I can call it the training design stage.

With the ENISA, the final stage in their framework is the evaluation part. I intend to evaluate the validity of our framework using a variety of methodologies, which will be covered in Chapter 8. The European Network and Information Security Agency (ENISA) (2019) also emphasizes measuring changes before and after the training keeping the same measurement process to make a clear assessment of the efforts undertaken.

While this framework does consider human aspects concerning cybersecurity, the ENISA framework largely focuses on general awareness related to cybersecurity instead of social media-related threats. The moot question remains if this framework can be employed to enhance cybersecurity awareness of all kinds of employees within an organisation who have varying levels of knowledge, preferences, and backgrounds. This model needs to be further modified and developed to fulfil our end objectives.

6.3 Competency Development and Assessment Framework

In the framework presented by Brilingaitė et al. (2020), the attempt has been made to develop and assess users including non-technical trainees' cybersecurity skills. While members differ in their background, job role, and experience, this framework takes into account team building, objective differentiation between user groups including steps for developmental assessment by supplementing measure methodologies for cybersecurity training programmes.

The framework presented by Brilingaitė et al. (2020) aims at addressing trainees' needs more discernibly. While emphasizing training for each member of the company, they employ a 'capture the flag (CTF)' exercise for finding an answer to their question - "does training the non-IT staff bring a positive outcome?" They insist that non-technical staff that includes managers, stores people, administrative staff, and alike needs to be trained along with technical people; in the CTF exercise, they are called the 'Purple Team.' This provides a clear indication that training merely a certain section of the staff, and everyone

needs to receive cybersecurity training and learn how to behave properly on social media and against hackers.

According to them, the training needs to pass through four stages: Pre-exercise assessment, pre-exercise training, live activity, and post-exercise assessment or evaluation. Our framework development process derives a meaningful insight from the process suggested by them.

The pre-exercise assessment suggested by them involves knowing the targeted audience and developing the objectives. In other words, collecting details about the trainees including their backgrounds will serve a better purpose in designing a unique practical training for the audience. In a way, the pre-exercise training is close to the third stage of our framework focusing on observing trainees' behaviors and feedback received. This establishes the importance of evaluating the trainees' previous knowledge before designing the training. Figure 6.3 below illustrates the phases of the training suggested by them.

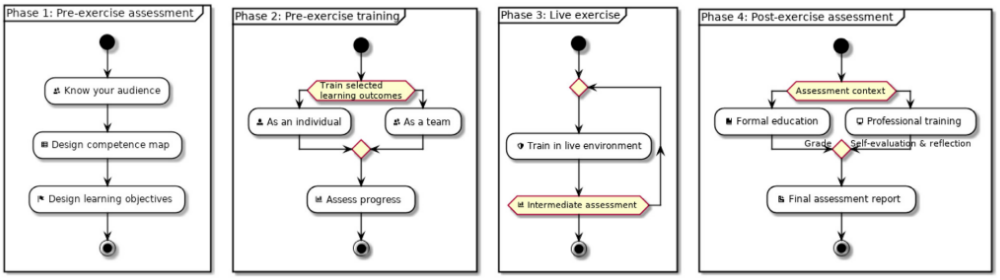


Figure 6.3: Training phases (Brilingaitė et al., 2020)

Brilingaitė et al. (2020) asserts that taking into consideration non-technical people while deciding on a training approach is useful. However, this framework has its limitations in designing a comprehensive framework because it rests on the gaming approach. Our framework focuses on adaptive training by considering all types of training taking into account preferences, perceptions, knowledge of participants, and their background based on the data collected and analysed from our survey results. Moreover, the moot question remains if the framework of Brilingaitė et al. (2020) can tackle social media threats.

6.4 Mission Cybersecurity Framework

Dawson (2018) proposes a framework that can be broken into three distinct areas: education, technology, and policy (see Figure 6.4). These three areas can address matters

that form cybersecurity training. Accordingly, these three core issues can cover up the cybersecurity environment of any country. This also expresses the main objective of our framework associated with social media policies and the best practices employed to educate and train staff across various hierarchies.

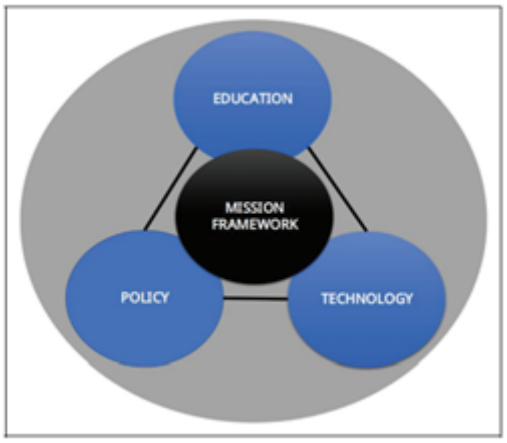


Figure 6.4: Mission cybersecurity framework (Dawson, 2018)

Dawson (2018) asserts that training people about cybersecurity policies and technologies is crucial for superior outcomes. He argues that the security policy serves as a basic guideline helping organisations to set their policies based on their needs. This sets the basic tone and the importance of SMPs to be employed as the best practices for our framework to be developed for developing adaptive training. Nevertheless, this framework is too generic to be applied to our objective of developing an adaptive training programme as it emphasises more on security policies rather than the human aspects of people. As such, the framework does not take into account ever-increasing social media threats in a dynamic environment.

6.5 Holistic Cybersecurity Maturity Assessment Framework (HCMAF)

Aliyu et al. (2020) introduce a novel web-based model that can be used as a cybersecurity assessment and audit tool. The model called "Holistic Cybersecurity Maturity Assessment Framework" that can be used to manage a gap analysis on 15 security terms. This assessment facilitates external clients and suppliers in identifying how strongly the organisation's methods are linked to recognise security measures. The model can be employed

to review compliance and gap that exists for an organisation. The tool can be used as a self-assessment or for building appropriate mitigation plans (see Figure 6.5 for more details).

The framework provides an insight to build an online tool for assessment, and I opt to deploy the Google Form quizzes for assessing trainees and collecting the necessary information. The HCMAF highlights how one can build a model that can measure employee's maturity in terms of best practices, skills, or standards employed. Accordingly, our framework envisages finding out the extent to which the social media users adhere to social media best practices, their knowledge, and skills for keeping themselves secure by following recommended standards and guidelines.

This framework is designed to define the weaknesses and strengths of organisational processes besides ascertaining how stringently the best practices are being followed. Moreover, the researchers assert that the information collected through this framework assessment will assist in identifying current security issues and prioritizing future security plans and funding actions. This supports our framework objectives in helping trainers/training formation and policymakers in planning and developing an adaptive training programme necessary to mitigate social media risks, safeguarding company assets besides saving precious company resources. I derive strengths and insight from the HCMAF model for finding gaps and vulnerabilities of trainees around social media best practices.

While the model provides good insight, it fails to take into account the ever-changing dynamic setup of social media platforms; it is more focused on current security issues. The model is not adequate in itself in developing an adaptive cybersecurity training programme for staff members.

Figure 6.5: Holistic cybersecurity maturity framework (Aliyu et al., 2020)

6.6 Testing, Evaluation, and Training (TET) Framework

Wang et al. (2018) have introduced a TET (Testing, Evaluation, and Training) framework, which has shown its effectiveness in raising cybersecurity awareness. According to them, this approach is superior to the traditional one because it begins with 'testing' to help create customized training emphasizing on trainees' skills and knowledge.

The cybersecurity awareness framework offered by Wang et al. (2018) encompasses three key elements: perception, protection, and behavior. They argue that cybersecurity awareness must have the cognitive proficiency of cybersecurity threats, which gives me an insight that a user must be aware of the dark side of social media - any omission may lead them to serious disaster for themselves. The users must know the ways to safeguard themselves without resorting to any help from others. Their framework, as depicted in Figure. 6.6 below, has three distinct levels namely cognition, knowledge, and skills related to testing, evaluation, and training. These three levels have been earmarked as core steps in our framework. As such, I will begin by testing members of our target group followed by evaluating and analyzing the results to grasp how much they are aware in social media cybersecurity, and then create a training programme that fits their needs, knowledge, and preferences. The framework provides me with great insight for designing an adaptive training programme. Researchers have incorporated a follow-up approach to validate their framework and that provides me good insight to validate the behaviours of

trainee participants in our framework. Nonetheless, the methodology from Wang et al. (2018) takes into account cybersecurity threats in a general sense. Our focus is on social media-related cybersecurity issues. According to them, training needs to be based on the knowledge of trainees. However, I will expand our analysis beyond knowledge and attempt to correlate different human aspects such as preferences, perceptions, attitudes, and demographic characteristics.

Figure 6.6: TET Framework (Wang et al., 2018)

6.7 Cybersecurity Awareness Model

Rieff (2018) proposes a model that can be employed to distinguish particular features of cybersecurity awareness training. The researcher argues that cybersecurity awareness contains three main aspects (Capability, Behaviour, and Context). He asserts that cybersecurity awareness is influenced by capability, which is related to the skills and knowledge of the person. Actions and attitudes speak about users' behavior while using technology; contextual factors focus upon an organisation, situations, and the threats imposed during interaction via the internet.

The framework proposed by (Rieff, 2018) displays how important it is to focus on trainees' behaviors and their capability pertaining to their cybersecurity awareness. While the framework is shown below (Figure 6.7) establishes learning through virtual games; however, it may work with other training approaches too. This framework establishes the importance of human factors when it comes to raising cybersecurity awareness.

Figure 6.7: Construct of cybersecurity awareness (Rieff, 2018)

The framework emphasizes using an evaluation process at all stages and not at the end only. While each stage is distinct from the other, it becomes imperative to represent all evaluation stages in different colors. For example, the first stage mentions objectives and training context; the second stage defines available resources, and the final stage discusses designing the training aspects. The framework evaluation is to be done by experts, and so is the case with me. This framework study provides a clue for developing adaptive training in our research.

The above framework is based on validating a single, especially gaming approach for a cybersecurity training programme. Our approach to validation is to take into account many training methodologies. While the framework is focused on cybersecurity threats in general with emphasis on trainees' capability and behaviour, our focus is on social media threats taking into account further factors such as preferences, perceptions, and human traits of training participants.

6.8 A Theory-Informed Intervention Development Process based on BCW

While developing adaptive training, one important aspect is to focus on ways and methodologies to bring about behavioral changes in users (Alshaikh et al., 2019).

Since traditional training modules mainly focus on imparting knowledge rather than

bringing behavioral changes, the BWC framework as seen in Figure6.8 largely helps to fill up this void. Alshaikh et al. (2019) argues that the lack of a theoretical foundation limits the effectiveness of current cybersecurity awareness programmes in influencing employee behaviour to adhere to security policies. As a result, he uses the BCW framework as the foundation for an intervention design process to create a theory-based training development process.

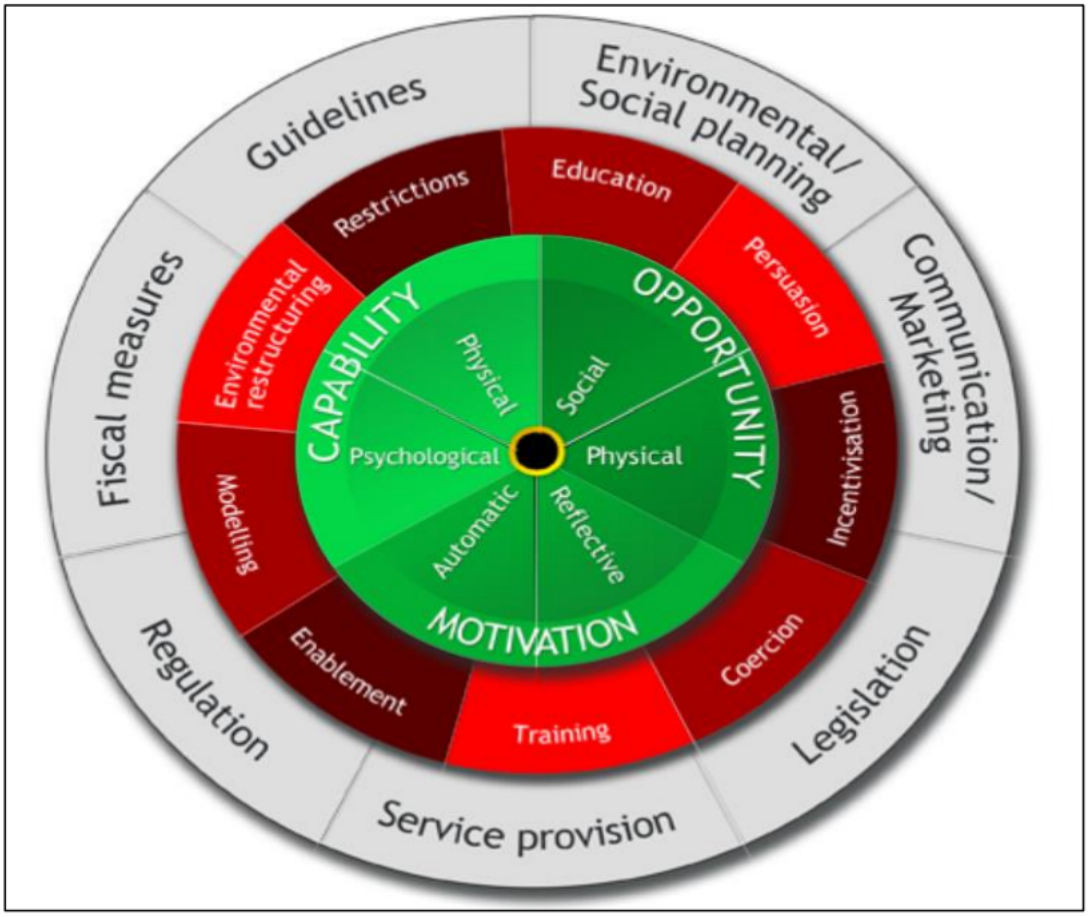


Figure 6.8: The BCW Framework (Alshaikh et al., 2019)

Alshaikh et al. (2019) process helped me to ask some specific kinds of questions in our assessment and understand trainees' needs, preferences, and their level of knowledge related to cybersecurity. The second stage in the framework is to identify the intervention options, which will help me develop our framework too. The last stage involves analyzing trainees' behavior for eliminating risks associated when they interact with others on social media platforms. This framework gives me an insight to apply the theory of change in our proposed model that aims to alter people's behavior (Figure 6.9 for more details).

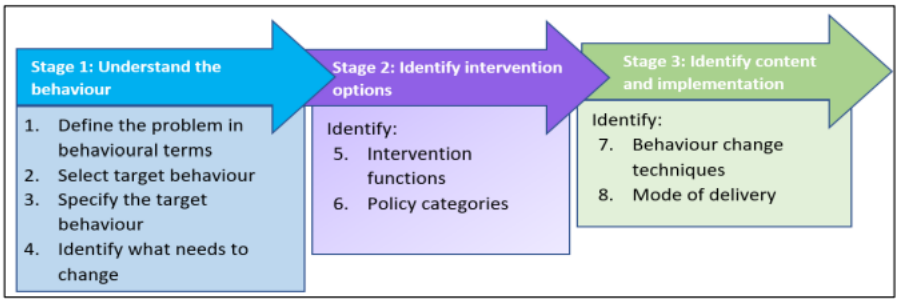


Figure 6.9: Theory-informed intervention development based on BCW (Alshaikh et al., 2019)

While it is true that Alshaikh et al. (2019) focus on the behavioural aspects of participants to validate their model, our focus is on bringing sustainable behavioural changes among trainees taking into account numerous other factors. Moreover, our focus is on social media threats rather than cybersecurity awareness in general. Further, Alshaikh et al. (2019) validated their job in the healthcare sector. However, I also want to know more about other industries, like the military and financial sectors. Thus, I have endeavored to collect information from employees working in various organisations performing many different roles.

6.9 Social Media Risk Management Model (SM-RMM)

Demek et al. (2018) argue that the majority of organisations resort to a reactive approach when they deal with social media risk. The framework put forward by these researchers focuses on social media risk from a cybersecurity perspective and it is supportive in extending some crucial insights for the development of our framework. They opine that social media risk cannot be avoided solely by formulating security policies, but security can be enhanced only by training staff members. In other words, in the absence of proper training, most employees tend to ignore security policies laid down by organisations. The perspective aligns fully with our findings. Their study aims at implementing SMPs across all levels of organisation for mitigating cybersecurity risks, and therefore, training of employees is crucial so that not only they all can be apprised with SMPs but made adept in handling cyber security threats time-to-time. The Enterprise Risk Management – Integrated Framework (ERM-IF) is a risk assessment model, which guides me in developing our framework for designing an adaptive training system. The framework involves

four components as shown in (Figure 6.10) below.

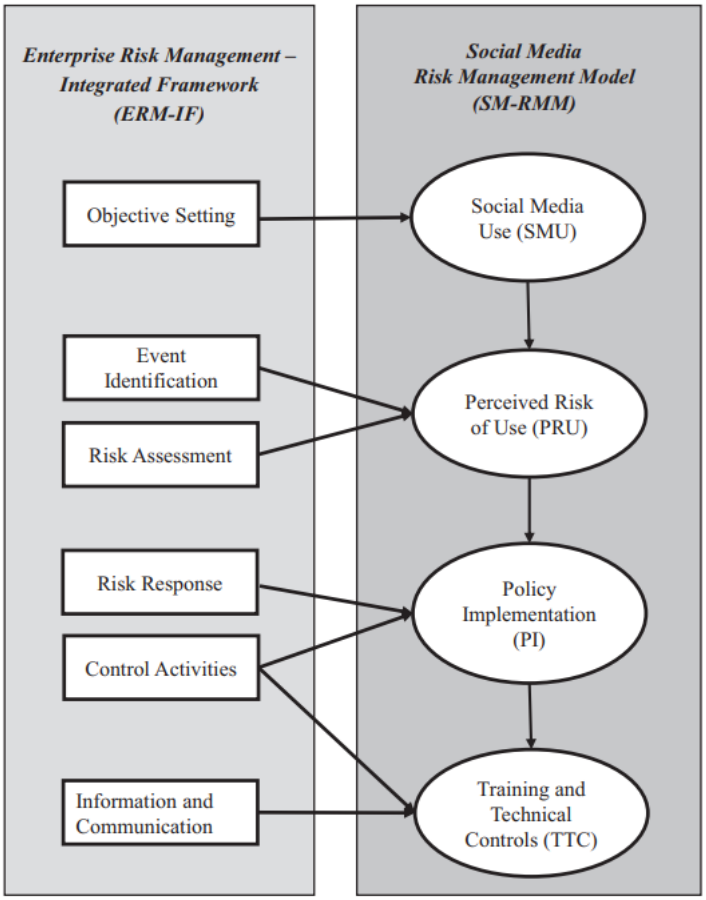


Figure 6.10: Social media risk management model (Demek et al., 2018)

According to the researcher, it is crucial to assess social media risk in its entirety for the reason that the cyber security risk varies with users and that is why it is important to evaluate the risk associated with human factors too. Moreover, he also recommends analysing the risk associated with each social media platform separately because security policies provided by these platforms updated considerably. This model provided me with valuable insight into the significance of educating people about the risks associated with social media in particular as well as a solid basis on which to create our framework process.

This model is supportive in examining if an organisation can address social media risks based on a formalised risk management process. While Demek et al. (2018)'s model does provide insight in a generic sense, our focus is on raising staff awareness through an adaptive training programme, which takes into account several behavioural aspects of social media users. Therefore, the Demek et al. (2018) model can be adopted partially for

fulfilling our objectives.

6.10 Hofstede's Cultural Dimension Theory

Hofstede's theory of cultural dimensions examines the study of international organisations. He gathered information from the multinational corporation IBM and analysed information from forty nations. His research and evaluation of empirical data concluded that (organisations are culturally constrained) Hofstede (2001).

Hofstede's (1984, 2001) work-related cultural dimensions have been employed as a research paradigm in communication between cultures, cross-cultural psychology, and international management over the past three decades. In order to expand Hofstede's (1984) research, my study has collected data from Western Asia, Kuwait, in 2020 to provide up-to-date information regarding work-related cultural values. Second, my study extends Hofstede's (1984, 2001) research by examining the relationship between work-related cultural values and social media cybersecurity.

Hofstede's theory of cultural dimensions argues that the survival of humanity is predicated primarily on the ability of individuals with diverse worldviews to cooperate. He indicated that a deeper awareness of invisible cultural differences is one of the primary contributions of social science to organisational policymakers. This is what I believe in this study, as I intend to investigate people's thoughts and perceptions regarding cybersecurity and social media in order to support those responsible for developing cybersecurity training, trainers, and policymakers in working effectively with the entire staff in organisations.

According to Hofstede's theory, the greater our understanding of a person's mental programming and the surrounding environment, the more precise our prediction will be. I agree with him; consequently, as you will see in my framework development chapter (Chapter 7), I launch my framework with an identification phase that will enable me to gain a thorough understanding of the employee's background and training preferences.

The validation strategy employed in Hofstede's research provided me with invaluable insight into how I could validate the behaviour of my participants. The behaviour of employees may be provoked (simulated by the researcher for research purposes) or natural (occurring regardless of the study and the researcher) based on his validation strategy depicted in Figure 6.11. Moreover, behaviour can be verbal (words) or nonverbal (deeds).

As a result, Hofstede endorses cells 1 and 4 for measurements and the validation procedure; he recommended using cell 1 measurement in conjunction with at least one other type. I realised while reading his book that he recommended integrating the validation process, but not simultaneously, because, as he stated, "Putting all of your eggs in one basket is insufficient." He recommended utilising two measurement techniques that are as dissimilar as feasible and proceeding only if the results converge. As you will see later in Chapter 8, my framework will be validated using this methodology.

	Provoked	Natural
Words	1 Interviews Questionnaires Projective tests	2 Content analysis of speeches Discussions Documents
Deeds	3 Laboratory experiments Field experiments	4 Direct observation Use of available descriptive statistics

Figure 6.11: Hofstede's validation strategy (Hofstede, 2001)

6.11 A Cyber-Security Culture Framework for Assessing Organisation Readiness

Georgiadou et al. (2022) suggests a system to analyse and assess the security preparedness of employees in organisations. Accordingly, they provide an application tool to enhance members' understanding and engagement toward cybersecurity policies.

As depicted in Figure 6.12 , the framework of Georgiadou et al. (2022) takes into account the two levels of a cybersecurity culture. The first is the organisational level that takes into account asset governance, continuity, access, trust, operations, defence, and security. The second level is related to attitudes, awareness, conduct, and competency of individuals in organisations. By using several methods such as questionnaires, simulations, quizzes, serious games, and observations, they attempt to find security flaws and vulnerabilities in an organisation and then organise training to fix those flaws.

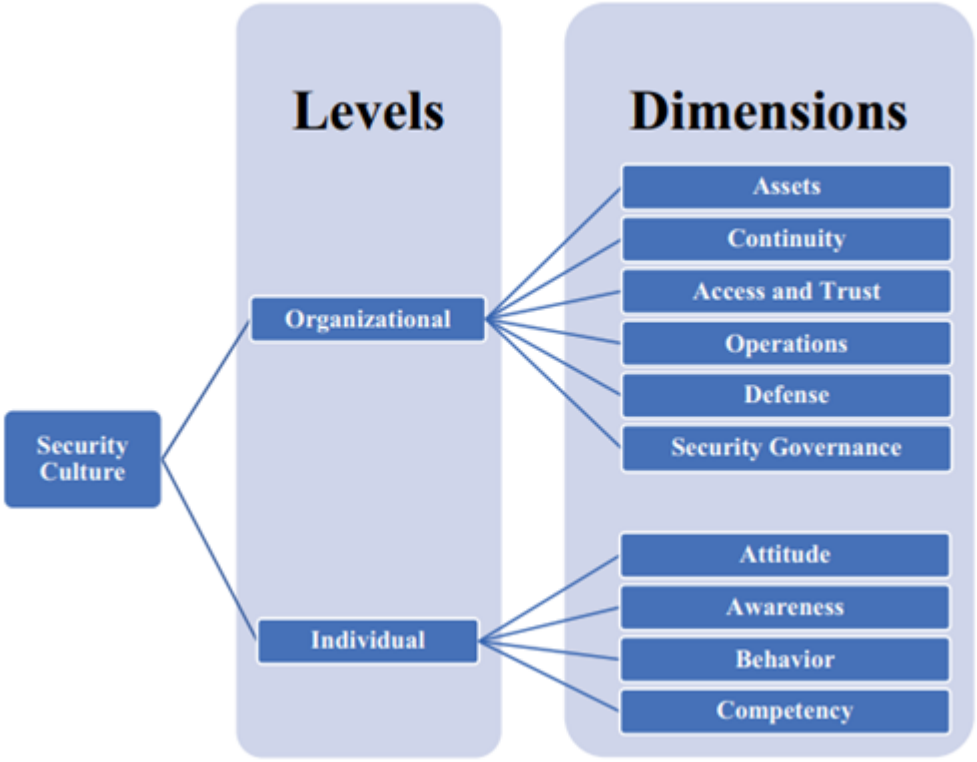


Figure 6.12: Cybersecurity culture model (Georgiadou et al., 2022)

In the framework, while Georgiadou et al. (2022) asserts the importance of human factors, they fail to prescribe how individuals with varying preferences and perceptions need to be approached to enhance security awareness. The researchers focus on the broader culture of cybersecurity without pinpointing the specifics of his approach. In contrast, our approach is to assess the risk levels of individual employees instead of taking a generalised approach. In short, the model proposed by Georgiadou et al. (2022) cannot serve the purpose of developing adaptive cybersecurity training for social media threats. Nevertheless, it does provide me insight into this process of developing an all-inclusive framework that can fulfil our objectives.

6.12 Addressing Human Factors in the Design of Cyber Hygiene Self-assessment Tools

Esparza et al. (2020) presents a framework that not only integrates human factors but also helps create self-assessment tools by simulating the characteristics of cyber hygiene (CH),

which according to them, is the key contributor to understanding cybersecurity issues. The researcher employs the Knowledge-Attitude-Behaviour (KAB) model to ascertain the risk involved in the healthcare industry. The KAB model that expresses the concept of CH is presented in Figure 6.13 below. According to the authors, knowledge is defined as the user's level of awareness, attitude as a general approach to cybersecurity, which is associated with their perceived level of risk, and behaviour as their situation response against the cybersecurity threat.

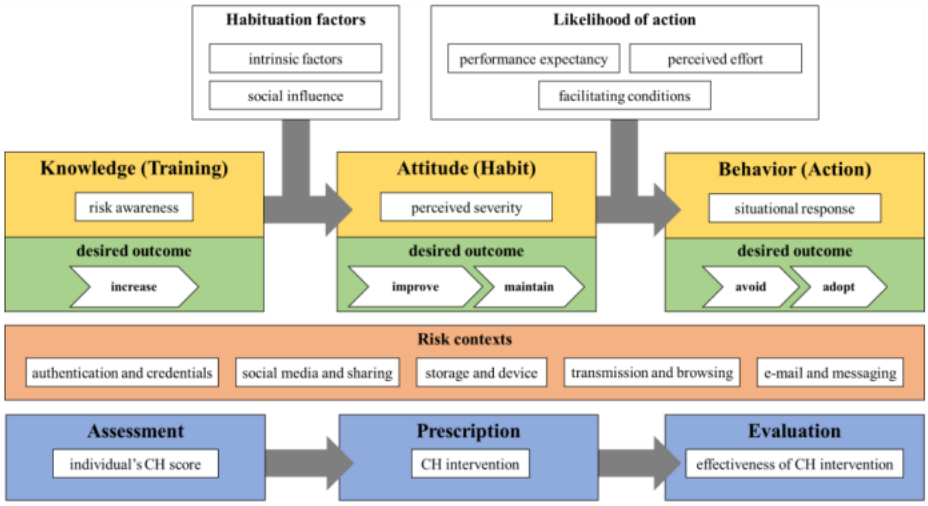


Figure 6.13: Human Factors in CH Self-assessment Tools (Esparza et al., 2020)

By incorporating self-assessment tools, Esparza et al. (2020) attempts to recognise different risk types and their underlying causes. However, it does not make comprehensive use of varying aspects of cybersecurity issues that takes into account the individual preferences and perspectives of users that I intend to develop in our model.

6.13 NIST Cybersecurity Framework

The National Institute of Standards and Technology (NIST) described cybersecurity as a risk management process as shown in Figure 6.14, which is adaptive in facilitating a "flexible and risk-based implementation" to be employed with a myriad of cybersecurity risk management processes (Barrett, 2018). In this study, I gain the ability from the framework to select and improve risk management processes suitable to their policies and controls. Although I am focusing on the human aspect of cybersecurity such as demographics variables, behaviors and attitudes, this framework simplifies for me the

risk assessment process to mitigate security risk. It needs to be noted that the NIST proposes a framework that helps improve the critical cybersecurity infrastructure, still it is complementary to a firm's risk management programme. Likewise, our framework fills the gaps found in the matters related to social media cybersecurity, and not across the whole area of cybersecurity. As their risk management process revolves around prioritising cybersecurity decisions, so is the case with me as I intend to prioritize the risks observed among the staff of the company.

Since the NIST framework provides a common language for understanding, managing, and expressing cybersecurity risk both internally and externally meaning users can access their accounts from any device and from anywhere leads to many challenges for control.

According to the NIST, a framework is a tool for aligning security policies to manage the risk; the same goes with our framework that aims at making employees adhere to SMPs in the organisation. In short, this framework proves to be an important cornerstone in designing and building our framework for.

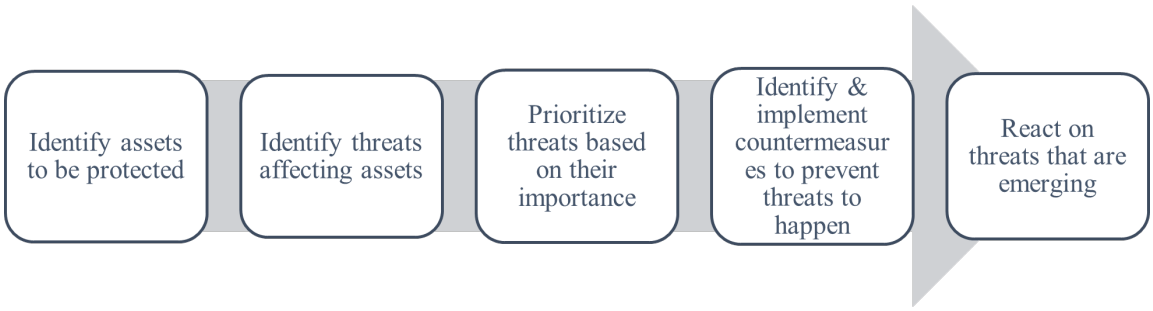


Figure 6.14: NIST cybersecurity framework

6.14 Chapter Conclusion

As to the identified gaps in the existing models, the key issue is that these models cannot be employed as adaptive cybersecurity training for social media risks because these models are too general as well as too complicated to implement. Moreover, the moot question remains if these frameworks can be adapted for all types of employees and could change their behaviors and attitudes on social media with varying levels of cybersecurity knowledge, preferences, and backgrounds?

Although I cannot rely on any of these frameworks to accomplish my goals, the frame-

works discussed in this chapter have had a significant impact on the development of my own framework. European Network and Information Security Agency (ENISA) (2019)' framework has enlightened me to the importance of considering the human element in cybersecurity; Brilingaitė et al. (2020)' framework aided me in designing the training phases; Dawson (2018)'s framework emphasised the significance of security policies as a training material; and Aliyu et al. (2020)'s framework showed me how to use my framework as an auditing tool for the company's stakeholders. The frameworks proposed by Wang et al. (2018), Esparza et al. (2020), and Rieff (2018) were extremely comparable to my own. Still, I expanded my thoughts on the user's knowledge, attitude, and behaviour to include preferences and perceptions of the training, among other factors.

Although we connect with Demek et al. (2018)'s model that focuses on social media risk in particular, and it has a significant impact on the development of my framework for social media risk management, I am filling a gap in this framework by defining risk management as a training tool that assists those responsible for managing the risk within the organisation.

Consequently, the works of Hofstede (2001) and Georgiadou et al. (2022) that focused on cultural differences within organisations substantially impacted the development of my framework, and I kept in mind the significance of cultural differences and human factors when designing adaptive training.

The NIST risk management framework affected my framework in terms of the phases followed to mitigate cybersecurity risk. However, I am attempting to bridge the gap by incorporating human factors that their framework did not account for.

Thus, the need for developing a novel framework towards adaptive training for social media remains. Nevertheless, the chapter has taken into consideration specific aspects of some of these frameworks. Additionally, the evaluation of these frameworks offers some insightful information for developing our novel framework, which aims to develop an adaptive cybersecurity training for social media risks. Accordingly, this chapter has laid down the strong foundation of our proposed framework; the following chapter will discuss our framework development strategies in great details.

To come to the point, this chapter explores a variety of frameworks proposed by different researchers in the field of human factors in cybersecurity. The next chapter discusses our framework development strategies in detail.

Chapter 7

The Framework Development

In this chapter, I will attempt to design and develop a novel framework for adaptive cybersecurity training that mitigates organisational social media threats. Based on the gaps, limitations, and insights gained in the previous works to develop cybersecurity training, risk management, and trying to change people's behaviour in organisations, I will also try with my framework to change people's behaviour in organisations toward social media.

This chapter outlines the techniques that were used to build the novel framework. This chapter goes to great length on the motivations for this framework, the methodology used, and the core functions, processes, domains, and metrics. The section that completes this chapter is about how to use this framework in organisations.

7.1 Introduction

While an innovation, other than developing physical and financial assets, produces new knowledge that eventually helps develop new human skills in an organisation, it is important to understand that this new knowledge requires systematic efforts and a high degree of organisational skill (Johannessen et al., 1999). Therefore, I adopted 'theory of change' as an approach to achieve our desire outcomes in this study. Connell & Kubisch (1998)'s theory of change outlines three key elements that are quite critical to the adoption of the theory which together referred to as "good theory of change," and they can be summed up as follows.

• Is it *'Reasonable'*? Do the data and common-sense show that the actions will produce the

desired results if taken?

• Is it *'Functional'* ? Will the initiative's financial, technical, institutional, and human resources be available to carry it out?

• Is it *'Testable'*? Does the idea of change provide sufficient detail and coverage for an evaluator to monitor its development in reliable and practical ways?

Referring to the theory of change, our framework aims at fulfilling the key operational features (OF) as described below.

• It is *reasonable* in that it gives clear and unambiguous definitions of its aims and purpose, and answer this question: *How and why is adaptive cybersecurity training for social media essential for raising awareness?*

• The simplicity and clarity with which metrics and domains may be tracked show the *functionality* of our framework, and these aspects will be discuss in this chapter.

Our framework is *testable* since, the evaluation methodologies are explicit and largely focused on human connection, which may be accomplished in a variety of ways that will be covered in further detail in chapter 8.

Our methodology aspires to be a novel framework that aims at satisfying these OF. While assessing social media best practices followed within some organisations, the proposed framework takes into account adaptability objectives too. Currently, the importance of social media in all domains is well understood; yet the difficulty involved in managing social media cybersecurity aspects cannot be undermined.

Knowing how much one is at risk and how much an employee can pose a threat to his or her company while interacting on social media platforms is the central issue of this project, and I assume that this can be resolved through adaptive training. *Overall, this framework aims to serve as a benchmark for policymakers, training formulators, and cybersecurity trainers seeking to develop adaptive social media cybersecurity training for their staff*.

I suggested creating a framework because it would guide every area of this study, evaluate our ideas, gather in-depth data, look over our processes, and construct our well-supported theories in the literature (Creswell, 2003). Our proposed framework called an adaptive cybersecurity training Framework for social media risk (ACSTF-SMR) and aims at achieving this key objective of *developing adaptive cybersecurity training to minimize social media risks*.

So, the proposed framework is a risk-based way for organisations to deal with social

media threats. It has five steps: identification, risk estimation, risk analysis, design, implementation training, and evaluation of how well the training sessions performed. This chapter will go over each framework phase in great detail.

7.2 ACSTF-SMR Domains

The overall framework is used as a tool to assess how aware an employee as a countermeasure to social media risks. It aims at identifying all aspects of social media best practices recommended. Based on our analysis, I believe that in order to fulfil our goals and objectives, these four domains should encompass our framework. The first domain is the *human aspect of cybersecurity*; the second domain is *cybersecurity training methodologies* and phases that seek to achieve training objectives; the third domain is social media cybersecurity to be perceived as *risk management*, which attempts to estimate, recognise, and prioritize social media cyber risks (Cybersecurity, 2018); and the last domain considers *social media best practices* employed in terms of guidelines, policies, and procedures. Each domain helps characterize training systems focusing on different areas of social media cybersecurity awareness training.

The domains draw their strengths from cybersecurity ability classifications as presented in the preceding chapter (Chapter 6). These four cybersecurity domains oversee every aspect of cybersecurity training for social media risks.

Several frameworks and models, such as European Network and Information Security Agency (ENISA) (2019), propose a framework for developing interventions for the human aspects of cybersecurity that emphasizes keeping employees aware by constantly analyzing, planning, implementing, and evaluating security awareness approaches, this draws attention to our first domain. For a second domain cybersecurity training, I found a variety of cybersecurity training frameworks on the methodologies being used to achieve training objectives that have been earmarked (details in Chapter 6). The third domain takes inspiration from Barrett (2018) which proposes a flexible and risk-based implementation framework using a multitude of cybersecurity risk management procedures to minimize cyber risks by developing appropriate countermeasures. Social media companies and subject matter experts form the basis for the fourth domain in this framework. Figure 7.1 below illustrates our domains in this study's framework.

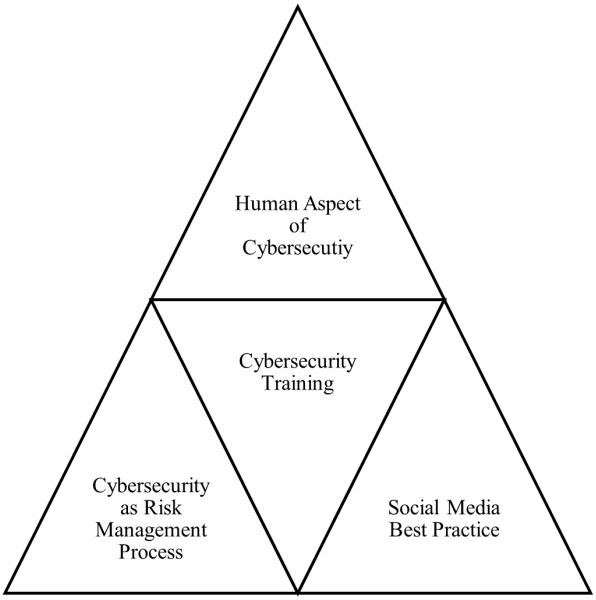


Figure 7.1: ACSTF-SMR Domains

7.3 ACSTF-SM Motivators

Based on our research, I intend to establish that our proposed framework summarise three specific motivating factors that describe trainees' adaptability to cybersecurity training. These three factors can be described as the following.

1- Identification factor

2- Preference factor

3- Awareness factor

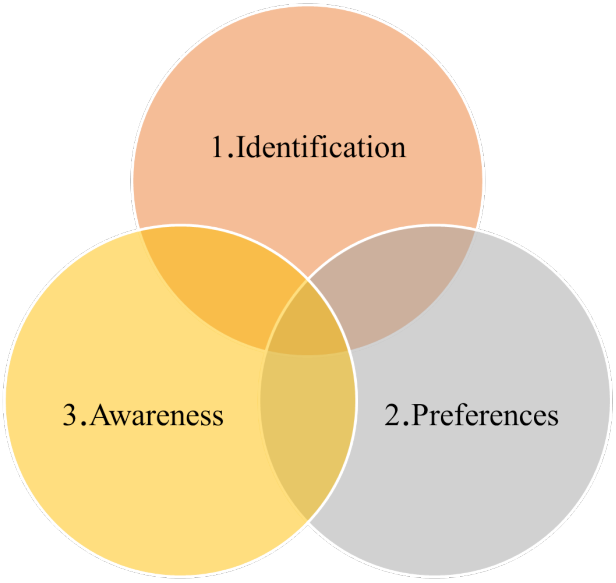


Figure 7.2: ACSTF-SMR Motivators

The first factor "identification" is related to the user's backgrounds such as, gender, age, educational level, working experience, and, most crucially, the role they play at work. Job role/responsibility is crucial in deciding an employee's level of adaptability to the cybersecurity training. While people differ in their preferences, attitudes, awareness, and perceptions, the job role becomes crucial amongst all; in other words, users' perception of cybersecurity is largely influenced by their job roles or responsibilities within the organisation.

Understanding social media users' "preferences" toward cybersecurity training is the **second important factor** of this study. The study also demonstrates that, as described in Chapter 4, individuals have different preferences and perceptions for training-based learning. While many others insist on online training, some others prefer classroom-style instruction. They are more likely to pay attention to their learning and become more aware participants when they enjoy the training. As a result, this factor is essential for creating a programme for adaptive cybersecurity training. Further, people's perceptions on cybersecurity training varied. The study discovered that important elements including motivation, customization, simplicity, the techniques utilised to provide the training, the environment, and the instructors who are skilled at the training session have an impact on how well learners adapt to training sessions. This factors subsequently plays a pivotal role to have an adaptive attitude towards training.

The **third and final factor** is the 'awareness' of users and practices followed by them to spoil cybersecurity threats on social media. People are found to be at different levels of awareness depending upon their age, gender, educational level, experiences, and roles. Fresh employees, for example, are frequently found to be less aware of cybersecurity threats on social media than their more senior colleagues, but this awareness decreases as age increases. So, one can argue that assessing employees' awareness of social media threats can eventually lead trainers to organize or develop a training programme that can deliver superior outcomes.

7.4 ACSTF-SMR Development Methodology

It is important to notice here that our framework of ACST- SM takes into account the Training Design Methodology proposed by Schürmann et al. (2020). According to them, cybersecurity training, as shown in Figure 7.3 below, needs to be done in three major steps. The first step is to carefully analyze the target group. The second step involves a risk assessment, defining physical and virtual assets. The third step is to identify gaps and vulnerabilities. The development of the training material and the evaluation of the training are the additional steps that complete the entire process.

1. Target group
   - Define the target group, target setting, tasks, and responsibilities
2. Risk assessment
   - Define the adversarial environment
   - Define assets, including physical and logical, and processes
3. Threat modeling and risk analysis
   - Model the entire socio-technical system using CORAS/attack trees
   - Derive and prioritize potential attacks
   - Derive the attack surface and tailor it for the target group.
4. Training materials
   - Base training on knowledge gained from (1.-3.)
   - Create an e-learning platform
   - Consider using videos, audio, games as part of the training
5. Evaluate training

Figure 7.3: Training design methodology (Schürmann et al., 2020)

7.5 ACSTF-SMR Core Functions

The framework's core provides a list of tasks to complete various cybersecurity goals and provides examples of advice on how to do so (Cybersecurity, 2018). The ACST-SM

framework consists of five cores functions depicted in Figure 7.4:

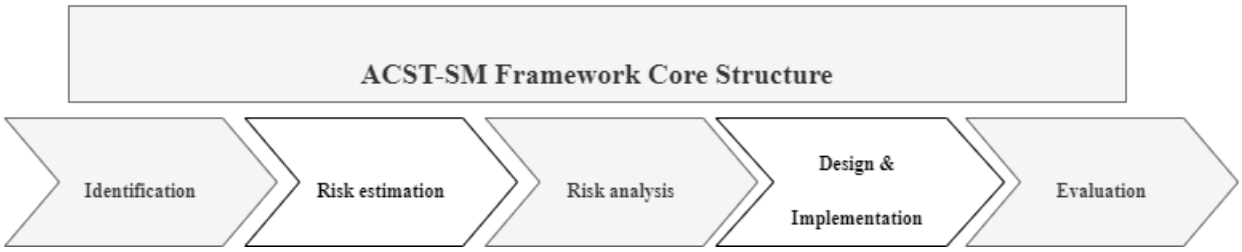


Figure 7.4: ACSTF-SMR Core Functions

The components of the ACSTF-SM core functions cooperate as illustrated below:

7.5.1 Identification

The proposed framework begins with identification that includes knowing users' background, role, age, gender, educational level, and work experience in years. Some other data such as employees' attitudes and behaviors while interacting with others on social media is crucial; moreover, it is equally important to know their preferred training approaches to segregate them into specific groups. European Network and Information Security Agency (ENISA) (2019) supports such an identification approach for the success of the training programme.

7.5.2 Risk Estimation

Risk awareness can be enhanced by communication and risk estimation (Chatterjee et al., 2020). Risk assessment is an important aspect of our proposed framework because it is crucial to know if the confidentiality and integrity of digital data are being compromised at the workplace because of social media usage. In a way, this phase assesses the cybersecurity culture within the organisation; it also attempts to explore the security weaknesses and issues.

Rajamäki et al. (2018) argue that continuous risk assessment and mapping are necessary to reduce cybersecurity incidents. This can be done in many ways including creating focus groups, phishing simulations, tests, and so on, but as per the European Network and Information Security Agency (ENISA) (2019), conducting tests can impart much useful information. Analysis of the collected data will throw light on the participants'

shortcomings and determine the extent to which they need training (Farooq et al., 2011).

In other words, the tool aims at assessing people's level of awareness related to social media threats. The *Social Media Risk Assessment Tool* created for this study is a novel online tool to determine risk based on several interrelated factors. To measure awareness, the tool includes questions that identify user background and assess compliance with social media best practices (refer to Appendix 9.3 to review the assessment).

All assessment questions are suggested by social media companies and mentioned on the NCSC website social media . Google Form Quizzes were used in this study as a web-based application for assessment and data collection. They are used as a tool to customize content and instructional objectives and to collect assessment data, connecting participants with instructors from different parts of the world (Castro, 2018).

Moreover, the survey also contains a question about the preferred training styles in the context of social media cybersecurity. However, instruction in the survey has been modified to read: "Choose the option that best describes your preferences when learning about social media cybersecurity (Please, select as many as apply)."

The web application has been customized in English. The tool also adheres to privacy norms by not collecting sensitive personal information like names and phone numbers. The tool also provides a web-based solution to assess users' risks and create an adaptive training system. The data collected will help formulate a training programme for trainers and policymakers, and the data analysis will also highlight if employees take social media policies seriously.

Depending on the situation, the risk assessment tool fulfils many objectives. Recognizing, prioritizing, and evaluating risks and the probability of cyber-attacks are all part of cyber risk assessment. As per Nurse et al. (2017), analyzing these threats is an important and critical step in establishing effective risk mitigation strategies.

For conducting risk assessment/computation mathematical approaches will be employed to collect data. Tool development for risk assessment is the next step to complete this phase:

Social Media Risk Assessment Tool

A risk assessment tool is a cornerstone of our framework; therefore, it becomes imperative to investigate how the cybersecurity risk management process can be implemented, and

how this process can meet our objectives.

The social media risk assessment tool proposed in this study is broadly based on two main factors: the target group (TG) and awareness (A). To explore the other sub-factors, trainees are asked to take a quiz to assess their level of knowledge regarding best practices followed in social media. The quiz is designed in such a way that it estimates the three levels of security awareness 'high, moderate, and low risk' (Schürmann et al., 2020).

The various parameters used to develop the assessment tool can be categorized as shown in Table 7.1 below.

Table 7.1: Risk assessment parameters

Target Group (TG)	**Awareness (A)**
Job Role (JR)	Hacking (H)
Gender (G)	Privacy and Security (PS)
Age (A)	Password Protection (PP)
Educational Level (EL)	Phishing (P)
Work Experience (WE)	Report Incidents (RI)
Time spent on Social Media (TS)	Two-Factor Authentication (TFA)
Training Preferences (TP)	

Based on awareness scores garnered by trainees, the training programme will be formulated; in fact, awareness score defines the level of knowledge a user or participant has in social media best practices. The score is made up of the three components as described below:

1- To what extent do the trainees know about safety behavior on social media (Knowledge)

2- How the trainees behave in response to any incidents (Behavior), and

3- How the trainees feel about the importance of following best practices recommended (Attitudes)

To arrive at the score for each trainee, a quiz is conducted that includes ten generic cybersecurity questions and five questions for each social media platform, i.e., five questions for Facebook, five for Twitter, and so on (Pls refer to 9.3 for more details). Participants can select from these choices based on their participation in social media.

To avoid ambiguity and for ease of participants, close-ended questions were chosen for this quiz (Reja et al., 2003).

I assume that 50% of the overall degree will be determined by the test results. The remain-

ing space will be used to account for the human characteristics identified in this study as being significant, including job roles, age, gender, educational level, work experience, and time spent on social media (see Table 7.2 for clarification).

Table 7.2: Risk assessment factors

Human Factor (s)	**Awareness Score**
Job Role (JR)	Hacking (H)
Gender (G)	Privacy and Security (PS)
Age (A)	Password Protection (PP)
Educational Level (EL)	Phishing (P)
Work Experience (WE)	Report Incidents (RI)
Time spent on Social Media (TS)	Two-Factor Authentication (TFA)
50%	**50%**

7.5.3 Risk Analysis

As per Chapple et al. (2021), risk analysis is the first stage for developing a defense against impending threats. Assessing how employees can pose risks to an organisation when they interact with others on social media and finding the measures to eliminate those risks is an important step toward fulfilling our objectives.

Social Media Risk Assessment Equation

Three methods are commonly used to evaluate security in an organisation: risk assessment, vulnerability assessment, and penetration testing Chapple et al. (2021). I have pursued the first method, and I have identified resources, threats, and weaknesses to estimate risk.

According to Chapple et al. (2021), the total risk is the amount of risk an organisation would face if no safeguards were implemented. The traditional formula for total risk involves threats and vulnerabilities:

$$\mathit{Risk} = \mathit{Threat} \times \mathit{Vulnerability}.$$

To be precise, risk can be understood as the possibility that a threat exploits a vulnerability to harm assets. As a result, a risk rises as a threat becomes more likely to occur.

To reduce risks to an acceptable level, organisations should identify elements that could

harm assets, and then implement strategies to prevent any harms to such assets. Since employees are commonly considered the weakest link within the organisation Chapple et al. (2021), I will consider them as our assets. Therefore, the harm posed by employees' attitudes and behaviours on social media constitute the vulnerabilities.

To quantify the risk, I propose to establish how much each human factor contributes to an increase of the total risk. I suggest considering the percentages stated in Table 7.3. However, these percentages are only estimates based on the data I have gathered and analysed in our work so far, as reported by Ben Salamah et al. (2022). Policymakers and trainers can be aided by this estimation, but they can also amend the percentages based on their own experience and the conditions of the organisations they work for.

Table 7.3: Calculation for risk assessment factors

Factor (s)	**Calculation**	Weight
Job Role (JR)	Summation of Risks Associated	40%
Age (A)		30%
Gender (G)		10%
Educational Level (EL)		10%
Work Experience (WE)		5%
Time spent on Social Media (TS)		5%

According to our survey findings (Chapter 5), 'job roles' and 'age' are the two most important elements associated with social media risk in organisations. While younger personnel in organisations are less aware than their older counterparts, it has also been found that users over the age of 55 require greater cybersecurity training to interact with others on social media.

Similarly, individuals working in business and financial operations are the most likely candidates for cybersecurity training, followed by those with job experience in office and administrative positions. Females are more vulnerable to cybersecurity risks than males. Furthermore, user education levels are found to be strongly associated with cybersecurity awareness.

Work experience and time spent on social media by users are positively associated with cybersecurity knowledge. However, individuals with more than 25 years of work experience and those with little work experience require more training than others; in other

words, these users are less knowledgeable of cybersecurity aspects than others. People who spend between 1-2 hours per day on social media are more knowledgeable about cybersecurity than those who spend less than 30 minutes, and exceeded three hours each day on social media. In other words, such people are more alert and conscious in dealing with cyber-attacks.

I assume that people in charge of the company's social media accounts will need intense training; this is due to their specific work duties in the organisation. Accordingly, job roles have been assigned more weight than any other factor for the calculation of risk assessment.

Thus, different parameters have been assigned a weight depending upon the replies received in the preceding survey (Appendix 9.3).

Several studies (Gasiba et al., 2021; Zhang et al., 2021) reveal that while imparting training to the employees their job roles need to be considered. Also, I found that a person's job is the most important factor regarding the risk of social media in organisations, and when considering cybersecurity training (Ben Salamah et al., 2022). Gender and age have been identified as major determinants in previous research, thus this study gives them significant weighting. While I was unable to locate any studies on the amount of time spent on social media, and work experience with cybersecurity concepts, our findings reveal some relevance to these factors. However, I have assigned a lower weight to these two factors.

Accordingly, assigning appropriate weights to the factors (as described in Table 7.3), I formulate the following equation for the human risk associated with social media cybersecurity calculation:

$$\mathtt{HumanFactorRisk} = (0.4 \times \mathsf{JR}) + (0.3 \times \mathsf{A}) + (0.1 \times \mathsf{G}) + (0.1 \times \mathsf{ES}) + (0.05 \times \mathsf{WE}) + (0.05 \times \mathsf{TS}). \tag{7.1}$$

The output based on the above calculation will provide three different risk scenarios, namely, *low*, *moderate*, and *high risk*. A value of at most 0.35 as a result of Equation 7.1 indicates low risk; a value greater than 0.35 and smaller than 0.65 indicates medium risk; and a value greater than 0.65 indicates high risk. These values are meant to estimate the risk associated with the employees in the company while they are using social media. I expect

this to help prioritise cybersecurity training. Table 7.1 shows all the risks associated with human factors considered in our study.

Table 7.4: Human factors' risk parameters

Risk (s)	**Impact**	**Probability**
Job Roles (s): 40%		
Education and training	0.4	0.3
Computer and technology	0.4	0.0
Healthcare	0.4	0.2
Leadership and management	0.4	0.1
Business and financial	0.4	0.4
Art, sport, entertainment	0.4	0.1
Office and administrative	0.4	0.4
Military	0.4	0.2
Age: 30%		
18-25	0.3	0.3
26-35	0.3	0.3
36-45	0.3	0.1
46-55	0.3	0.1
>55	0.3	0.3
Gender: 10%		
Male	0.1	0.0
Female	0.1	0.1
Education Status: 10%		
<Secondary	0.1	0.1
Secondary	0.1	0.1
Courses, but no degree	0.1	0.1
Bachelor	0.1	0.0
Postgraduate	0.1	0.0
Years of Experience: 10%		
<2 years of experience	0.05	0.1
2-5 years of experience	0.05	0.05
5-10 years of experience	0.05	0.05
10-15 years of experience	0.05	0.05
15-20 years of experience	0.05	0.05
20-25 years of experience	0.05	0.00
>25 years of experience	0.05	0.1
Time Spent on Social Media: 10%		
<30 min	0.05	0.1
30-60 min	0.05	0.00
1-2 hours	0.05	0.00
2-3 hours	0.05	0.00
>3 hours	0.05	0.1

Examples of ways to apply the formula:

To illustrate how Equation 7.1 can be applied in organisations, I suggest a couple of examples below. In the first case, a female employee who is 45 years old, with a bachelor's degree in Management and 15 years of experience, works in an administrative role, and

spends 2 to 3 hours per day on social media. Because of her "high" risk profile, she must be given priority for training. Her risk will be determined as follows:

$$HumanRisk = (0.4 \times JR) + (0.1 \times A) + (0.1 \times G) + (0.0 \times ES) + (0.2 \times WE) + (0.0 \times TS) = 7/10$$

Our second example involves a 26-year-old male employee who has 10 years of experience working in the IT sector, spends 1-2 hours per day on social media, and does not have a university degree. His risk profile should be placed at the second level of training, because he is at "medium" risk.

$$HumanRisk = (0.0 \times JR) + (0.3 \times A) + (0.0 \times G) + (0.0 \times ES) + (0.0 \times WE) + (0.0 \times TS) = 4/10$$

7.5.4 Designing and Implementing

Raising awareness is a 'skills building' activity that encourages employees to deal with cybersecurity threats (European Network and Information Security Agency (ENISA), 2019); thus, after analyzing the data collected in the previous two stages, I can develop an effective and practical training approach that meets the needs and preferences of the participants.

At this point, it is critical to analyze the variables that influence the process of developing adaptive training for users of social media. Accordingly, attitudes and training approach preferences of people were given due consideration to ensure that designing steps remain methodical and effective for developing adaptive training (Ben Salamah et al., 2022).

Four pilot tests were undertaken to confirm the process, and the general procedures were supported by one cybersecurity expert, one academic and two professional trainers. The training sessions were organized after all of its components were in place. It is important to keep track of the actual training process and its progress (Chowdhury & Gkioulos, 2021). It was possible to record facial expressions and other physical movements when participants underwent virtual training, but it was not possible to do so with other training methods such as videos, posters, or emails. Owing to this reason, different validation methodologies were used that will be discussed in detail in the following chapter.

Utmost care was taken to ensure that the training sessions matched the trainees' needs and preferences to provide me with desired insight into this entire process (Velada & Caetano, 2007). It must be noticed here that I used the ADDIE Model (Figure 7.5) to develop and organize our training sessions (Molenda, 2003).

ADDIE Model

Analyze

The model begins with the analysis process where the emphasis is on finding important parameters such as age, gender, educational level, work experience, training preferences, attitudes, behavior, and so on. The process helps in developing adaptive training.

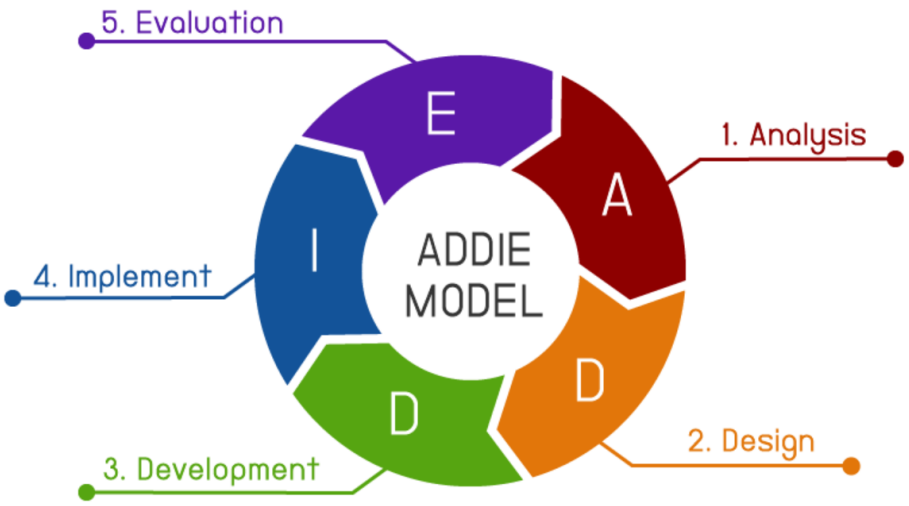


Figure 7.5: ADDIE Model

Design

The design phase search into available training approaches such as online, in-class, gaming, narrative, and so on so that an effective approach can be chosen. Based on the factors known at the analysis stage, all efforts are made to design an appropriate training session for achieving the ultimate objectives of the adaptive training session. It also puts in place a feedback system to determine the efficacy of the session.

Development

The training process may likely have some shortcomings that need to be rectified and developed to the next level. After all, the ultimate objective of the training session is to achieve superior outcomes. Using inputs available from participants and trainers

themselves, necessary modification is done to implement the same in the next training session.

Implementation

Implementing what has been designed is in itself a challenging task (Johannessen et al., 1999). Designing could be flawless but if its implementation is not perfect then the whole exercise may give me wrong feedback, so it becomes of utmost importance to ensure that things are implemented as designed or formulated.

Evaluation

Without proper evaluation, no programme can be improved further. In the entire exercise, evaluation is as important as other processes and that must be done precisely. Evaluation is a continuous process and must be done at all phases to arrive at a summative evaluation after the training programme (Peterson, 2003). Evaluation methods will be covered in greater depth in the next chapter.

The following illustration (Table 7.5) depicts how the ADDIE model is applied to our framework design:

Table 7.5: ADDIE model

Phase	**How the model applied**
Analysis (Goal-setting stage)	Targeting the audience, exploring gaps, weaknesses, and preferences
Design (A systematic approach)	Identifying the training goals, and determining how to achieve them.
Development (Putting into action)	Based on the information acquired in the previous two phases, develop training sessions for each participant.
Implementation (Continuous modification)	Ensuring the positive results of training
Evaluation (Determine if the goals have been met)	Using the formative and summative evaluation approach to ensure that training objectives have been achieved.

7.5.5 Validation

According to European Network and Information Security Agency (ENISA) (2019), every intervention may be assessed in terms of 'process and outcome.' Process validation seeks to determine how the intervention has worked through, and whether it has been implemented correctly. The assessment score, on the other hand, is used to judge if the training meets its stated objectives. In other words, the evaluation phase assesses processes to know whether they have served their purposes or not. I have employed several validation strategies, which are addressed in further depth in the following chapter.

7.6 ACSTF-SMR Process

The framework development process as shown in Figure. 7.6 consists of the following: The first phase in our technique is to identify and characterize the target population (Schürmann et al., 2020). Based on the data obtained in the first stage and the NCSC's social media best practices (NCSC, 2019), the risk posed by the participants will be estimated by collecting data through a quiz administered to them.

Organisations can set priorities for cybersecurity actions and decide how to reduce risks if they have a better grasp of their risk tolerance (Cybersecurity, 2018). Therefore, analyzing the information gathered in phase three will allow me to determine the associated risks, the nature of likely threats, and their preferences for various training options. Based on this, a relevant and realistic cybersecurity training programme for users will be designed and implemented.

The goal of the final phase of our process is to evaluate the success of the training programme so that it may be enhanced further. These Functions offer a high-level, strategic perspective of the organisation's cybersecurity risk management lifecycle when taken collectively (Barrett, 2018).

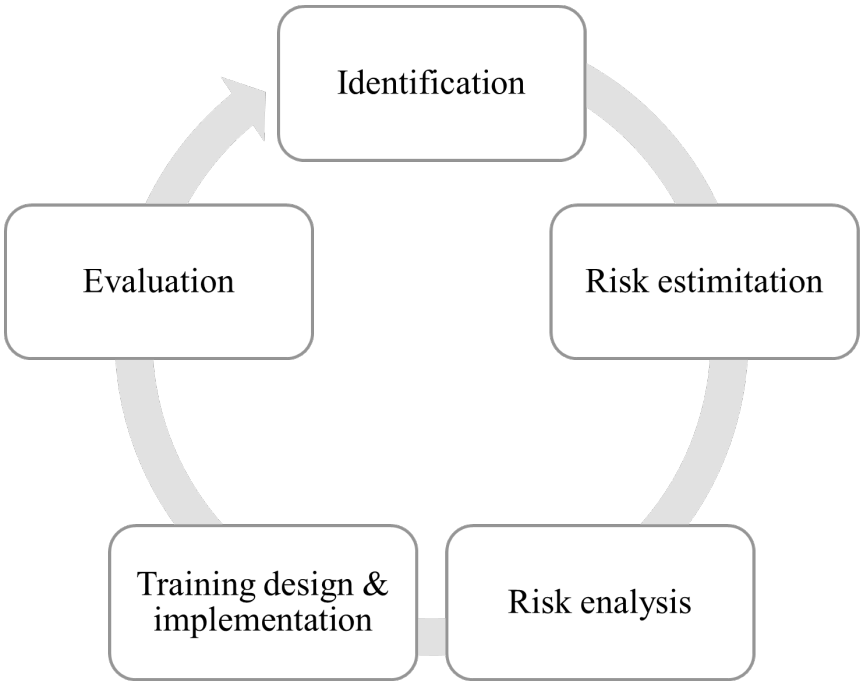


Figure 7.6: ACSTF-SMR Process

To be more explicit, the proposed framework will:

• Aid in identifying employees' backgrounds, which include gender, age, work experience, educational level, time spent on social media, and their role in the organisation. Also, it will aid in assessing employees' preferences for cybersecurity training,

• Assist in estimating the associated risk level based on identification phase and test results,

• Assist in the analysis of the participant data to determine the training's priority,

• Assist in developing adaptive cybersecurity training to reduce social media risks depending on the results of the two prior stages,

• Assist in providing tools for assessing the effectiveness of the training being provided,

7.7 ACSTF-SMR Description

The Framework was created and designed to be:

• A flexible, scalable, and implementable instrument.

• A tool for recognizing, assessing, and managing cybersecurity risks in social media platforms.

• A tool for supplement existing social media guidelines and policies in organisations.

• A tool for increasing understanding of the risks associated with social media cybersecurity concerns, as well as the strategies for managing those risks.

• A tool to improve self-awareness and staff resilience to social media best practices,

7.8 Metrics

Metrics help firms understand their positions in the areas of importance and schedule them for their benefit (Hauser & Katz, 1998). Metrics act as guidelines for organisations to arrive at more efficient methods to accomplish their objectives.As such, the 'security metrics' system estimates a specific aspect of an information system to know the effectiveness of the information security management system (Pendleton et al., 2016). By determining metrics, organisations may strengthen their security posture, increase the awareness of their workforce, benchmark against best practices, and reach a desired level of maturity.

In general, metrics serve a variety of purposes such as customer service, job satisfaction, increasing sales, etc. However, the ACSTF-SM metrics aim at impacting employees' social media behavior by creating an adaptive cybersecurity training system. Our metrics aim at making decision-makers including policymakers, training formulators, and cybersecurity trainers work smarter, not harder. In this study, I carefully selected our metrics and then tested them to determine their effectiveness (The testing results will be discussed in the following chapter 8).

How did I choose our metrics?

According to Hauser & Katz (1998), a good metric should include several useful steps; accordingly, our metrics comprise the following.

First, listen to stakeholders

In this study, in the process of implementing cybersecurity training in an organisation, employees, policymakers, trainers and training formulator are all stakeholders. Through our research, survey, and interviews, I could comprehend how participants perceive cybersecurity training. I could also know what issues prevent employees to get the maximum benefit of the training; moreover, I could also understand what kind of challenges policymakers and trainers perceive in communicating SMPs to the staff. Based on such information, I can build useful metrics. It needs to be noticed that employees tend to change their behaviour in response to a metrics system when these known obstacles are removed,

Second, Understanding the Linkages

I need to have a clear view of what I am attempting to achieve with our metrics. I need to establish linkages between our objectives and metrics. Based on the chosen metrics, I attempt to design our training programme and analyse its effectiveness.

Third, finding correlations and participants' reactions

In this study, I analyse the relationship between the elements of the proposed metrics. Then I evaluate the scores gained before and after using these metrics through the participants' responses. To examine the efficiency of adaptive training vs standard training, I create two groups of participants, one with the customised training and the other with standard training (details will be discussed in the following chapter 8).

7.9 ACSTF-SMR Metrics

It adheres to the principle that what cannot be valued cannot be managed effectively. Therefore, metric is the process of giving an object a value (Pendleton et al., 2016). I will illustrate five metrics selected by me. Metrics descriptions, the way they are measured, the rules, and some recommendations are explained in the following subsections:

7.9.1 Metric one: Risk

Metric Description

One of the study's main objectives is to estimate how much risk a social media user poses to his or her organisation. Their level of knowledge in this area and their backgrounds determine their risk percentage.

I estimated the risk to be calculated by the our risk formula 7.1. The expression of this formula has been illustrated in Table 7.3. It is recommended that employees with higher risk scores be given higher priority in training.

7.9.2 Metric 2: Compliance

Metric Description

One of the primary goals of this framework is to determine whether an employee adheres to the company's SMPs. If a staff member attends training but fails to follow the instructions, it will be construed that they have not been appropriately trained.

However, inspecting staff gadgets to find out if they have activated TFA or not, will not be a proper way to measure compliance with SMPs. Instead, I considered having an anonymous survey (Rise, 2021) at the end of the training to evaluate whether they are complying with SMPs. This survey asks them if they have allowed specific features along with asking other questions.

In this study, pre-and post-test scores were used to measure compliance. Still, it is recommended to find out why staff does not comply with SMPs by interviewing them regularly.

7.9.3 Metric 3: Adaptation

Metric Description

Developing adaptive cybersecurity training is a key factor in this study. The better employees adapt to the training, the more encouraging the results will be.

This metric can be measured by taking feedback from employees at the end of each training session and by knowing how the training can be improved to meet their needs. This metric can also be assessed by asking trainers what they perceive about trainees and the overall training environment. The trainer is also evaluated by taking feedback from staff/trainees about the trainer's effectiveness for the training programme.

I will ensure the participants' anonymity to get impartial feedback.

7.9.4 Metric 4: Report Incidents

Metric Description

The number of social media-related incidents recorded is one way of evaluating employee awareness. According to Ahmad et al. (2021), organisations must incorporate situational awareness into their incident response practices. The lesser the better in our scenario. Many social media incidents can be avoided by following SMPs. Also, instead of contacting IT or subject matter experts within the company, employees need to know how to report social media incidents to the social media companies themselves.

I assume that by tracking the number of social media incidents that are reported, I might calculate this metric. This process is known as auditing and monthly reporting. The development of the next training materials depends on the analysis and categorization of incidents.

7.9.5 Metric 5: Training Quality

Metric Description

The quality of training is an important factor in this study. Is the training topic regularly updated, does the training include appropriate and mixed delivery approaches or is it routine and uninteresting? Is the training tailored to the needs, preferences, and level of understanding of the staff? Is the training easy to understand or complex and does it

include technical terms? Is the training enticing to staff, or do they feel that it is part of their duty and obligatory? Are the training environment and the methods used to deliver the training fascinating?

Five-point Likert scale Feedback survey will be used to measure this metric. Further, the quality of the training can be determined through the survey feedback of the trainees, and the results obtained after the training.

It is important to have experienced trainers for providing the latest knowledge and approaches in the field.

7.10 How to use the ACSTF-SMR

This framework is designed to assist those policymakers, training formulators/designers, and cybersecurity trainers in their job. The framework aids those stakeholders in working more efficiently rather than more diligently, but it is not intended to replace current practices. An organisation can provide adaptive training using this framework as a strategy for managing social media risks, which could result in time, resource, and cost savings. By assessing the degree of employee knowledge in this area, organisations can determine which employees most urgently require training.
The framework can be the foundation for cybersecurity awareness initiatives and improve current cybersecurity processes. The framework will make recognizing employees' social media cybersecurity gaps and vulnerabilities more manageable.

The framework can be applied throughout its five life cycle phases of identifying, estimating, analyzing, designing, and evaluating. The identification phase begins by knowing who our staff is, what they are doing, how they use social media, and what they prefer regarding training. In the second phase, the *Social Media Risk Tool* will assist in understanding how much risk they pose because of using social media; analyzing these data in the third phase will accomplish this task. In the fourth phase, those responsible for designing and formulating cybersecurity training can develop and implement training that meets employees' needs, preferences, and levels of awareness. The evaluation strategies discussed in detail in the following chapter will help those relevant people evaluate their training effectiveness in achieving their stated goals.

7.11 Chapter Conclusion

Thus, the framework as discussed in this chapter helps an organisation to develop capabilities for thwarting and tackling social media cybersecurity-related incidents. While the development of the framework is a continuous process, it helps enhance overall awareness within an organisation. Through risk assessment tools, it can help organisations in establishing risk mitigation strategies in place firmly.

Accordingly, I attempt to see that our proposed framework stands to the test of some key operational features such as reasonability, functionality, testable and adaptability. Thus, the four key elements guide me well in developing our framework.

That is how it is a systematized approach to develop an adaptive cybersecurity training for all types of employees, and the Adaptive Cybersecurity Training of social media risk (ACST-SMR) provides a framework for organisations, particularly trainers, training formulators, and policymakers, to approach the challenges of social media cybersecurity training in a way that meets employees' training needs and preferences. The evaluation methods used to measure the effectiveness of the proposed framework will be discussed in depth in the following chapter.

Chapter 8

Validation Strategies

This chapter is devoted to the validation procedure for our suggested framework; the chapter also examines the metrics addressed in the previous chapter. While a variety of validation procedures has been discussed in this chapter, I begin by testing the metrics and the framework using a couple of case studies followed by a survey and interviews to put the point in the right perspective.

8.1 Introduction

Two different models with the same set of data could anticipate different results with varying degrees of perfection; hence the question comes to validate the proposed framework. According to Schürmann et al. (2020), the framework's validity is established when it is effective in achieving its end objectives. In the current research, the validation of the framework will lead to an adaptive cybersecurity training programme for organisations. There can be a variety of approaches to handle the evaluation of training programmes (Ostroff, 1991), and the best way to know if the programme meets its objectives (Holgado Tello et al., 2006). Evaluation needs to be applied throughout the entire training process (Chowdhury et al., 2022) so that weaknesses in the processes can be eliminated (Chowdhury & Gkioulos, 2021). From the above perspective, it makes sense to apply several validation strategies for our suggested cybersecurity training framework.

8.2 ACSTF-SM Validation Strategies

The validation of ACSTF-SM and its metrics has been done using the following methods:

1-Case Studies: For designing a framework, case studies act as guiding tools for identifying issues that are observed in the actual scenarios (Yin, 2009). Case studies are prepared because they allow me to identify and analyze issues that are likely to be omitted/overlooked in the usual circumstances before it assumes a final shape (Denzin & Lincoln, 2011), it allows me to examine the process in greater detail (Creswell, 2003); and increase the validity of research findings (Bygstad & Munkvold, 2007).

The suggested framework is tested empirically through case studies to find evidence if it supports the outcomes of a training programme. It needs to be noted that the ACSTF-SM has been applied to a variety of people with different roles and backgrounds in Kuwaiti organisations that forms a part of the case study.

2-Survey and Interviews: An online survey has been conducted to get feedback from participants on the structure and content of the training programme. The survey ends with open-ended questions to provide respondents an opportunity if they want to further expand or clarify their views.

Moreover, the trainer also records the reactions of the participants during the training sessions, which were organized virtually. Chowdhury et al. (2022) argues that a trainer/instructor must be involved in the validation process of a training model. Being a certified trainer since 2018 and having conducted several cybersecurity and general soft skills training sessions, the first author is also involved as an instructor in this validation process of the ACST-SM framework.

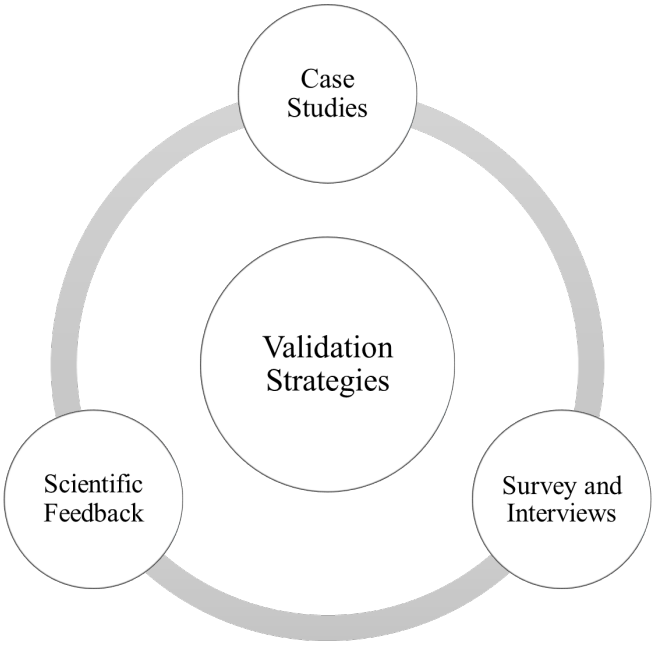


Figure 8.1: ACSTF-SMR Validation strategies

8.3 Strategy One: Case Studies

Case studies take into account Kuwaiti employees who are over 18 and use social media. In all, 38 people are selected for the experimental study, and case studies are used to test the validity of our metrics discussed in the previous chapter. The scenario goes as per the following: participants are identified by taking a test, and the assessment, based on their test results leads me to assess their risk of using social media. Then, they are trained as a countermeasure to thwart the risks, which is based on the information obtained in the first and second phases. The training is then evaluated using a variety of measures to ascertain if the training programme is sufficient.

8.3.1 Background of Study's Subjects

In all, an email invitation was sent to 250 individuals working across various Kuwaiti organisations to participate in an experimental study. The email included information about their role in the study, how long it would take to complete, and their right to withdraw from the study at any time without providing a reason (refer to Appendix 9.3 for more details). Like the previous survey in this project, the Google Form was employed

to collect all data.

Counting, 80 out of the 250 individuals who received this invitation responded and engaged in completing the initial evaluation, and 38 people remained with me all the way through.

In this experimental study, the details of participants have been described in Table 8.1. This information includes their job roles, gender, age, educational level, experience in years, and amount of social media time they spend with social media per day – the variables with significant correlations selected in this study.

Table 8.1: Background of study participants

ID	Job role	Gender	Age	Education	Experience	Time spent on SM
1	Business	M	34	Bachelor	9	120
2	Education	M	55+	Postgraduate	25+	180+
3	Leadership	M	43	Postgraduate	20	60
4	Education	F	40	Postgraduate	15	180+
5	Office	F	36	Bachelor	13	120
6	Education	M	29	Bachelor	7	120
7	IT	M	39	Bachelor	18	180+
8	Business	F	44	Bachelor	22	120
9	Business	M	46	Bachelor	22	90
10	Office	M	33	Secondary	5	120
11	Leadership	F	30	Bachelor	8	180+
12	Office	M	35	Secondary	6	60
13	Office	F	26	Colleges	1	180+
14	Military	M	40	Bachelor	16	180+
15	Office	M	44	Colleges	20	180+
16	Military	M	38	Postgraduate	17	180+
17	Office	F	26	Bachelor	3	180+
18	Leadership	F	49	Postgraduate	22	180+
19	IT	F	41	Bachelor	18	120
20	Leadership	F	32	Postgraduate	10	120
21	IT	M	48	Postgraduate	15	180+
22	IT	F	36	Postgraduate	13	60
23	Leadership	F	43	Bachelor	22	60
24	IT	M	31	Bachelor	5	60
25	Education	F	45	Bachelor	17	150
26	Business	F	33	Bachelor	6	150
27	Office	F	33	Postgraduate	6	180+
28	IT	M	29	Bachelor	5	180+
29	Military	M	42	Postgraduate	24	180+
30	Education	M	32	Postgraduate	7	90
31	Business	M	31	Bachelor	11	150
32	Art, design	M	35	Bachelor	8	60
33	Business	M	35	Postgraduate	15	120
34	Military	M	40	Bachelor	20	120
35	Military	M	37	Bachelor	17	180+
36	Education	F	38	Postgraduate	15	180+
37	Office	F	38	Colleges	12	180+
38	Leadership	M	30	Bachelor	5	150

8.3.2 Case studies to validate the risk equation

The following case studies are drawn from individuals who participated in the experimental phase to assess how well our formula 7.1 developed and covered in the previous chapter performed. Further, this is to evaluate our first metric, 'risk'. Examples of our two most important study variables—job positions and age—will be given.

Case studies on the job role risk

The first scenario is for a 29-year-old employee, with a bachelor's degree and seven years of experience, working in *office and administrative* responsibilities for one of Kuwait's well-known organisations. He claimed that he used social media for about two hours every day. Based on the equation developed, I may argue that his risk is calculated as follows:

$$\text{Risk} = (\text{JR} \times 0.4) + (\text{A} \times 0.3) + (\text{G} \times 0.0) + (\text{ES} \times 0.0) + (\text{YS} \times 0.0) + (\text{TS} \times 0.0) = 7/10$$

According to the results of the risk formula, he is at a *high risk*. To validate the equation, I compared the results of the formula's computation with the results of his test (risk assessment), I discovered that he poses a threat because of his lower awareness score (11 out of 25).

Another example is a 40-year-old woman working in the *education and training* sector who has 15 years of experience and a postgraduate degree. She uses social media more than three hours a day on average. Using this data, I calculated her estimated risk in the following manner:

$$\text{Risk} = (\text{JR} \times 0.4) + (\text{A} \times 0.1) + (\text{G} \times 0.1) + (\text{ES} \times 0.0) + (\text{YS} \times 0.2) + (\text{TS} \times 0.5) = 7.5/10$$

Since the formula calculated that she is at *high risk*, I compared this result to the results of her awareness test and discovered that she had a lower awareness score as well (14 out of 20).

For the purpose of this study, these two examples were chosen to verify how crucial it is

to take job roles into account while creating and prioritizing the training session for social media cybersecurity.

Case studies on age risk

In order to further illustrate the importance of taking age into account while developing and implementing social media cybersecurity training, another two examples will be given. The first one is for a man over *55 years old* working in the education and training sector who spends over three hours a day on social media, has a postgraduate degree and more than 25 years of experience. Using our formula, I calculated his risk as follows:

$$\mathtt{Risk} = (\mathsf{JR} \times 0.3) + (\mathsf{A} \times 0.3) + (\mathsf{G} \times 0.0) + (\mathsf{ES} \times 0.0) + (\mathsf{YS} \times 0.05) + (\mathsf{TS} \times 0.05) = 7/10$$

His formula calculation indicates that he is at a high risk, and to verify this finding, I compared it to the results of a risk assessment test, where he received a lower rating (7 out of 25).

The second scenario involves a *33-year-old* man who works in office and administrative positions for one company in Kuwait, has five years of experience, a secondary degree, and spends, on average, two hours each day on social media. According to our formula, his risk is calculated as follows:

$$\mathtt{HumanRisk} = (\mathsf{JR} \times 0.4) + (\mathsf{A} \times 0.3) + (\mathsf{G} \times 0.0) + (\mathsf{ES} \times 0.1) + (\mathsf{YS} \times 0.02) + (\mathsf{TS} \times 0.0) = 8.2/10$$

He is at a *high risk* and needs to be given priority for the training, according to the results mentioned above. By comparing this score to the results of his awareness test (11 out of 20), I was able to confirm that he was posing a threat to his company because of using social media.

8.3.3 Case studies to validate the framework's methodology

Validation Process

Some researchers argue that training effectiveness can be evaluated only through partici-

pants/trainees (Holgado Tello et al., 2006; Velada & Caetano, 2007; Hamtini, 2008).

The validation process of our framework involves several stages as shown below (Figure 8.2).

Step 1: involves collecting information about participants such as their backgrounds, training preferences, and testing them accordingly, (Identification and risk assessment)

Step 2: this involves evaluating the risks associated when participants interact through social media (Analyzing).

Step 3: involves segregating applicants into two groups, one group will receive customized training and the other group will receive standard training (Design and Implement training).

Step 4: involves evaluating the risks after the training of participants is over (Analyzing).

Step 5: Those who had customized training will be split into two groups. The first group will be granted follow-up training, but the other group will not get any follow-up training.

Step 6: Everyone who participated in the study will be tested again in *two months* to see if their behavior has changed. For a flowchart of the process, see Figure.8.2.

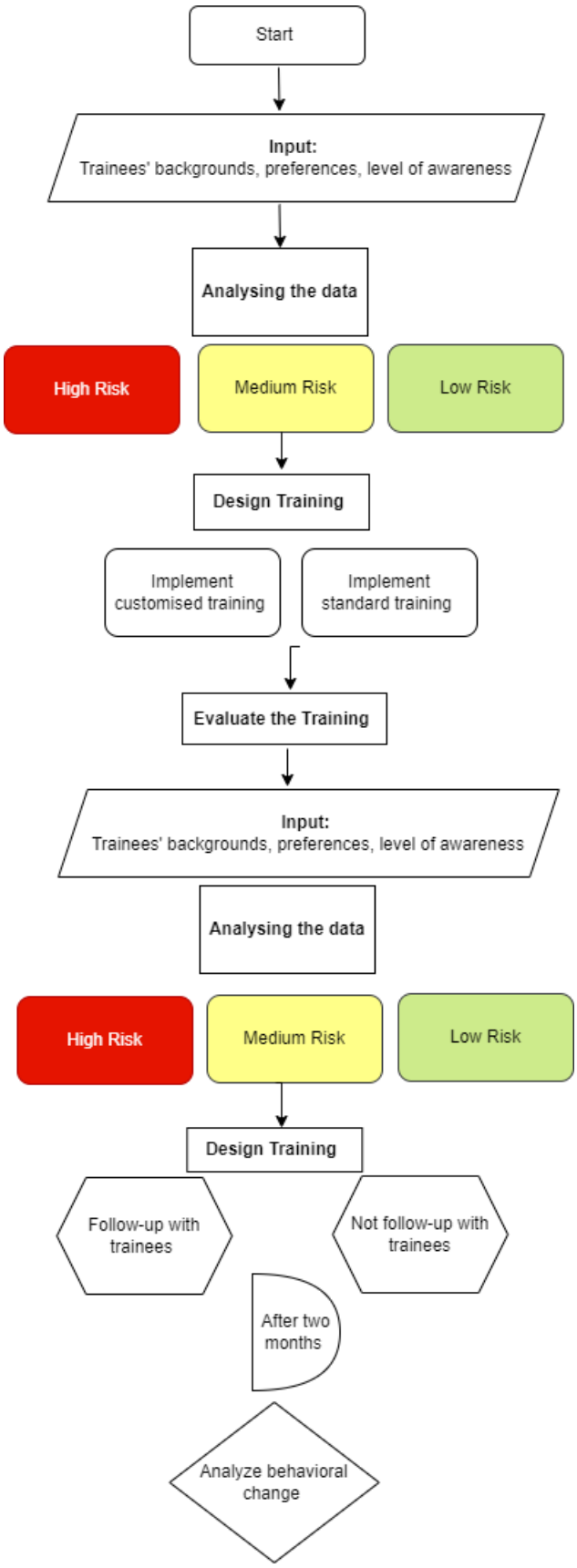


Figure 8.2: Flowchart of the validation process

8.3.4 Kirkpatrick Model

While several methodologies can be used for evaluation (Ostroff, 1991), I have focused on Kirkpatrick's model of evaluation because it helps explore the behavioral outcomes of the participants. This model not only helps assess participants' satisfaction levels (Kirkpatrick, 1978; Holgado Tello et al., 2006) but also evaluates outcomes of the training programme at four levels: reaction, learning, behavior, and results.

The two most standard measures for training effectiveness are trainee reactions and learning (Velada & Caetano, 2007). However, in this project, our focus is on the four aspects for the evaluation of the training outcomes, as seen in Figure 8.3.

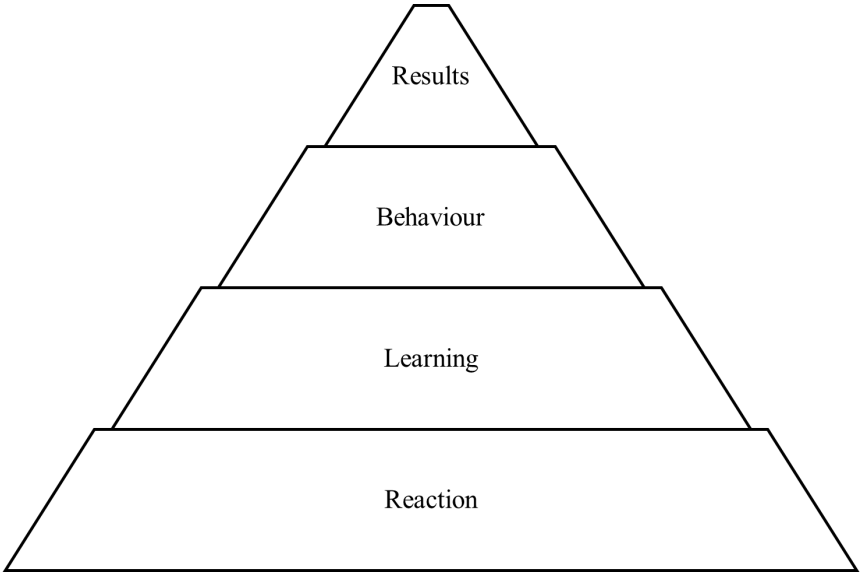


Figure 8.3: Kirkpatrick evaluation model (Kirkpatrick, 1978)

While trainers usually follow the model by first measuring the reaction and then ending at the results, Wang et al. (2018) study states that a better method to measure training effectiveness is to perform the reverse. So, to say, they recommended beginning with the last level 'Results', and then working backward towards the last level for achieving desired results. Following this approach, the focus is on developing a training programme that matches trainees' needs, preferences, and level of knowledge, followed by measuring the other levels of the Kirkpatrick evaluation model.

The *t-test* is employed for level two 'Learning' to find out if the training has achieved its purpose. As European Network and Information Security Agency (ENISA) (2019) suggests quantifying the efforts by using the same measures and metrics before and after

the process, the test leads to statistical proof that the variance of the means is some tangible figure (Schürmann et al., 2020).

However, the first level 'Reaction' will be tested with different questions at the end of the training to know if the trainees have found the training meaningful. It is to be noted here that all the questions were designed with an aim to get reaction/feedback as well as learning levels of participants following Kirkpatrick's model Figure 8.3. All participants were retested after two months of training to assess if there is a significant change in their 'behaviors'.

To meet our study's major objective, the participants have been split into two groups. In one group, 24 members were offered customized training, leaving 14 of the 38 participants to provide standard training Figure 8.4 for more clarification.

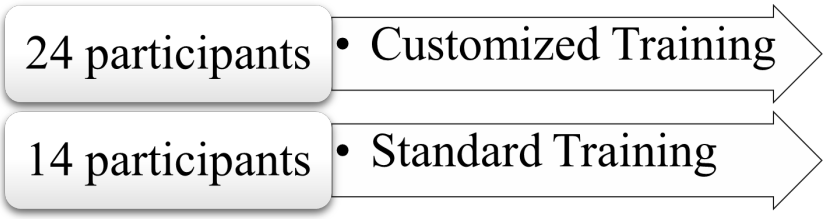


Figure 8.4: Participants' classification

Customised training

Taking into account the needs and interests of the participants, a total of 24 training sessions were designed. Based on the assessment (as described in the previous chapter), trainees' needs, and preferences were identified.

While 11 participants preferred to attend the training sessions in person, 12 participants zeroed on videos to learn new things and improve their skills. Only one participant preferred to get information from posters. Accordingly (as shown in Table 8.2 below), 11 virtual training sessions were designed for those who preferred workshops or physical training sessions owing to the restrictions imposed by the COVID-19 pandemic. The virtual training sessions were conducted via Zoom software, and other training methods such as videos and posters.

While introducing the study's objectives, the trainer sought honest feedback on the training, which will in turn help enhance the training system/programme whether virtual or recorded on video. The outcomes of the customized training sessions can be viewed in

Table 8.2 below.

Table 8.2: Participants in customized training

ID	Training Preferences	Training Received	Pre-training results	Post-training results
1	Online + presentations + videos	Video	21/25	24/25
2	Workshops + Online training	Virtual	7/25	18/25
3	Online training	Online	13/25	25/25
4	Video + Short presentation	Video	14/20	19/20
5	Online + Video + Presentations	Video	12/20	17/20
6	Video + Presentation	Video	11/25	17/25
7	Workshops	Virtual	11/15	15/15
8	Online + Posters + Tip-sheets	Video	20/25	24/25
9	Workshops + Online + Videos	Virtual	11/20	18/20
10	Workshops + Posters	Virtual	11/20	17/20
11	Video + Games	Video	12/20	20/20
12	Workshops + Video + Presentation	Virtual	16/25	23/25
13	Video +Presentations + Games	Video	7/15	12/15
14	Workshops	Virtual	14/25	23/25
15	Videos	Video	5/15	15/15
16	Short presentations + Videos	Video	10/20	17/20
17	Video + Posters + Presentations	Video	6/15	14/15
18	Online +Video + Presentations	Video	11/20	20/20
19	Workshops + Posters + Presentations	Virtual	14/20	20/20
20	Workshops + Posters + Presentations	Virtual	11/20	19/20
21	Workshops + Online + Games	Virtual	14/20	19/20
22	Workshops + Online + Posters	Virtual	14/20	19/20
23	Online + Presentations + Games	Video	12/25	17/25
24	Posters + Phishing tests + Games	Posters	23/25	25/25

To compare the means of the two groups, a statistical test called the *t-test* has been performed (Kim, 2015). The confidence interval has been set to 95% and 99% respectively for these two groups. It means that p-values between 0.05 and 0.01 have to be considered statistically significant.

The *t-test* results demonstrate that the intervention (training sessions) has a *significant* impact on the score outcomes. The post-training overall score is, on average, greater than the pre-training overall score (Mean= -6.542) with a p-value of .000.

It can be stated that after organizing training sessions according to participants' requirements, preferences, and perceptions, their knowledge base has increased dramatically (as shown in Figure 8.5).

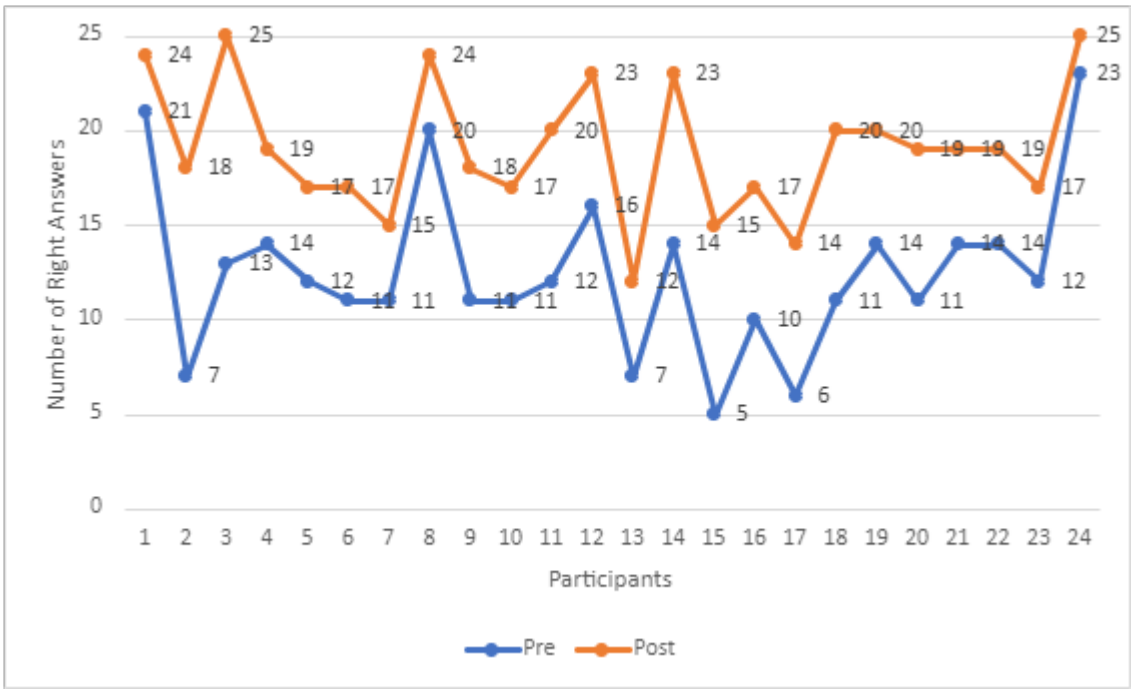


Figure 8.5: Customized training

Standards training

As was already said, the 14 people in the other group got standard cybersecurity training that did not consider their preferences, needs, or anything else that was part of this study. The results both before and after the training programmes have been tabulated here below (Table 8.3).

Table 8.3: Participants in standard training

ID	Training Preferences	Training Received	Pre-training results	Post-training results
1	Posters + Presentations + Flyers	Video	8/20	16/20
2	Videos + Phishing tests + Emails	Posters	12/15	12/15
3	Online + Videos + Posters + Emails	Tip-sheet	15/20	15/20
4	Social media posts	Tip-sheet	11/15	11/15
5	Workshops	Video	4/15	3/15
6	Workshops +Online + Phishing tests	Video	16/20	13/20
7	Presentations + Videos + Posts	Tip-sheet	13/20	17/20
8	Workshops	Video	3/20	6/20
9	Videos + Games + Posts	Tip-sheet	12/15	12/15
10	Social media posts	Tip-sheet	9/20	10/20
11	Online training	Tip-sheet	11/15	11/15
12	Workshops +Online +Videos	Tip-sheet	9/25	15/25
13	Games +Posts + Emails	Video	9/20	8/20
14	Social media posts	Tip-sheet	9/15	8/15

However, on examining the outcomes (before and after) of the standard training sessions that 14 participants underwent, it has been discovered that the associations with a p-value (.182) and means (-1.143) are *not statistically significant*. This establishes that standard training is not effective as it has failed to enhance participants' knowledge base as shown in Figure 8.6 below.

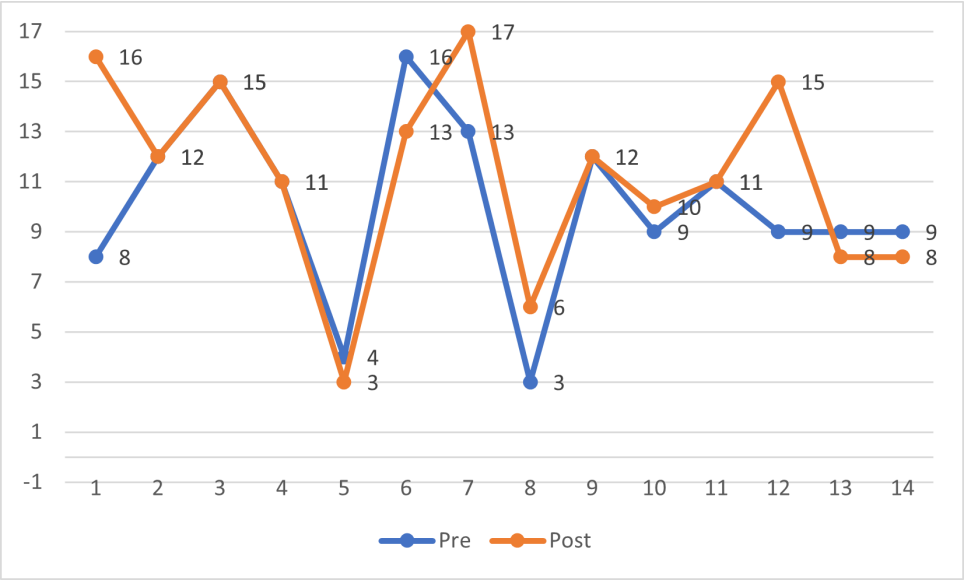


Figure 8.6: Standard training

8.4 Strategy Two: Survey and Interviews

8.4.1 Training Feedback

Training feedback has much to do with trainees' level of adaptability to the training programme including the overall perceived quality of the training sessions. Training feedback is a real predictor of how the training has been effective for trainees (Velada & Caetano, 2007). This also denotes the satisfaction level of the trainees from the training sessions that include the training environment and the trainer's effectiveness in transferring knowledge.

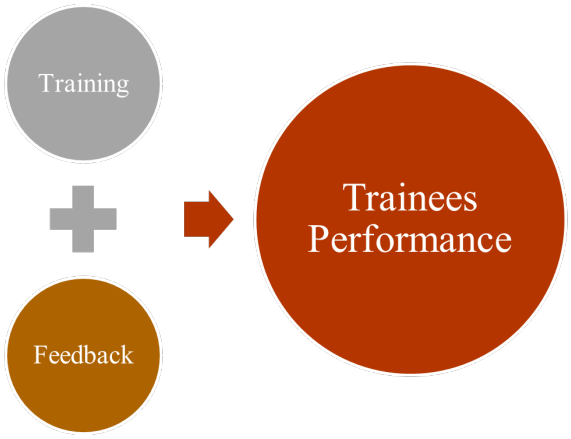


Figure 8.7: Training and feedback (Velada & Caetano, 2007)

Trainer gets feedback in several ways that include trainees' facial expressions, personal comments, and the questions that they raise concerning the subject matter. Essentially, there are two kinds of feedback from trainees: formative feedback, and summative feedback. While formative feedback is received throughout the session, summative feedback is provided at the end of the session (Ertmer et al., 2007). Summative feedback is important because the feedback speaks in totality about the programme (Velada & Caetano, 2007); the feedback helps improve or modify the programme by comprehending trainees' needs (DeFranzo, 2020). Andriotis (2021) emphasizes that the training feedback needs to be analyzed based on some key factors such as engagement, suggestions, comprehension, and effectiveness, and our feedback analysis follows these factors as our ultimate objective is to improve the design, tone, and subject matter of our training programme.

It is strictly ensured that no personal information such as contact number is collected in the feedback form; also, only anonymous feedback forms are accepted from trainee participants as advised by (Ertmer et al., 2007).

Training effectiveness or how the trainees feel about if the training objectives have been fulfilled or can be gauged from the results of the training session. Whether the training content was enticing, clear, and simple to comprehend, and whether the training takes into consideration the trainees' preferred learning styles or not are the crucial factors to make training effective and successful. Quizzes, sharing real-life stories, and presentation through PowerPoint slides with enticing images keep them engaging. While reply to open-ended questions was optional, they can always convey their specific experiences about the training programme that in turn, helps to improve the training programme.

While an online questionnaire needs to be developed to get comprehensive feedback on the training session (Andriotis, 2021), the questions that I posed to the participants for proper feedback are summarized in Table 8.4.

Table 8.4: Feedback survey questions

Element	**Question s**
Effectiveness	1- I am satisfied with the training session. 2- I would recommend this training to others.
Comprehension	3-The training motivates me to pursue more about social media risks
Attractiveness	4- The training session accommodates my learning styles.
Engagement	5- I feel that the training was worth my time.
Suggestions	6- What did you like the most about the training session? 7- What can be improved?

8.4.2 Likert Scale

A Likert scale, one of the most elementary and frequently used psychometric instruments in educational, social sciences, and other research, is the instrument used to collect participants' feedback. The Likert scale has been employed because it focuses on some complex issues such as validity, reliability, and scale analysis (Joshi et al., 2015).

Participants are asked to assess different aspects of the training and match their agreement with a statement regarding the session using a scale of 1 to 5, with 1 indicating strong disagreement and 5 indicating strong agreement followed by two optional open-ended questions to reply to (as shown in Figure 8.8 below).

Figure 8.8: Scale used in the feedback-survey

8.4.3 Likert Scale Reliability

When utilising Likert-type scales, the internal consistency and reliability must be assessed using the Cronbach's alpha coefficient, which must be calculated and reported. This refers to how well-coordinated an instrument's components are with one another and with the instrument as a whole. The initial test's Cronbach's alphas ranged from 0.76 to 0.90 (Croasmun & Ostrom, 2011). With a Cronbach's alpha of 0.99, this study's internal

consistency was *quite high*.

8.4.4 Survey and Interview Results

This largely collects the information from trainees before, during, and after the training session. The key objective is to verify the methodology being followed and the goals that are intended for our proposed framework, ACST-SM including its adaptation for organisations. The results of the survey for both groups — customized training and standard training have been presented in the section that follows.

Customized Training Feedback

As previously indicated participants in this research have been divided into two groups (customized training and standard training groups) essentially to explore if customized training can meet our objectives.

The majority of the participants who have taken customized training are positive towards the training programme. Nearly 96% of the participants stated that the training has motivated them to learn more about the risks of social media including various tools that keep them secure. Moreover, they also showed their eagerness to educate others. Overall, they were found to be satisfied with the training programme.

The open-ended questions serve the purpose of creating qualitative data set for the validation of the study's framework; this helps to have more insight into trainees' perceptions and views. The question reads: *"What did you like the most about the training session?"*

Through the interview process, a variety of responses were received; they can be listed as the following: "I enjoy how obvious and straightforward the subject is!" Another participant said, "I like the way the instructor explains the material so anyone can understand it even if they have no expertise in IT," another interviewee stated, "Information was provided simply and directly." One participant stated, "Explaining my typical mistakes and teaching me to adopt best practices were the key strengths of the session." Another participant said, "I preferred the fact that the training was tailored to my need rather than being generic". Another person replied, "It was exceptional for me," in support of their claim.

When the trainer/specialist is an expert in the field, it provides added confidence to trainees. "I can feel the presenters' high level of knowledge", as one of the interviewers

put it. "The trainer was extremely friendly and kind" is another additional comment with that. "The trainer was not only well organized but also properly addressed my difficulty," another participant stated. One person proposed uploading those videos to YouTube so that anyone can access them as and when required. This amply indicates that he supports the instructor's teaching style. "The trainer's manner is fascinating and enticing, and the content has a scientific basis in simple terms", according to one of the interviewees from the academic field. One lady participant said: "Everything was perfect, the session was helpful, enjoyable, and very enlightening".

Standardized Training Feedback

This section focuses on those participants who obtained standardized training or one-size-fits-all training. The feedback was collected through an online survey that included open-ended questions so that participants could elicit their thoughts and ideas; direct engagement (quick chat) was also a part of this.

It is important to notice that those who received standard training left the majority of the open questions unanswered. Their recommendations regarding the training can be listed as the following: "More images and infographics are needed"; "videos' screenshots needed to be improved"; "Quiz questions need to be asked unambiguously." Some of them suggested adding screen images of the steps to make them more understandable.

From the participants receiving standard training, two of the 14 participants admitted that they did not review the training at all; one of them said, "To be honest, I didn't see the posters!" This woman received a poster through email, but she preferred videos and phishing tests instead. On questioning her about this, she stated, "I detest reading posters". One of the participants gave a casual look at videos sent to him because he preferred workshops as a method of instruction.

In short, a significant difference was noticed between those who received customized training and those who received standard training in terms of feelings and adaptability. Those who received customized training exhibited a sense of satisfaction and awe towards the training programme. At the same time, the participants from the other group (who received standard training) appeared more like casual learners – as if they were doing a favor to the trainer by participating in the programme.

8.4.5 Behavior

Diamantidis & Chatzoglou (2014) argue that people's behavior can be gauged from the fact of how much they apply the learning they have gained from the training programme. The key objective of any training programme is to transfer learning to the participants; therefore, post-training behavior becomes important (Hamtini, 2008). While transforming trainees' behavior is the responsibility of the trainers, they need to choose the right approaches for their success.Galanou & Priporas (2009) argue that the effectiveness of the training programme needs to be ensured through the behavioral changes of trainees. However, if the trainees behave positively in the training session does not become a guarantee that they will implement the same in their job (Velada & Caetano, 2007).

The purpose of the quiz in this study is to understand people's behavior and attitudes toward social media. The mention of "Compliance" in the previous chapter as a second metric, refers to whether or not trainees comply with the policies conveyed to them. For example, in pre-assessment, a question is asked if they are turning the TFA feature on social media accounts with a follow-up question to give reasons if they are not. In the post-assessment if they have begun turning TFA on then as per Laker (1990) this can be called 'near transformation' and success of the training programme. Usually, this kind of approach is more suitable for technical training where specific knowledge needs to be applied after the learning is complete.

In this experimental study, three participants selected the "I don't know" option when asked whether they have the TFA enabled on their social networking profiles, while seven others said they do not. The table below demonstrates how their behavior changed as a result of the training they received (noting that these participants are from the customized training category).

Table 8.5: TFA enabling

ID	Pre-training	Post-training
Have you enabled the two-factor authentication feature on your SM accounts yet?		
1	I don't know	Yes
2	I don't know	Yes
3	No	Yes
4	No	Yes
5	No	Yes
6	I don't know	Yes
7	No	Yes
8	I don't know	Yes
9	No	No
10	No	No

When participants select no, they are asked an open-ended question to justify their stand. One of the participants replied, "My social media accounts are not that important." Many of the participants were ignorant of this feature and replied, "I just forgot about it"; "I am not sure how to use it", and "I don't think about it." One of the participants viewed TFA to be a programme and not a feature that was automatically turned on with every social network account. Someone indicated that too by saying, "I need to learn more about the application before utilizing it".

Sookhai & Budworth (2010) define 'self-efficacy' as the factor that employees feel exuberant about applying what they have learned in the training session for protecting themselves and the resources of the company in which they are working.By improving training effectiveness, learners' self-efficacy enhanced (Sookhai & Budworth, 2010),and that will inspire confidence in their capacity to do the mission (Chiaburu & Marinova, 2005).

To assess the 'self-efficacy' factor, it is crucial to evaluate the outcomes of a training session once again after a lapse of some time. Several researchers (Hamtini, 2008; Diamantidis & Chatzoglou, 2014; European Network and Information Security Agency (ENISA), 2019) endorse this procedure. Accordingly, I decided to test the behavioral changes of trainees after two months of completing the training session. For this, I split the participants into two groups of 12 participants each. One group continued with weekly training updates

through posters, emails, short videos, and social media posts. The other group was not kept updated after the initial training. After approximately two months, the participants from both groups were invited to take the same quiz. Of these 24 participants, only 20 were available to take a quiz. The below-mentioned table describes the results from both groups.

Table 8.6: Behavioral change analysis

ID	Quiz result	After 2months	ID	Quiz result	After 2 months
	Follow-up group			**Non-follow-up group**	
1	24	24.5	1	19	14
2	18	18.5	2	17	11
3	17.5	21	3	17	13
4	15	14	4	20	18
5	17	18	5	20	17
6	18	16	6	19	11
7	17	19.5	7	23	18
8	15	15	8	19	18
9	23	20	9	19.5	17
10	14	13	10	25	23.5

As discussed previously, the p-values between 0.05 and 0.01 are statistically significant. However, with p-value (.876) and mean -.1, it is revealed that there is no significant correlation between the initial assessment and the results of the assessment two months after the training. This also informs that by keeping in touch with the participants and updating them regularly, participants' behavior remained stable (as shown in Figure 8.9 below).

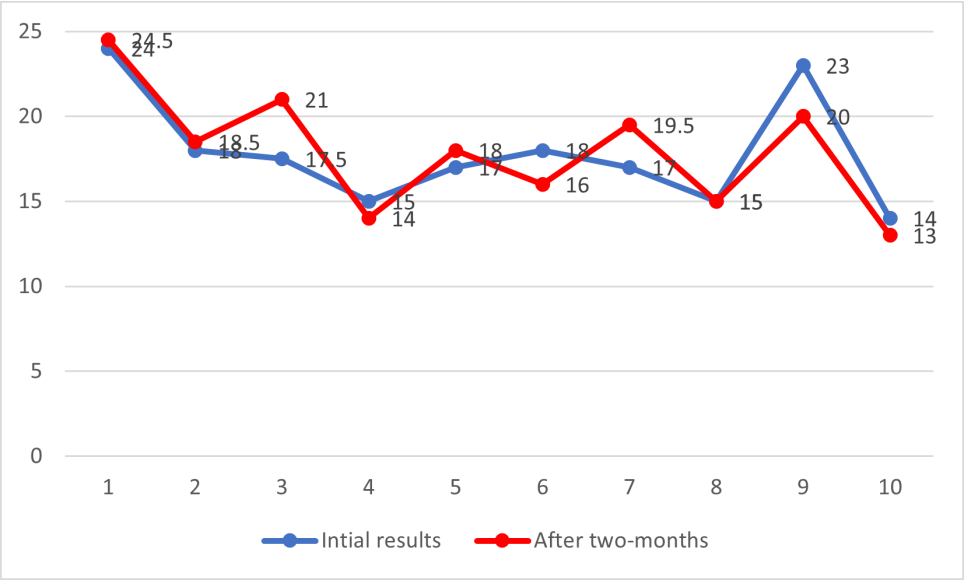


Figure 8.9: Behavior analysis (follow-up group)

However, the participants from the second group who were *not* updated after the initial training had a big impact on their score- *dropped down*- when tested again after two months (mean = 3.8) on average, and p-value =.000 (see Figure 8.10 for more clarification).

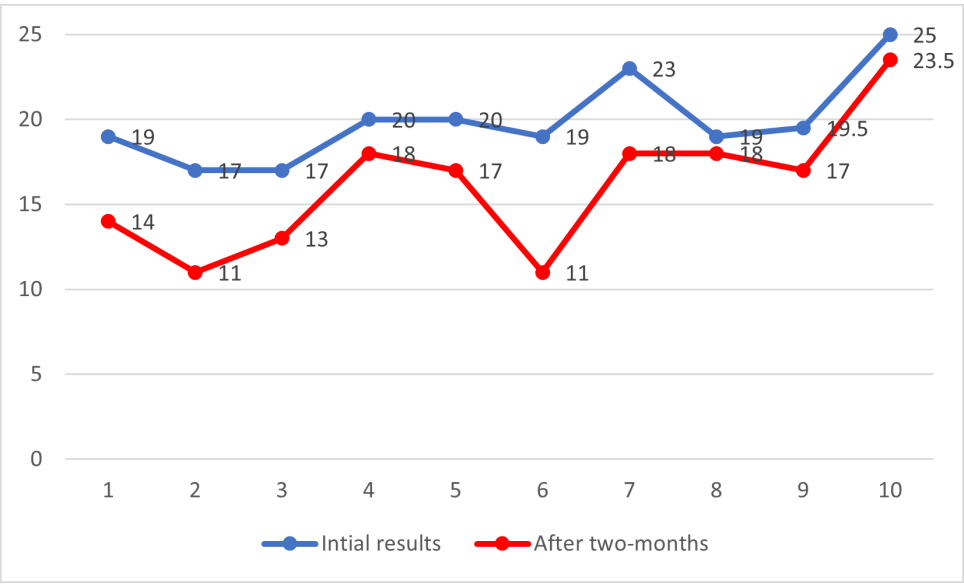


Figure 8.10: Behavior analysis (non-follow-up group)

On comparing the findings of these two groups of trainees it can be construed that it is crucial to keep people updated and informed throughout by utilizing a variety of training methods so that they remain safe and secured.

The methods employed in this study to analyze participants' behaviors are summarized

in Table 8.7 below.

Table 8.7: Behavioral analysis approaches

	Approach name	**Author (s)**	**How used in this study?**
1	Near transfer	Laker (1990)	Pre & Post quiz results
2	Self-efficacy	Sookhai and Budworth (2010)	Monitoring, feedback results, and interviewing
3	Continuous observation	Kirkpatric (2008)	Participants were tested again 2-months after their training.

8.5 Enhancements and Changes Suggested

The validation of the framework involves having feedback from participants by asking them some open-ended questions as qualitative inputs. All participants faced the following question:

'What could be improved?'

One of the participants opined that the quiz could be improved by quantifying the degree of uncertainty attached to each response. Another participant wanted the survey assessment should display the correct response immediately explaining why this response turned false. “This will not only save the considerable time of the participant as well as the trainer but also increase the user awareness at the same time," commented the same participant.

Another participant who chooses videos as her preferred method of instruction states, “Videos should demonstrate how to develop a safe cyberculture that makes one not a victim but a hero.” She was interested in a professional video clip to enhance her cyber awareness. Many participants preferred to have more screenshots, images, and graphs to have more clarity on the subject. A large proportion of the participants, especially those who received customized training, commented on the training positively as is evident from their responses: "It was perfect," "Everything was great," "All good, no need for more," and "It was suitable for me!"

In the first paper, we had an opportunity to discuss how organisations around the world can benefit from this. At that time, we had included data and statistics for the state of

Kuwait to demonstrate that this framework methodology could be applies to all organisations.

8.6 ACSTF-SM Revision

The validation process discussed above has been created to examine if the designed framework can be used in organisations for all types of employees with different roles, gender, age, educational level, expertise, and attitude.

Our survey, interviews, and case studies with participants demonstrate that employees prefer customized training over standard training because they find customized training adaptive in nature meeting their needs, preferences, and perception, which emphasizes the first domain in our framework called human factor in cybersecurity.

Those who prefer videos for learning seek more advanced video clips that can update them regularly. In addition, trainees prefer a brief awareness film or a recorded video for instructions. Moreover, the suggestions made by the participants allow me to modify the format of the evaluation questions for individuals who prefer reading for training. Those who select tip sheets, emails, posters, or postings respond to their assessment straight away. They need to be provided with additional techniques in follow-up in subsequent times.

Going ahead, the second stage of our framework, "risk assessment," will be different for different participants. They will be segregated into two kinds. Those preferring reading approaches such as "emails, posters, tip-sheets, etc." will have a different kind of test than those who prefer workshops, videos, online, etc., as their preferred training approach. For further explanation, individuals who would rather read than watch or practice will receive a test that explains why their answers are incorrect as soon as they turn in their test, simply because reading makes them feel more adaptive.

The third stage of our suggested approach, "risk analysis," will remain the same emphasizing the significance of taking into account job roles, age, other human characteristics, user behavior and social media attitudes as addressed in earlier chapters. Risk analysis, in this study, reveals that not all people have the same level of comprehension, and awareness in safeguarding themselves and their organisations.

"Social media best practices" is the fourth domain of our framework which needs to be

viewed as a dynamic element for our participants to follow. For example, one of the Instagram questions was: *After making your account private, what can you do to prevent your followers from seeing your posts?* The usual answer to that is to *block* them, but Instagram recently has improved a feature that allows users to *remove* participants. The point is that social media best practices keep on updating themselves time-to-time. In short, the validation process emphasizes regularly reviewing training sessions by receiving feedback from participants.

8.7 Chapter Conclusion

Since validation is an important procedure for any work to be adopted, our suggested framework is subjected to scrutiny in a variety of ways for its effectiveness. Several validation methods have been adopted that include case studies, surveys and interviews, and the presentation of scholarly papers to experts for their comments on the subject. Kirkpatrick's evaluation model has been employed for measuring the four aspects such as results, behavior, learning, and reaction of participants.

To assess the effectiveness of the risk equation proposed in this research, four scenarios from individuals who took part in the experimental phase were chosen as case studies: two to emphasize the significance of job role as the primary risk and two to show age risk. By contrasting the formula score with the outcome of the initial awareness test, this verification was carried out.

To understand the effectiveness of customized training, participants were split into two groups. The first group was offered customized training while the second group was offered standard training. The customized training takes into account each participant's needs, preferences, perceptions, and degree of knowledge. Results were compared by using the *t-test* before and after the training, which demonstrates that customized training had superior outcomes in comparison to standard training.

Participants' feedback was collected by administering survey questions. While a Likert scale was used in the questionnaire to have feedback from participants, the participants were also served open-ended questions at the end for getting qualitative feedback on the training programme. The results so obtained establish that the ACST-SM framework for training is dependable when it comes to mitigating social media risks in organisations.

It has been demonstrated here that I can examine and analyze the variations between different groups by creating hypothetical case studies and putting into practice various training scenarios.

Obviously, people have different preferences for social media cybersecurity training, varying degrees of awareness and expertise in this area, and different perceptions and attitudes, and all of this needs to be taken into account for developing an effective training programme.

Chapter 9

Conclusion and Future Work

This chapter analyses the research findings and provides responses to the nine research questions, which would eventually help formulate an adaptive cybersecurity training system to mitigate social media risks in organisations. Before concluding, the chapter also attempts to highlight the likely challenges and opportunities that lie ahead for additional work.

9.1 Introduction

As mentioned in the introductory Chapter 1, the major objective of this study is to explore how and why adaptive social media cybersecurity training programme can raise employee's awareness within an organisation. The literature review, as discussed in Chapter 2, reveals that there are technical and nontechnical ways to reduce or eliminate social media risks. While technology attempts to thwart cyber-attacks by incorporating certain technological means, nontechnical methods include training programmes, policy settings, risk management, and campaigns were used to raise social media cybersecurity awareness among employees.

An approach called mixed methodology – referred to as a quantitative and qualitative research strategy (Chapter 3) has been employed. Google form was used to run a web survey, which has helped to get a response for our questions 1,2 and 4. In addition, certain subject matter experts are interviewed who are either involved as formulators of cybersecurity training in various organisations or policymakers in various organisations in the state of Kuwait. Many of them have had the experience of conducting cybersecurity

training previously, which has enabled me to respond to study question no.3. In all, 641 participants and 25 stakeholders participated in this survey.

I carried up 38 case studies on employees from various roles and backgrounds in Kuwaiti organisations in order to validate the framework processes and the novel risk equation developed based on this preliminary data. As a result, this assists me in addressing our last-remaining project-related questions.

9.2 Summary of research questions and findings

9.2.1 RQ1: What differences exist between trainees' preferences for cybersecurity training?

The data in this study indicated that trainees' preferences for cybersecurity training vary widely and significantly. These preferences have been discussed in chapter 4 in detail. However, to summarize, the job roles or responsibilities of the participants lead to different preferences for training. This has also been endorsed in the studies completed by various researchers (Alshaikh et al., 2018; Schürmann et al., 2020; Zhang et al., 2021; Ki-Aries & Faily, 2017). While people involved in financial and business functions consider webinars more realistic ways of training, people working with education sectors show their inclination towards workshops or in-class instruction. Contrary to this, people in leadership or managerial roles do not seem to enjoy classes in person. Even they do not have any preference for phishing or mock tests for learning. They rather prefer tip sheets and instructions sent to them through emails, which they can learn in their privacy. At the same time, learning through email attachments is not preferred by people in military such as police and army.

Storytelling is the preferred method for those who work in arts, sports, and entertainment fields. While healthcare workers prefer raising their awareness through social media, people in office and administrative jobs do not consider this tool appropriate. Gaming is largely a preferred method for raising cybersecurity awareness; however, people in leadership roles and military personnel do not see gaming as an appropriate way for cybersecurity learning.

As per the research, preferences differ based on gender as well as job roles, but to a lesser extent. The information reveals that women prefer emails, webinars, gaming, posters, and

online cybersecurity training. Additionally, male trainees support mock attack/ phishing tests as their training method.

Training preferences also differ according to the age of participants. While posters are the preferred way of learning by the 46–55 age group, the people in the 18–26 age group have been found to prefer the storytelling method. The length of experience exerts influence on people's preferences on training methods. People with 15-20 years of work experience place the greatest importance on workshops and in-person instructions; however, people with 10-15 years of expertise prefer online training methods including gaming over workshops and webinars. The people with lesser experience (2-5 years) prefer webinars as well as posters as training tools. New hires prefer learning through 'mock cyber attacks' but that does not stand true for the people with 5-15 years of experience. The educational level of participants also play a role in deciding people's cybersecurity training; the same has been described in detail in Chapter 4.

9.2.2 RQ2: What factors encourage adaptive cybersecurity training?

A close interaction between trainers and trainees is crucial for developing adaptive cybersecurity training for participants. In addition, the content of the training is extremely crucial in designing an adaptive training session for trainees. Experts recommend using case studies, assignments, quizzes, and stories for effective learning; the same has also been endorsed by numerous researchers in the past (European Union Agency for Cybersecurity, 2014; Alshaikh et al., 2018; Chowdhury & Gkioulos, 2021; Schreuders & Butterfield, 2016). The point is that cybersecurity training needs to be free from jargon as also expressed by other studies (Ghafir et al., 2018; Bada & Nurse, 2019).

Trainees feel more adaptive with customized training over a one-size-fits-all kind of strategy, which is consistent with the studies of other researchers (Glaspie & Karwowski, 2017; Bada & Nurse, 2019; Haeussinger & Kranz, 2017; Aldawood & Skinner, 2019; Pattinson et al., 2018; Gasiba et al., 2021; George et al., 2020; Alshaikh et al., 2018; Furnell & Vasileiou, 2017; Zhang et al., 2021). Customized training that includes preferences of people based on their job roles and levels of knowledge can significantly work towards developing adaptive training for participants. Interestingly, it has been discovered that women prefer customized training instead of a one-fits-all approach to training more than men.

The training environment is another crucial factor in making training effective. Length

of training and timing are the other factors to make it successful. People with higher education have been found to give more importance to the training environment. People in the age group of 26-45 and those with higher education have shown an inclination towards an amiable training environment. Some other research studies also endorse a similar viewpoint on the training environment (Chowdhury & Gkioulos, 2021; Al-Daeef et al., 2017).

As usual, trainers themselves are the backbone of any training process. It is the trainer who engages the audience fully and makes their participation meaningful. Trainer occupies a central position in the process of developing adaptive training system. Several other research studies endorse a similar viewpoint (Brilingaitė et al., 2020; European Network and Information Security Agency (ENISA), 2012; Stockhardt et al., 2016; Antonaci et al., 2017; Safa et al., 2016; Taniuchi et al., 2018; Javidi et al., 2019). Moreover, the findings of Demek et al. (2018) are in line with me in that trainer must maintain participants' attention throughout the training session in order for it to be effective.

9.2.3 RQ3: What elements affect an employee's potential level of risk when using social media?

The findings of this study reveal that human behaviors and characteristics play a significant role in understanding the risk involved when they use social media. Individuals' level of security awareness depends much on their employment roles and responsibilities, which is consistent with the findings listed in Toth & Klein (2014). For example, people working in administrative offices are more susceptible to phishing attacks. People using public Wi-Fi networks are less likely to follow social media security policies. People involved in management and leadership functions need more intensive training than others to safeguard themselves from cyber-attacks. People working in education fields do not bother to update their anti-virus software resulting in security violations. Often, they fail to make their credentials secured. These findings are also supported by Hadlington (2018). The people working in business and finance-related fields do not care to install anti-virus software and fail to verify the legitimacy of URLs before acting with them. No surprise that they become the target of cyber-attacks, which corresponds well with the findings of (Pedley et al., 2020).

I found that healthcare workers suffer due to spam emails and messages, which is also

supported by (Nifakos et al., 2021). This is not the case with the people involved in IT-related fields – endorsed in the study done by Gasiba et al. (2021).

The findings highlight age as another aspect that this study has discovered. According to this study, employees under the age of 35 and those over the age of 55 are more at risk for cyber-attacks. The findings assert that younger users are more likely to be the victims of cyber-attacks when compared with older users, which is in line with Hadlington (2018); George et al. (2020) findings. Moreover, I found that those old users who exceeded 55 years old require more cybersecurity training than younger individuals, which is corresponds well to Saridakis et al. (2016); Blackwood-Brown et al. (2021) findings.

Gender itself plays a role in cybersecurity safeguards. Women are found to be more prone to cyber-attacks in comparison to men; several other studies also endorse the same (Jagatic et al., 2007; Venter et al., 2019; Parker & Flowerday, 2020; Akbari Koochaksaraee, 2019). That is perhaps so because women care less about building strong passwords and protecting them; often, they have been found to struggle with email spam and phishing activities. Educational level also plays an important role in protecting people from cyber-attacks.

The number of hours people are involved with social media has an impact on social media awareness. For example, the findings provide evidence that people who use social media for less than 30 minutes a day are more prone to cyber-attacks because they have little understanding of security concepts. Moreover, those who use social media for more than three hours a day are found to be at greater risk; often, they are found to be using Wi-Fi in public areas; the findings are supported by Van Schaik et al. (2018). This information allows me to develop a novel equation 7.1 known as the *Social Media Risk Assessment Equation*, which was covered in detail in Chapter 7.

9.2.4 RQ4: What challenges do cybersecurity formulators, trainers, and policymakers encounter in their work?

Previous research, such as (Bennett & Manoharan, 2017; Chen et al., 2016; Stoessel, 2016), have shown the importance of having SMPs in place. However, the study found that trainers, cybersecurity training formulators and policymakers encounter several challenges with this task. First of all, they need to devise a language, which is free of jargon as non-technical participants may have difficulty comprehending the technical terms, this is

corresponded well to (Wisniewski et al., 2017; Bhatnagar & Pry, 2020; Nyoni & Velempini, 2018) findings, which showed that individuals find SMPs complicated to comprehend. This becomes even more difficult when participants' first language is not English.

Our data shows that policymakers have issues when the management is not encouraging. The rigid mindset of employees poses another challenge in presenting and implementing security policies across. Often, these kinds of employees assume that it is the job of IT specialists to take care of all security issues.

9.2.5 RQ5: What limitations existed in earlier attempts to develop human factors-based adaptive cybersecurity training?

Chapter 6 aims at identifying research gaps and discussing a variety of models and frameworks to arrive at the most suitable framework for this project. The proposed framework by European Network and Information Security Agency (ENISA) (2019) describes the ways to enhance cybersecurity awareness among people, and the same has helped to construct our novel framework. Brilingaitė et al. (2020) emphasize considering job roles as an important element for devising training methods. At the same time, the framework proposed by Dawson (2018) asserts in favor of imparting practical training to participants considering effective policies and practices.

The framework proposed by Aliyu et al. (2020) has helped me to create a web-based framework for use as a cybersecurity assessment and audit tool. The model helped me to segregate trainees as per their awareness levels, which eventually allowed me to impart effective training. Similarly, the framework offered by Alshaikh et al. (2019) in conjunction with the model proposed by Rieff (2018) allowed me to acknowledge the behavior of trainees regarding their awareness levels.

Georgiadou et al. (2022) provides a system to evaluate and analyze employees' security readiness within enterprises. In addition to incorporating human factors, Esparza et al. (2020)' framework aids in the development of self-assessment tools by replicating the elements of cyber hygiene (CH), which is, in their perspective, the primary factor in comprehending cybersecurity challenges.

The works mentioned above take into account human factors responsible for lapses in the field of cybersecurity. Considering frameworks related to cybersecurity risk management has helped me to develop a risk-based framework. While the NIST framework, which

describes the risk management process, makes the security risk assessment procedure simpler, it is the framework by Alshaikh et al. (2019) that describes social media risk estimation in detail.

Even though these models and frameworks taught me a lot, I could not use them in our proposed framework because they needed to be more specific and easier to implement. Because people's demographics, attitudes, and behaviors differ, these older works need to be improved for adaptable cybersecurity training for social media risks.

9.2.6 RQ6: What new techniques have been discovered in this research to build an adaptive cybersecurity training for social media risks in organisations?

The proposed framework is a new technique for developing adaptive cybersecurity training to mitigate social media risks. The framework is used to evaluate an employee's awareness level towards social media risks.

The risk equation developed in this study (equation 7.1) will help policymakers, those developing training materials, and cybersecurity trainers in their work by calculating the level of threat that a particular employee poses while using social media. In other words, this innovative formula will help stakeholders create applicable social media cybersecurity training and prioritize the training for individuals who are at 'high risk'.

Our framework's technique effectively enhanced employee awareness of and adherence to SMPs. The fourth phase, building an adaptive training that considers trainees' needs, perceptions, preferences, and level of knowledge, is the most important phase in our framework strategy, which are, identifying people, assessing them, analyzing those data to categorize and create training priorities and evaluate the effectiveness through many approaches.

This study also demonstrates the importance of keeping stable behavior toward social media best practices by regularly training employees on the most recent information instead of employing a single training technique.

9.2.7 RQ7: What evaluation techniques and approaches are being used to verify the framework's effectiveness?

A variety of ways has been employed to validate the framework. Case studies, online surveys, and interviews with stakeholders have been used to get feedback and validate the framework process. Some data have been published for scientific validation.

The framework techniques and the risk equation were validated using case studies. I compared the results of the risk formula for four participants with their test results in order to confirm it and determine how important it is to take job role and age as the two most critical factors in this study.

The process for validating the framework has multiple steps (Figure 8.2) including gathering data from participants and testing them repeatedly. The Kirkpatrick Model has been used as a basis for the work because it, unlike other models, helps examine the behavioral responses of participants. The Kirkpatrick Model evaluates training programme outcomes at four different levels: reaction, learning, behavior, and results. A variety of statistical analyses including *t-tests* have been conducted to find statistical evidence. Chapter 8 describes the validation process in detail.

9.2.8 RQ8: What recommendations for developing adaptive cybersecurity training in organisations can be derived from the research objectives?

The results of this study have a variety of implications that may be significant for organisations, particularly for those that act as policymakers, trainers, and formulators for cybersecurity training. While most participants look forward to adaptive cybersecurity training (ACST) systems for their learning, organisations need to work towards the same. Following are the recommendations for developing adaptive cybersecurity training in an organisation:

- In addition to job roles, age, educational level, gender, online behavior of people causes a considerable impact on the training that needs to be imparted to them; it is important to recognise the staff accordingly.

- Factors such as customization, training environment, trainer/instructor, and content are crucial for developing an adaptive cybersecurity training system.

• Most participants prefer short training sessions, and this is an important aspect that policymakers and trainers must take into account.

• Management must choose the trainer carefully, keeping in mind the specialty in the field.

• The trainer needs to keep the vocabulary simple and free of jargon so that audience may feel fully engaged.

• Close interaction with the audience is a must for adaptive cybersecurity training. Trainers must find ways to keep the audience involved so that their learning becomes simple and enjoyable.

• The riskiest staff such as finance, business, and administrative personnel need to be trained first because it is necessary to see that organisational assets are not jeopardized. Newbies and people over 55 are more vulnerable to cyber-attacks; therefore, they need to be trained before others. Similarly, training for the people with matriculation or higher secondary education (in contrast to the people with higher education) needs to be prioritized.

• As per the study, women need to receive priority in training since they are more vulnerable to cyber-attacks in comparison to their counterparts.

• Employees who use the internet and social media less frequently and those who use it more than usual (3+ hours a day) are perhaps less familiar with social media cybersecurity issues; therefore, they need to be given priority in training.

9.2.9 RQ9: What are the chances and difficulties for applying the findings to other locations, cultures, or peoples?

This study is based on the people from the State of Kuwait; however, the moot question remains if these findings can be applied to other locations, cultures, or people.

Although I only gathered information from Kuwaiti employees, the conditions of Kuwait allowed me to gain a deep understanding of some of the cybersecurity issues that are present worldwide. Indeed, Kuwait is one of the top five Arab countries in the use of social media (Alansari et al., 2019). Kuwait is also ranked number eight in email malware attacks, and number six in frequency of spam attacks (Cleary et al., 2018). Thus, concentrating on Kuwait's case cannot guarantee that our research has global coverage, but can provide me

with invaluable insight into cybersecurity issues that are present in Arab countries and worldwide too.

Our research involves looking at global findings that have already been collected and analyzed from a large sample of data (641 responses and 25 in-depth interviews) with employees in Kuwaiti organisations with different jobs, experiences, and online behaviors. Further, the fact remains that everyone whether one lives in Kuwait or somewhere else considers his or her privacy and confidentiality extremely important and is always eager to learn about cybersecurity safety issues to safeguard their accounts. However, it needs to be acknowledged that human behaviors vary from culture to culture, and country to country, and that is why the findings of this study may need to be applied cautiously. The Government of Kuwait has enacted its National Cyber Security Strategy, and so is the case with most other countries too. Moreover, demography and educational level differ from country to country, and therefore, people's awareness of cybersecurity issues may also vary. However, the framework's process for adaptive cybersecurity training needs to remain the same.

9.3 Challenges and Opportunities for Future Work

While the study has met many of its objectives, it has limitations too that must be acknowledged.

The fact that people are the weakest link in cybersecurity issues, and their behaviors decide the outcome of any cyber-attacks. That is so because human behavior is unpredictable and that needs to be disciplined through training. Given the different socio-cultural backgrounds of people in different geographies, understanding human behavior about their social media interactions is in itself a challenging task from where all cybersecurity issues emanate. Since technology alone cannot tackle cyber issues, it becomes important to study the target audience intensely before a structured training programme is implemented.

During the experimental phase, time and resource limitations become another challenge while devising a training strategy – whether virtual or online. While this study emphasizes respecting the preferences of people, a fresher or a newcomer cannot have a choice because they are not much acquainted with the subject matter. Future research may focus exclusively on those with previous experience with more than one cybersecurity

training method and find ways to devise why such training is more adaptive than others. While this study can become a basis for all future studies in this field of social media cybersecurity to develop adaptive training for social media users, some recommendations for future studies can be given below.

- Verifying that the proposed framework holds good when applied to organisations in other geographies.

  • Examining the validation methodologies used in this study about other upcoming social media platforms.

  • Examining the significance of the variety of components this study has discovered about different human factors and attitudes such as demographics and time spent on social media.

  • Examining the risk evaluation equation of the framework used here about case studies in organisations in other parts of the world

  • Researching and identifying if any other risk element exists that this study may have missed taking into account, and then incorporating the same formulating an improved equation for estimation of social media risk.

Bibliography

Abdullahi, A. A., & Kaya, M. (2021). A deep learning based method to detect email and sms spams. In *2021 International Conference on Decision Aid Sciences and Application (DASA)*, (pp. 430–435). IEEE.

Ahmad, A., Maynard, S. B., Desouza, K. C., Kotsias, J., Whitty, M. T., & Baskerville, R. L. (2021). How can organizations develop situation awareness for incident response: A case study of management practice. *Computers & Security*, *101*, 102122.

Aïmeur, E., & Schőnfeld, D. (2011). The ultimate invasion of privacy: Identity theft. In *2011 Ninth Annual International Conference on Privacy, Security and Trust*, (pp. 24–31). IEEE.

Akbari Koochaksaraee, A. (2019). *End-user security & privacy behaviour on social media: Exploring posture, proficiency & practice*. Ph.D. thesis, Université d'Ottawa/University of Ottawa.

Al-Daeef, M. M., Basir, N., & Saudi, M. M. (2017). Security awareness training: A review. *Lecture Notes in Engineering and Computer Science*.

Alansari, M. M., Aljazzaf, Z. M., & Sarfraz, M. (2019). On Cyber Crimes and Cyber Security. In *Developments in Information Security and Cybernetic Wars*, (pp. 1–41). IGI Global.

Aldawood, H., & Skinner, G. (2018). Educating and raising awareness on cyber security social engineering: A literature review. In *2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)*, (pp. 62–68). IEEE.

Aldawood, H., & Skinner, G. (2019). Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues. *Future Internet*, *11*(3), 73.

Alenezi, A. (2019). The regional challenges affecting kuwait's national security. *Review of Economics and Political Science*.

Aliyu, A., Maglaras, L., He, Y., Yevseyeva, I., Boiten, E., Cook, A., & Janicke, H. (2020). A holistic cybersecurity maturity assessment framework for higher education institutions in the united kingdom. *Applied Sciences*, *10*(10), 3660.

Alshaikh, M., Maynard, S. B., Ahmad, A., & Chang, S. (2018). An exploratory study of current information security training and awareness practices in organizations. *Proceedings of the 51st Hawaii International Conference on System Sciences*.

Alshaikh, M., Naseer, H., Ahmad, A., & Maynard, S. B. (2019). Toward Sustainable Behaviour Change: An Approach for Cyber Security Education Training and Awareness. In *27th European Conference on Information Systems*, (pp. 1–14). Kista, Sweden.

Ameen, A. K., & Kaya, B. (2018). Spam detection in online social networks by deep learning. In *2018 International Conference on Artificial Intelligence and Data Processing (IDAP)*, (pp. 1–4). IEEE.

Andriotis, N. (2021). Elements to include in any post training evaluation questionnaire. *Retrieved on May 14th*.

Antonaci, A., Klemke, R., Stracke, C. M., Specht, M., Spatafora, M., & Stefanova, K. (2017). Gamification to empower information security education. In *International GamiFIN Conference 2017*, (pp. 32–38).

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender Difference and Employees' Cybersecurity Behaviors. *Computers in Human Behavior*, *69*, 437–443.

Aromataris, E., & Pearson, A. (2014). The systematic review: an overview. *AJN The American Journal of Nursing*, *114*(3), 53–58.

Awan, M. J., Khan, M. A., Ansari, Z. K., Yasin, A., & Shehzad, H. M. F. (2022). Fake profile recognition using big data analytics in social media platforms. *International Journal of Computer Applications in Technology*, *68*(3), 215–222.

Awojana, T., & Chou, T.-S. (2019). Overview of Learning Cybersecurity Through Game Based Systems. In *ASEE Conference for Industry & Education Collaboration (CIEC)*. New Orleans, LA.

Bada, M., & Nurse, J. R. (2019). Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (smes). *Information & Computer Security*.

Baker, M. (2016). Striving for effective cyber workforce development. *Software Engineering Institute, May. https://resources. sei. cmu. edu/library/asset-view. cfm*.

Banghart, S., Etter, M., & Stohl, C. (2018). Organizational boundary regulation through social media policies. *Management Communication Quarterly*, *32*(3), 337–373.

Barrett, M. P. (2018). Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. `https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11`.

Ben Salamah, F., Palomino, M. A., Papadaki, M., & Furnell, S. (2022). The Importance of the Job Role in Social Media Cybersecurity Training. In *IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, (pp. 454–462).

Bennett, L. V., & Manoharan, A. P. (2017). The use of social media policies by us municipalities. *International Journal of Public Administration*, *40*(4), 317–328.

Bhatnagar, N., & Pry, M. (2020). Student attitudes, awareness, and perceptions of personal privacy and cybersecurity in the use of social media: An initial study. *Information Systems Education Journal*, *18*(1), 48–58.

Blackburn, J., De Cristofaro, E., Sirivianos, M., & Strufe, T. (2018). Cybersafety in modern online social networks (dagstuhl reports 17372). In *Dagstuhl Reports*, vol. 7. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik.

Blackwood-Brown, C., Levy, Y., & D'Arcy, J. (2021). Cybersecurity awareness and skills of senior citizens: a motivation perspective. *Journal of Computer Information Systems*, *61*(3), 195–206.

BRC (2015). BRC RETAIL CRIME SURVEY 2015. Tech. rep., British Retail Consortium. `https://brc.org.uk/media/54300/51309-4_2015_crime_survey_report_p7.pdf`.

Brilingaitė, A., Bukauskas, L., & Juozapavičius, A. (2020). A framework for competence development and assessment in hybrid cybersecurity exercises. *Computers & Security*, *88*, 101607.

Bygstad, B., & Munkvold, B. E. (2007). The significance of member validation in qualitative analysis: Experiences from a longitudinal case study. In *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*, (pp. 243b–243b). IEEE.

Calculator.net (2022). Confidence Interval Calculator.

Castro, S. (2018). Google forms quizzes and substitution, augmentation, modification, and redefinition (samr) model integration. *Issues and Trends in Educational Technology*, *6*(2).

Caulkins, B. D., Badillo-Urquiola, K., Bockelman, P., & Leis, R. (2016). Cyber workforce development using a behavioral cybersecurity paradigm. In *2016 International Conference on Cyber Conflict (CyCon US)*, (pp. 1–6). IEEE.

Chapple, M., Stewart, J. M., & Gibson, D. (2021). *Certified Information System Security Professional (CISSP)*. SYBEX, ninth edition ed.

Chatterjee, R., Bajwa, S., Dwivedi, D., Kanji, R., Ahammed, M., & Shaw, R. (2020). Covid-19 risk assessment tool: Dual application of risk communication and risk governance. *Progress in Disaster Science*, *7*, 100109.

Chen, Q., Xu, X., Cao, B., & Zhang, W. (2016). Social media policies as responses for social media affordances: The case of china. *Government information quarterly*, *33*(2), 313–324.

Chiaburu, D. S., & Marinova, S. V. (2005). What predicts skill transfer? an exploratory study of goal orientation, training self-efficacy and organizational supports. *International journal of training and development*, *9*(2), 110–123.

Chowdhury, N., & Gkioulos, V. (2021). Cyber security training for critical infrastructure protection: A literature review. *Computer Science Review*, *40*, 100361.

Chowdhury, N., Katsikas, S., & Gkioulos, V. (2022). Modeling effective cybersecurity training frameworks: A delphi method-based study. *Computers & Security*, *113*, 102551.

Christopher, L., Choo, K.-K., & Dehghantanha, A. (2017). Honeypots for employee information security awareness and education training: a conceptual easy training model. In *Contemporary Digital Forensic Investigations of Cloud and Mobile Applications*, (pp. 111–129). Elsevier.

CITRA (2022). National Cyber Security Strategy For The State Of Kuwait 2017-2020. Tech. rep., Communication and INFO Technology Regulatory Authority. `https://citra.gov.kw/sites/en/Pages/cybersecurity.aspx`.

Clark, R. M., & Hakim, S. (2016). *Cyber-physical security: protecting critical infrastructure at the state and local level*, vol. 3. Springer.

Clavin,D (2022). Famous Phishing Incidents from History. `https://www.hempsteadny.gov/635/Famous-Phishing-Incidents-from-History..`

Cleary, G., Corpin, M., & Cox, O. (2018). Symantec Internet Security Threat Report. Tech. Rep. 23, Symantec Corporation, Mountain View, CA. `https://docs.broadcom.com/doc/istr-23-executive-summary-en`.

Connell, J. P., & Kubisch, A. C. (1998). Applying a theory of change approach to the evaluation of comprehensive community initiatives: progress, prospects, and problems. *New approaches to evaluating community initiatives*, *2*(15-44), 1–16.

Creswell, J. (2003). Creswell, jw (2003). one,"a framework for design." research design qualitative quantitative and mixed methods approaches, 3–26.

Croasmun, J. T., & Ostrom, L. (2011). Using likert-type scales in the social sciences. *Journal of adult education*, *40*(1), 19–22.

Cybersecurity, C. I. (2018). Framework for improving critical infrastructure cybersecurity. *URL: https://nvlpubs. nist. gov/nistpubs/CSWP/NIST. CSWP*, *4162018*.

Das, R., & Patel, M. (2017). Cyber security for social networking sites: Issues, challenges and solutions. *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, *5*(4,833-838).

Dawson, M. (2018). Applying a holistic cybersecurity framework for global it organizations. *Business Information Review*, *35*(2), 60–67.

DBIR (2020). Data Investigations Report 2020. Tech. rep., verizon. `https://www.cisecurity.org/wp-content/uploads/2020/07/The-2020-Verizon-Data-Breach-Investigations-Report-DBIR.pdf`.

De Swert, K. (2012). Calculating Inter-Coder Reliability in Media Content Analysis Using Krippendorff's Alpha. *Center for Politics and Communication*, *15*.

DeCuir-Gunby, J. T., Marshall, P. L., & McCulloch, A. W. (2011). Developing and using a codebook for the analysis of interview data: An example from a professional development research project. *Field methods*, *23*(2), 136–155.

DeFranzo, S. (2020). Reasons why feedback is important.

Demek, K. C., Raschke, R. L., Janvrin, D. J., & Dilla, W. N. (2018). Do organizations use a formalized risk management process to address social media risk? *International Journal of Accounting Information Systems*, *28*, 31–44.

Denzin, N. K., & Lincoln, Y. S. (2011). *The Sage handbook of qualitative research*. sage.

Dhakal, R. (2018). *Measuring the Effectiveness of an Information Security Training and Awareness Program*. Ph.D. thesis, Charles Sturt University, Bathurst, Australia.

Diamantidis, A. D., & Chatzoglou, P. D. (2014). Employee post-training behaviour and performance: evaluating the results of the training process. *International Journal of Training and Development*, *18*(3), 149–170.

Downes, S. (2022). Instagram impersonation fraud up by 155 percent as organised crime continues to thrive on social media.

Duan, Y., Zhao, J., Chen, J., & Bai, G. (2016). A Risk Matrix Analysis Method Based on Potential Risk Influence: A Case Study on Cryogenic Liquid Hydrogen Filling System. *Process Safety and Environmental Protection*, *102*, 277–287.

Duff, A. (1996). The literature search: a library-based model for information skills instruction. *Library review*.

Dugan, N. (2018). *Security awareness training in a corporate setting*. Ph.D. thesis, Iowa State University.

Edgar, T., & Manz, D. (2017). *Research methods for cyber security*. Syngress.

Elliott, M. (2018).
URL `https://www.cnet.com/tech/mobile/50-million-facebook-accounts-were-compromised-`

Ertmer, P. A., Richardson, J. C., Belland, B., Camin, D., Connolly, P., Coulthard, G., Lei, K., & Mong, C. (2007). Using peer feedback to enhance the quality of student online postings: An exploratory study. *Journal of Computer-Mediated Communication*, *12*(2), 412–433.

Esparza, J., Caporusso, N., & Walters, A. (2020). Addressing human factors in the design of cyber hygiene self-assessment tools. In *International Conference on Applied Human Factors and Ergonomics*, (pp. 88–94). Springer.

European Network and Information Security Agency (ENISA) (2010). Cyber Europ 2010 – Evaluation Report. https://www.enisa.europa.eu/publications/ce2010report/at_download/fullReport.

European Network and Information Security Agency (ENISA) (2012). Collaborative Solutions for Network Information Security in Education. https://www.enisa.europa.eu/publications/.

European Network and Information Security Agency (ENISA) (2019). Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity. https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity.

European Union Agency for Cybersecurity (2014). Good Practice Guide on Training Methodologies. https://www.enisa.europa.eu/publications/good-practice-guide-on-training-methodologies/.

European Union Agency for Cybersecurity (2017). Stocktaking of Information Security Training Needs in Critical Sectors. https://www.enisa.europa.eu/news/enisa-news/.

Farooq, M., Khan, M. A., et al. (2011). Impact of training and feedback on employee performance. *Far east journal of psychology and business*, *5*(1), 23–33.

Ferrara, E. (2019). The history of digital spam. *Communications of the ACM*, *62*(8), 82–91.

Furnell, S., & Vasileiou, I. (2017). Security education and awareness: just let them burn? *Network Security*, *2017*(12), 5–9.

Galanou, E., & Priporas, C.-V. (2009). A model for evaluating the effectiveness of middle managers' training courses: evidence from a major banking organization in greece. *International Journal of training and development*, *13*(4), 221–246.

Gasiba, T., Lechner, U., & Pinto-Albuquerque, M. (2021). CyberSecurity Challenges for Software Developer Awareness Training in Industrial Environments. In *International Conference on Business Information Systems*, (pp. 370–387). Springer.

George, Ioannidis, S., Smyrlis, M., Spanoudakis, G., Frati, F., Goeke, L., Hildebrandt, T., Tsakirakis, G., Oikonomou, F., Leftheriotis, G., et al. (2020). Modern aspects of cybersecurity training and continuous adaptation of programmes to trainees. *Applied Sciences*, *10*(16), 5702.

Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D. (2022). A cyber-security culture framework for assessing organization readiness. *Journal of Computer Information Systems*, *62*(3), 452–462.

Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S., Jabbar, S., & Baker, T. (2018). Security threats to critical infrastructure: the human factor. *The Journal of Supercomputing*, *74*(10), 4986–5002.

Gharawi, M. A., Badawy, A., Ramadan, D. E., & Elsayed, S. (2021). Social media impersonation in the virtual world. *Al-hikmah: International Journal of Islamic Studies and Human Sciences*, *4*(1), 57–65.

Ghazvini, A., & Shukur, Z. (2016). Awareness Training Transfer and Information Security Content Development for Healthcare Industry. *International Journal of Advanced Computer Science and Applications*, *7*(5).

Gjertsen, E. G. B., Gjære, E. A., Bartnes, M., & Flores, W. R. (2017). Gamification of information security awareness and training. In *Information Certified Information Security System Proffessional- ICISSP*, (pp. 59–70).

Glaspie, H. W., & Karwowski, W. (2017). Human factors in information security culture: A literature review. In *International Conference on Applied Human Factors and Ergonomics*, (pp. 269–280). Springer.

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *computers & security*, *73*, 345–358.

Green, J. S. (2016). *Cyber Security: An Introduction for Non-Technical Managers*. Routledge.

Griffin, L. L. (2021). *The Effectiveness of Cybersecurity Awareness Training in Reducing Employee Negligence Within Department of Defense (DoD) Affiliated Organizations-Qualitative Exploratory Case Study*. Ph.D. thesis, Capella University.

Guerar, M., Merlo, A., Migliardi, M., & Palmieri, F. (2018). Invisible cappcha: A usable mechanism to distinguish between malware and humans on the mobile iot. *Computers & Security*, *78*, 255–266.

Gupta, S., Singhal, A., & Kapoor, A. (2016). A literature survey on social engineering attacks: Phishing attack. In *2016 international conference on computing, communication and automation (ICCCA)*, (pp. 537–540). IEEE.

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, *3*(7).

Hadlington, L. (2018). Employees Attitudes towards Cyber Security and Risky Online Behaviours: An Empirical Assessment in the United Kingdom. *International Journal of Cyber Criminology*, *12*(1), 262–274.

Hadnagu, C. (2019). *Social Engineering: The Science of Human Hacking*. Gildan Media.

Haeussinger, F., & Kranz, J. (2017). Antecedents of employees'information security awareness-review, synthesis, and directions for future research. *Association for Information Systems AIS Electronic Library*.

Hamtini, T. M. (2008). Evaluating e-learning programs: An adaptation of kirkpatrick's model to accommodate e-learning environments. *Journal of Computer Science*, *4*(8), 693.

Harding, L. (2014).
URL `https://www.theguardian.com/world/2014/aug/14/dmitry-medvedev-russian-pm-twitter-account-hacked`

Hauser, J., & Katz, G. (1998). Metrics: you are what you measure! *European Management Journal*, *16*(5), 517–528.

Healey, J. F. (2014). *Statistics: A tool for social research*. Cengage Learning.

Hiltz, S. R., Kushma, J. A., & Plotnick, L. (2014). Use of social media by us public sector emergency managers: Barriers and wish lists. *ISCRAM*, *10*(2.1), 3122–4005.

Hofstede, G. (2001). *Culture's consequences: Comparing values, behaviors, institutions and organizations across nations*. sage.

Holgado Tello, F. P., Chacon Moscoso, S., Barbero Garcia, I., & Sanduvete Chaves, S. (2006). Training satisfaction rating scale: development of a measurement model using polychoric correlations. *European Journal of Psychological Assessment*, *22*(4), 268–279.

Hossain, M. S., Paul, A., Islam, M. H., & Atiquzzaman, M. (2018). Survey of the protection mechanisms to the ssl-based session hijacking attacks. *Netw. Protoc. Algorithms*, *10*(1), 83–108.

Hovav, A., & Putri, F. F. (2016). This is my device! why should i follow your rules? employees' compliance with byod security policy. *Pervasive and Mobile Computing*, *32*, 35–49.

Irshad, S., & Soomro, T. R. (2018). Identity theft and social media. *International Journal of Computer Science and Network Security*, *18*(1), 43–55.

ITU (2022). Global Cybersecurity Index. `https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx`.

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social Phishing. *Communications of the ACM*, *50*(10), 94–100.

Jamil, A., Asif, K., Ghulam, Z., Nazir, M. K., Alam, S. M., & Ashraf, R. (2018). Mpmpa: A mitigation and prevention model for social engineering based phishing attacks on facebook. In *2018 IEEE International Conference on Big Data (Big Data)*, (pp. 5040–5048). IEEE.

Jardine, E. (2015). Global cyberspace is safer than you think: Real trends in cybercrime.

Javidi, G., Sheybani, E., & Pieri, Z. (2019). A holistic approach to k12 cybersecurity education. In *Proceedings of the International Conference on Frontiers in Education: Computer Science and Computer Engineering (FECS)*, (pp. 77–80). The Steering Committee of The World Congress in Computer Science, Computer ....

Jeong, J., Mihelcic, J., Oliver, G., & Rudolph, C. (2019). Towards an improved understanding of human factors in cybersecurity. In *2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC)*, (pp. 338–345). IEEE.

Jeske, D., & Van Schaik, P. (2017). Familiarity with internet threats: Beyond awareness. *Computers & Security*, *66*, 129–141.

Jethava, G., & Rao, U. P. (2022). User behavior-based and graph-based hybrid approach for detection of sybil attack in online social networks. *Computers and Electrical Engineering*, *99*, 107753.

Jin, G., Tu, M., Kim, T.-H., Heffron, J., & White, J. (2018). Evaluation of game-based learning in cybersecurity education for high school students. *Journal of Education and Learning (EduLearn)*, *12*(1), 150–158.

Johannessen, J.-A., Olsen, B., & Olaisen, J. (1999). Aspects of innovation theory based on knowledge-management. *International journal of information management*, *19*(2), 121–139.

Joshi, A., Kale, S., Chandel, S., & Pal, D. K. (2015). Likert scale: Explored and explained. *British journal of applied science & technology*, *7*(4), 396.

Jupin, J. A., Sutikno, T., Ismail, M. A., Mohamad, M. S., Kasim, S., & Stiawan, D. (2019). Review of the machine learning methods in the classification of phishing attack. *Bulletin of Electrical Engineering and Informatics*, *8*(4), 1545–1555.

Kadena, E., & Gupi, M. (2021). Human factors in cybersecurity: Risks and impacts. *Security science journal*, *2*(2), 51–64.

Kemp, S. (2020). Digital 2020: 3.8 billion people use social media. We Are Social Ltd.

Khaled, S., El-Tazi, N., & Mokhtar, H. M. (2018). Detecting fake accounts on social media. In *2018 IEEE international conference on big data (big data)*, (pp. 3672–3681). IEEE.

Khandpur, R. P., Ji, T., Jan, S., Wang, G., Lu, C.-T., & Ramakrishnan, N. (2017). Crowdsourcing cybersecurity: Cyber attack detection using social media. In *Proceedings of the 2017 ACM on Conference on Information and Knowledge Management*, (pp. 1049–1057).

Ki-Aries, D., & Faily, S. (2017). Persona-centred information security awareness. *computers & security*, *70*, 663–674.

Kim, T. K. (2015). T test as a parametric statistic. *Korean journal of anesthesiology*, *68*(6), 540–546.

King, Z. M., Henshel, D. S., Flora, L., Cains, M. G., Hoffman, B., & Sample, C. (2018). Characterizing and Measuring Maliciousness for Cybersecurity Risk Assessment. *Frontiers in Psychology*, *9*, 39.

Kirkpatrick, D. L. (1978). Evaluating in-house training programs. *Training and Development Journal*, *32*(9), 6–9.

Kuwait Central Statistical Bureau (2021). Population Estimates.

Laker, D. R. (1990). Dual dimensionality of training transfer. *Human Resource Development Quarterly*, *1*(3), 209–223.

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, *105*, 102248.

Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons*, *64*(5), 659–671.

Liew, C. L. (2021). National memory institutions' social media policies and risk management: a content analysis. *Online Information Review*, *46*(2), 205–223.

Lin, X., & Wang, X. (2020). Examining Gender Differences in People'S Information-Sharing Decisions on Social Networking Sites. *International Journal of Information Management*, *50*, 45–56.

Löffler, E., Schneider, B., Zanwar, T., & Asprion, P. M. (2021). Cysecescape 2.0—a virtual escape room to raise cybersecurity awareness. *International Journal of Serious Games*, *8*(1), 59–70.

Luo, W., Liu, J., Liu, J., & Fan, C. (2009). An analysis of security in social networks. In *2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing*, (pp. 648–651). IEEE.

Maglaras, L., Ferrag, M., Derhab, A., Mukherjee, M., Janicke, H., & Rallis, S. (2018). Threats, countermeasures and attribution of cyber attacks on critical infrastructures. *EAI Endorsed Transactions on Security and Safety*, *5*(16).

Markowski, A. S., & Mannan, M. S. (2008). Fuzzy Risk Matrix. *Journal of Hazardous Materials*, *159*(1), 152–157.

McHugh, M. L. (2013). The Chi-Square Test of Independence. *Biochemia Medica*, *23*(2), 143–149.

McKim, C. A. (2017). The value of mixed methods research: A mixed methods study. *Journal of mixed methods research*, *11*(2), 202–222.

Milkovich, D. (2021). 15 Alarming Cyber Security Facts and Stats. Cybint Solutions. https://www.cybintsolutions.com/cyber-security-facts-stats/.

Molenda, M. (2003). In search of the elusive addie model. *Performance improvement*, *42*(5), 34–37.

Mousavi, R., Chen, R., Kim, D. J., & Chen, K. (2020). Effectiveness of privacy assurance mechanisms in users' privacy protection on social networking sites from the perspective of protection motivation theory. *Decision Support Systems*, *135*, 113323.

Muhirwe, J., & White, N. (2016). Cybersecurity awareness and practice of next generation corporate technology users. *Issues in Information Systems*, *17*(2).

NCSC (2019). Social media: how to use it safely.
URL https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely#:~:text=Use

Nicholson, D., Massey, L., O'Grady, R., & Ortiz, E. (2016). Tailored cybersecurity training in lvc environments. In *MODSIM World Conference, Virginia Beach, VA*.

Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organisations: A systematic review. *Sensors*, *21*(15), 5119.

Nurse, J. R., Creese, S., & De Roure, D. (2017). Security Risk Assessment in Internet of Things Systems. *IT professional*, *19*(5), 20–26.

Nurse, J. R., Creese, S., Goldsmith, M., & Lamberts, K. (2011). Trustworthy and effective communication of cybersecurity risks: A review. In *2011 1st Workshop on Socio-Technical Aspects in Security and Trust (STAST)*, (pp. 60–68). IEEE.

Nyoni, P., & Velempini, M. (2018). Privacy and user awareness on facebook. *South African Journal of Science*, *114*(5-6), 1–5.

of interior Kuwait, M. (2022). Electronic and Cyber Crime Combating Department . Tech. rep., Communication and INFO Technology Regulatory Authority. https://www.moi.gov.kw/main/sections/cyber-crime.

Ostroff, C. (1991). Training effectiveness measures and scoring schemes: A comparison. *Personnel Psychology*, *44*(2), 353–374.

Ozkaya, E. (2018). *Cybersecurity Challenges in Social Media*. Ph.D. thesis, Charles Sturt University.

Pandey, S., & Bright, C. L. (2008). What are degrees of freedom? *Social Work Research*, *32*(2), 119–128.

Parker, H. J., & Flowerday, S. V. (2020). Contributing Factors to Increased Susceptibility to Social Media Phishing Attacks. *South African Journal of Information Management*, *22*(1), 1–10.

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*.

Pattinson, M. R., Butavicius, M. A., Ciccarello, B., Lillie, M., Parsons, K., Calic, D., & McCormac, A. (2018). Adapting cyber-security training to your employees. In *HAISA*, (pp. 67–79).

Pedley, D., Borges, T., Bollen, A., Shah, J. N., Donaldson, S., Furnell, S., & Crozier, D. (2020). Cyber security skills in the uk labour market 2020.

Pendleton, M., Garcia-Lebron, R., Cho, J.-H., & Xu, S. (2016). A survey on systems security metrics. *ACM Computing Surveys (CSUR)*, *49*(4), 1–35.

Peterson, C. (2003). Bringing addie to life: Instructional design at its best. *Journal of Educational Multimedia and Hypermedia*, *12*(3), 227–241.

Qazi, A., & Akhtar, P. (2020). Risk matrix driven supply chain risk management: Adapting risk matrix based tools to modelling interdependent risks and risk appetite. *Computers & Industrial Engineering*, *139*, 105351.

Rahman, T., Rohan, R., Pal, D., & Kanthamanon, P. (2021). Human factors in cybersecurity: a scoping review. In *The 12th International Conference on Advances in Information Technology*, (pp. 1–11).

Rajamäki, J., Nevmerzhitskaya, J., & Virág, C. (2018). Cybersecurity education and training in hospitals: Proactive resilience educational framework (prosilience ef). In *2018 IEEE Global Engineering Education Conference (EDUCON)*, (pp. 2042–2046). IEEE.

Reja, U., Manfreda, K. L., Hlebec, V., & Vehovar, V. (2003). Open-ended vs. close-ended questions in web questionnaires. *Developments in applied statistics*, *19*(1), 159–177.

Reznik, M. (2012). Identity theft on social networking sites: developing issues of internet impersonation. *Touro L. Rev.*, *29*, 455.

Rieff, I. (2018). Systematically applying gamification to cyber security awareness trainings: A framework and case study approach.

Rise (2021). website.
URL `https://risepeople.com/blog/5-metrics-team-member-performance/`

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *computers & security*, *56*, 70–82.

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet*, *11*(4), 89.

Saridakis, G., Benson, V., Ezingeard, J.-N., & Tennakoon, H. (2016). Individual Information Security, User Behaviour and Cyber Victimisation: An Empirical Study of Social Networking Users. *Technological Forecasting and Social Change*, *102*, 320–330.

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. *BT technology journal*, *19*(3), 122–131.

Sasse, M. A., & Flechais, I. (2005). Usable security: Why do we need it? how do we get it? O'Reilly.

Scholefield, S., & Shepherd, L. A. (2019). Gamification techniques for raising cyber security awareness. In *International Conference on Human-Computer Interaction*, (pp. 191–203). Springer.

Scholl, M. C., Fuhrmann, F., & Scholl, L. R. (2018). An Exploratory Study of Current Information Security Training and Awareness Practices in Organizations. In *Annual Hawaii International Conference on System Sciences*, (p. 2235–2244). Honolulu, HI: IEEE Computer Society.

Schreuders, Z. C., & Butterfield, E. (2016). Gamification for teaching and learning computer security in higher education. In *2016 USENIX Workshop on Advances in Security Education (ASE 16)*.

Schürmann, C., Jensen, L. H., & Sigbjörnsdóttir, R. M. (2020). Effective cybersecurity awareness training for election officials. In *International Joint Conference on Electronic Voting*, (pp. 196–212). Springer.

Siami Namin, A., Aguirre-Muñoz, Z., & Jones, K. (2016). Teaching cyber security through competition an experience report about a participatory training workshop. In *CSEIT 2016: 10th International Conference on Computer Science Education: Innovation and Technology*.

Smith, E. D., Siefert, W. T., & Drain, D. (2009). Risk Matrix Input Data Biases. *Systems Engineering*, *12*(4), 344–360.

Sookhai, F., & Budworth, M.-H. (2010). The trainee in context: Examining the relationship between self-efficacy and transfer climate for transfer of training. *Human Resource Development Quarterly*, *21*(3), 257–272.

Southampton, U. (2022). Chi Square. University of Southampton. `https://www.southampton.ac.uk/passs/full_time_education/bivariate_analysis/chi_square.page`.

Stefaniuk, T., et al. (2020). Training in shaping employee information security awareness. *Entrep. Sustain*, *7*.

Stockhardt, S., Reinheimer, B., Volkamer, M., Mayer, P., Kunz, A., Rack, P., & Lehmann, D. (2016). Teaching phishing-security: which way is best? In *IFIP International Conference on ICT Systems Security and Privacy Protection*, (pp. 135–149). Springer.

Stoessel, J. W. (2016). *Social Media Policy Implications in Higher Education: Do Faculty, Administration, and Staff have a Place in the" Social Network"?*. Seton Hall University.

Suryotrisongko, H., & Musashi, Y. (2019). Review of cybersecurity research topics, taxonomy and challenges: Interdisciplinary perspective. In *2019 IEEE 12th Conference on Service-Oriented Computing and Applications (SOCA)*, (pp. 162–167). IEEE.

Taniuchi, S., Aoyama, T., Asai, H., & Koshijima, I. (2018). Training cyber security exercise facilitator: Behavior modeling based on human error. In *International Conference on Applied Human Factors and Ergonomics*, (pp. 138–148). Springer.

Tapanainen, T. (2017). Sense-making in cyber security–examining responder behaviors in cyber-attacks.

Tayouri, D. (2015). The human factor in the social media security–combining education and technology to reduce social engineering risks and damages. *Procedia Manufacturing*, *3*, 1096–1100.

Terlizzi, M. A. (2019). *Privacy concerns and protection motivation theory in the context of mobile banking*. Ph.D. thesis, ESCOLA DE ADMINISTRAÇÃO DE EMPRESAS DE SÃO PAULO.

Thakur, K., Hayajneh, T., & Tseng, J. (2019). Cyber security in social media: Challenges and the way forward. *IT Professional*, *21*(2), 41–49.

Toth, P., & Klein, P. (2014). A Role-Based Model for Federal Information Technology/Cybersecurity Training. *National Institute of Standards and Technology (NIST)*, *800*(16), 1–152.

Triplett, W. J. (2022). Addressing human factors in cybersecurity leadership. *Journal of Cybersecurity and Privacy*, *2*(3), 573–586.

Tsokkis, P., & Stavrou, E. (2018). A password generator tool to increase users' awareness on bad password construction strategies. In *2018 International Symposium on Networks, Computers and Communications (ISNCC)*, (pp. 1–5). IEEE.

University of Plymouth (2022). Plymouth Ethics Online System (PEOS). `https://www.plymouth.ac.uk/research/plymouth-ethics-online-system`.

Uzun, E., Chung, S. P. H., Essa, I., & Lee, W. (2018). rtcaptcha: A real-time captcha based liveness detection system. In *NDSS*.

van der Kleij, R., Wijn, R., & Hof, T. (2020). An application and empirical test of the capability opportunity motivation-behaviour model to data leakage prevention in financial organizations. *Computers & Security*, *97*, 101970.

Van Schaik, P., Jansen, J., Onibokun, J., Camp, J., & Kusev, P. (2018). Security and privacy in online social networking: Risk perceptions and precautionary behaviour. *Computers in Human Behavior*, *78*, 283–297.

Velada, R., & Caetano, A. (2007). Training transfer: the mediating role of perception of learning. *Journal of european industrial training*.

Venter, I. M., Blignaut, R. J., Renaud, K., & Venter, M. A. (2019). Cyber security education is as essential as "the three r's". *Heliyon*, *5*(12), e02855.

Walkington, C., & Bernacki, M. L. (2020). Appraising research on personalized learning: Definitions, theoretical alignment, advancements, and future directions.

Wang, Y., Qi, B., Zou, H.-X., & Li, J.-X. (2018). Framework of raising cyber security awareness. In *2018 IEEE 18th International Conference on Communication Technology (ICCT)*, (pp. 865–869). IEEE.

Weiss, C. H., et al. (1995). Nothing as practical as good theory: Exploring theory-based evaluation for comprehensive community initiatives for children and families. *New approaches to evaluating community initiatives: Concepts, methods, and contexts*, *1*, 65–92.

Weiss, R. S. (1968). Statistics in social research: An introduction. *(No Title)*.

William, O. (2022). Kuwait. Britannica. `https://www.britannica.com/place/Kuwait`.

Wisniewski, P. J., Knijnenburg, B. P., & Lipford, H. R. (2017). Making privacy personal: Profiling social network users to inform privacy education and nudging. *International Journal of human-computer studies*, *98*, 95–108.

Yang, X., Kim, S., & Sun, Y. (2019). How do influencers mention brands in social media? sponsorship prediction of instagram posts. In *Proceedings of the 2019 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*, (pp. 101–104).

Yin, R. K. (2009). *Case study research: Design and methods*, vol. 5. sage.

Yockey, R. D. (2016). *SPSS Demystified: A Simple Guide and Reference*. Routledge.

Yuan, X., Zhou, J., Huang, B., Wang, Y., Yang, C., & Gui, W. (2019). Hierarchical quality-relevant feature representation for soft sensor modeling: A novel deep learning strategy. *IEEE transactions on industrial informatics*, *16*(6), 3721–3730.

Zárate-Moedano, R., Canchlola-Magdaleno, S., & Arrington, A. (2021). Remote laboratory, based on raspberry pi, to facilitate scientific experimentation for secondary school students. *International Journal of Online & Biomedical Engineering*, *17*(14).

Zarei, K., Farahbakhsh, R., Crespi, N., & Tyson, G. (2020). Impersonation on social media: a deep neural approach to identify ingenuine content. In *2020 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, (pp. 11–15). IEEE.

Zhang, Z., & Gupta, B. B. (2018). Social media security and trustworthiness: overview and new direction. *Future Generation Computer Systems*, *86*, 914–925.

Zhang, Z. J., He, W., Li, W., & Abdous, M. (2021). Cybersecurity awareness training programs: a cost–benefit analysis framework. *Industrial Management & Data Systems*.

Zheng, H., Xue, M., Lu, H., Hao, S., Zhu, H., Liang, X., & Ross, K. (2017). Smoke screener or straight shooter: Detecting elite sybil attacks in user-review social networks. *arXiv preprint arXiv:1709.06916*.

Zwilling, M., Lesjak, D., Natek, S., Phusavat, K., Anussornnitisarn, P., et al. (2019). How to deal with the awareness of cyber hazards and security in (higher) education. In *Thriving on future education, industry, business and society. Proceedings of the Makelearn and TIIM International Conference*, (pp. 433–439).

Publications

Salamah, Fai Ben, et al. "The Importance of the Job Role in Social Media Cybersecurity Training." 2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). IEEE, 2022.

DOI : 10.1109/EuroSPW55150.2022.00054

PEARL(OA):http://pearl.plymouth.ac.uk/bitstream/handle/10026.1/19477/bensalamaheurocsep20

Ben Salamah, F., et al. "Evaluating the Risks of Human Factors Associated with Social Media Cybersecurity Threats." 2023.

PEARL (OA) :http://pearl.plymouth.ac.uk/handle/10026.1/21051

DOI: 10.1007/978-3-031-38530-8_28

Appendices

Survey Questions

Section 1 (Information Sheet)

Dear Participant:

My name is Fai Bensalama, and I am a PhD student at Plymouth University. As part of my project, I am examining social media security risks and existing training approaches that help users address social media security risks more effectively. Where, this project attempt to identify social media user's preferences, limitation and challenges toward different security training approach. Because you are Kuwaiti employee using social media and working in Kuwait, I am inviting you to participate in this research study by completing this survey.

The following questionnaire is user-friendly and will require approximately 10-15 minutes to complete. Your responses will be kept entirely secret, and to ensure that all information will remain confidential, please do not include your name. Copies of the project will be provided to my Plymouth University supervisory team. Please answer all questions as honestly as possible.

Moreover, this project requires a second level assessment, where we are planning to do in-depth interviews with stakeholders to supplement the study. Your participation in this project would go a long way towards helping us achieve our research goals. The interview would last approximately 30-40 minutes and, should you agree to participate, I would be grateful if you could let me know by sending me an email or text message.

Please note that participation in this project is voluntary; it is up to you to decide whether to participate. If you choose to participate in this survey and continue into the second level of assessment, please note that you could withdraw after no more than two months.

Thank you for taking the time to assist me in my educational endeavors. 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. If you require additional information or have questions, concerns or complaints, please contact us at the number or/and E-mail address listed below. Student name: Fai Ben Salamah Phone number: +44 7500 282526 Email address: fai.bensalamah@plymouth.ac.uk DOS name: Dr Marco Palomino Email address: marco.palomino@plymouth.ac.uk Faculty ethics: scienghumanethics@plymouth.ac.uk

Section 2 (The survey qyestions)

1-Age:

- 18-25

- 25-35

- 36-45

- 46-55

- Over 55

- Prefer not to say

2-Gender: -Male

-Female

- Prefer not to say

3-Education Level:

- Less than secondary school degree

- Secondary school degree

- Bachelor degree

- Post Graduate degree (e.g.; Masters, PhD)

- Prefer not to say

4-Which of the following best describes your current job role or discipline?

-Education, Training and Library

-Computer and Technology

-Healthcare Support

-Leadership and Management

-Business and Financial operations

-Arts, Design, Entertainment, Sport and Media

-Office and Administrative Support

-Military such as, the Army and Police

-Others (Please Specify)

-Prefer not to say

5-Total Years of Work Experience in your current role/discipline:

-Less than 2 years

-2-5

-5-10

-10-15

-15-20

-20-25

-More than 25

-Prefer not to say

6- How much time do you spend on social media per day?

-Less than 30 minutes

-30-60 minutes

-1-2 hours

-2-3 hours

-+3 hours

7-What is your current social media account profile status?

	Public	Private	Don't know	I don't use it
Instagram				
Twitter				
Facebook				
LinkedIn				
Snapchat				
WhatsApp				

If you have any other social media accounts, pls specify it with its current status...

8- What devices you normally use to access social media? , and for how long per day?

	0	1-2 Hr	3-4 Hr	5-6 Hr	+ 6 Hr	Prefer not to say
Mobile phone						
Tablet						
Home desktop/laptop						
Work desktop/laptop						

9.Please state the degree to which you agree with the following statements (Please enter one answer per question):-

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Privacy and security are important to me					
I'm not responsible for my information security as it is the function of IT staff.					
Technology alone protection programmes can protect devices from being hacked.					
I read and understand security policies related to social media					
I know how to navigate the social media system settings , and set the security options that are available.					

10- Have you been a victim of a cyber-attack, breach, or loss of privacy?

-Yes

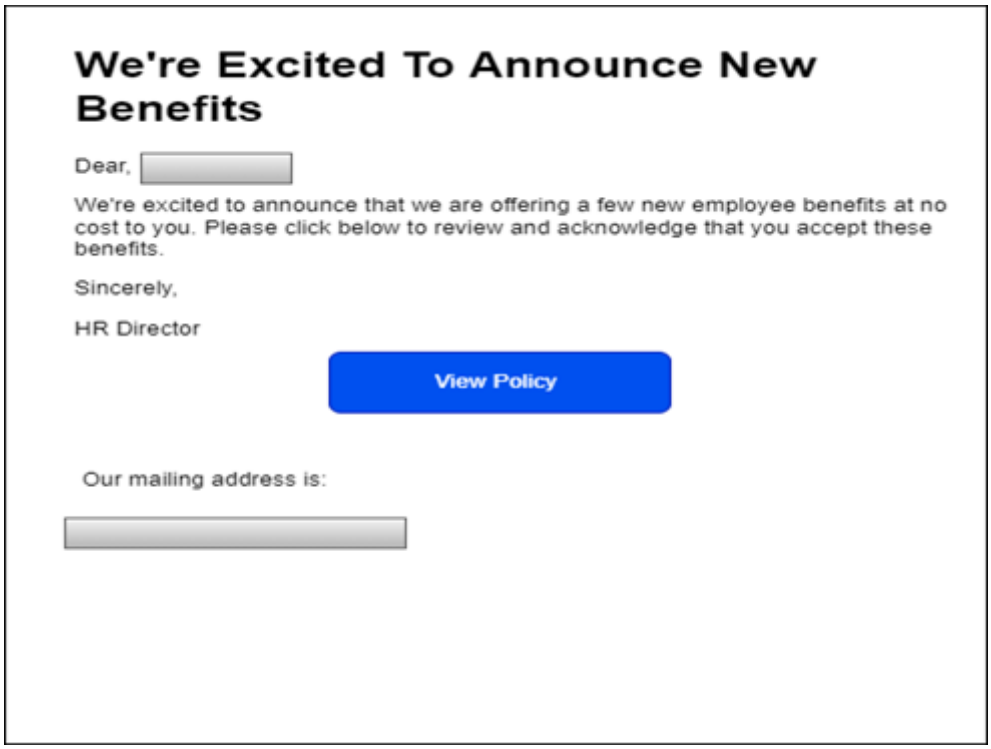
-No

-Maybe

If yes, pls provide more details about the incident, and how you combated this inci-

dent?

11- What do you do if you receive this email?



- I will click on the blue button to view policy
- I will ignore it
- I will report is as spam
- I will contact the HR department through a separate email thread asking about the new benefits
- Others (pls specify)

12-Could you justify your reasoning? ...

13-Which of the following considered sensitive details if it posts on social media? (please select all appropriate)

- Your phone number
- Group photo with your colleagues
- Your home address
- You are on vacation
- Something you have achieved (e.g. win an award, Graduation)
- Your email address

14-Which of the following options best describes phishing? (pls select one answer)

- A type of attack to destroy your device
- A method of trying to gather sensitive information using deceptive emails and websites
- An attempt to obtain more followers on social media
- A technical skill of managing a ship
- I don't know

15-Which of the following links is considered more secure?

- http://www
- https://www

16. To What extent you agree with those statements:

	Never	**Rarely**	**Sometimes**	**Often**	**Always**
I use public networks, like those in the cafes or airports.					
I use a combination of letters, numbers and special characters when choosing a password.					
I use antivirus software to protect my devices.					
I regularly check the antivirus software update on my devices.					
I always check the spelling of the URLs in links before I click or enter sensitive information.					

17-Please select the training approach that you would prefer or that you have found most useful for cybersecurity training/learning?

	Not at all useful	**Slightly useful**	**Moderately useful**	**Very Useful**	**Extremely useful**
Workshops/Inclass					
Online					
Posters					
Games/Gamification					
Webinars					
Social Media					
Story telling					
Offer incentives					
Tip-sheets					
Mock attack					
Events					
Videos					
Emails					

18-Have you ever been trained/taught about cybersecurity?

-Yes (The system will take you to Q.19)

-No (The system will take you to Q.23)

Section 3

You have been training/ learning about cyber security;

19-Where did you receive this training/learning about cybersecurity?

-school

- University

-Work

-Online resources

20- How many times a year did you train/learn for cybersecurity?

-Once a year

-Twice a year

-Every three months

-Every month

- Other (please specify)

21- What best describes the cybersecurity training you have received? Please select all appropriate options below?

N	Training\Learning Methods	
1	Workshops/Inclass	
2	Online	
3	Posters	
4	Regular Meetings	
5	Presentations	
6	Videos	
7	Webinars	
8	Games	
9	Social media	
10	Flyers	
11	Phishing tests	
12	Tip-sheets	
13	Emails	
14	Others (pls specify)	

22-Does this training include any issues or references to social media?

-Yes

-No

-Unsure

Section 4

You never trained/ learn about cybersecurity, but;

23- Which cybersecurity areas do you struggle with the most? (please select all appropriate)

-Privacy and confidentiality

- Password protection

-Phishing

-Email and spam

-Hacking

-Others (pls specify).

24- Please state to which degree you agree with the following statements:

	Strongly disagree	**Disagree**	**Neutral**	**Agree**	**Strongly agree**
Employees must receive training on social media security issues.					
Organizations must have sufficient and clear social media security policy in place.					
Organizations must train their staff to understand their social media policy.					
It is crucial to learn about social media security and risks related to it.					

25-To what extent do you agree with those statements. Cyber security training fails if:

	Strongly disagree	**Disagree**	**Neutral**	**Agree**	**Strongly agree**
It is boring and routine					
It is difficult and includes technical languages.					
It is provided in a one-size-fits all					
Delivery training methods are poor.					
The training environments are limited.					
The trainers are unskillful.					

Would you be happy if the principal investigator contacted you for further details on your answers? If so, please provide the email address that can contact you on.

Thank you„

Interview Questions

The interview consent letter

Dear Participant:

This project examining social media security risks and existing training approaches that help users address these risks more effectively. The interview questions are user-friendly and will require approximately 30-40 minutes to complete. We do not anticipate any risks associated with your participation, but you have the right to stop the interview or withdraw from the research at any time.

Thank you for agreeing to be interviewed as part of this research project. Ethical procedures for academic research undertaken from UK institutions require that interviewees explicitly agree to being interviewed and how the information contained in their interview will be used. This consent form is necessary for us to ensure that you understand the purpose of your involvement and that you agree to the conditions of your participation.

Would you, therefore, read the accompanying information:

-The interview will "audio recorded" in English and it will be via the Zoom application ,and a transcript will be produced

-you will be sent the transcript and given the opportunity to correct any factual errors

-the transcript of the interview will be analysed by (Fai Bensalamah) as a research investigator

- access to the interview transcript will be limited to the supervisory team who might collaborate as part of the research process

-any summary interview content, or direct quotations from the interview, will be anonymized so that you cannot be identified, it will be taken to ensure that other information in the interview that could identify yourself is not revealed.

- all recordings will be deleted once they have been transcribed.

- you have the right to withdraw after two months of your participation only.

The interview questions:

Part A (for all) - Participant details

Participants' Details	
1	Age
2	Gender
3	Education and academic qualifications
4	Job role/Discipline
5	Years of experience
6	What social media platforms do you use, and for how long per day?
7	What is your current social media platform status?
8	Have you ever been trained/taught about cybersecurity?
9	Does this training/ learning include any issues or references about social media?
10	Have you been responsible for the provision of cybersecurity training to employees, or for the formation of cyber security policies in your organization?

Part B – Cyber security and social media security training approaches

If you answered yes in Q10 (Policy makers, training formation):

If you have answered Yes in Q.9 (received training about social media security)

You are policy makers or Training formation/ provision for "Cybersecurity"

1. What social media platforms does your organization use? How important was cybersecurity in the selection of these platforms?
2.Do you feel that your organization controlling and managing their social media accounts effectively/ completely? (pls provide details) / How does your organization manage and monitor their social media accounts? / E.g., do you use specialized/ expert people for this purpose, weekly report etc.,
3.Did your organization expose to any incident because of using social media such as, loss of sensitive data, financial disclosure, brand hijacking, reputation loss, compliance violations, account hacking, or your employee's personal safety being at risk because of using social media? If yes, can you give more details about these incidents, how you deal with them and what lesson you learn?
4.Imagine you want to train your employees about social media risks and how to avoid any incidents related to social media security, what do you think in your experience is the

most appropriate training method/ approach? and why?

Policy Makers Questions

5.Can you give me more details about your social media policy, which are the main aspects it covers?
6.If you have social media policy in place, how important do you consider it to be for your organization and how is it promoted/communicated with employees?
7.Do you measure/check the compliance to this social media policy? If yes, how?
8.What do you consider the main challenges of promoting / enforcing social media policy in place?
9.Does your organization train your employees on this policy? If yes, what kind/ type of training they use for this purpose? And does this policy complement by cyber security training or with other areas of practice? And is this training mandatory for all/some employees?
10.How useful do you think the training is at supporting a social media policy in your organization? / Do you think that training has a significant role in employees 'compliance with this policy?

Cybersecurity Training Provision/ formation Questions

11.If you are a cybersecurity training provider/ formatting, do you feel the need to adjust your training accordingly? E.g., What do you consider, e.g., age, gender, education level etc,. And why?
12.What training approaches does the cybersecurity training use? E.g., online training, workshops, conducting mock attack, sending emails, presentations, posters and etc., and in your experience, what is the most effective training approach for the cybersecurity area?
13.Do you measure the effectiveness of training? If so, what are the main methods you use?
14.Please indicate the main topics that you covered by the cyber security training. Do you feel these topics are sufficient? On what basis are the training topics determined/updated? / Do you have training in social media security topic?
15.What are the main challenges and difficulties of delivering cybersecurity training? For

example, budget, time, noncompliance behavior among employees,

If you have answered Yes in Q.9 (received training about social media security)

1.Can you tell me more about the training course that you attend about social media?
2.Did the training system content meet your original expectations? 'Why or why not?' / Would you take a training like this again without it being mandatory? Why or why not?
3.Do you see that the training topic was relevant to you? / Was the training relevant to your needs?
4.Did you face any challenges, such as; difficulties in engaging, problems in understanding some terms or words, hardness in adapting with the training, challenges in following up with the trainer, disliking the methods used for delivering the training, or the training atmosphere was not helping while applying this training system?
5.Do you feel that your knowledge or skills have improved by taking the training? / Do you feel that your training needs have changed since then? Do you find yourself unsure at times about social media security?
6.Did the training you received involve examples, videos, interactive games, case studies, quizzes, posters, slogans, text descriptions for delivering the information? Could you comment which (if any) you found useful and why?
7.Did the training take place on a regular basis, or on a single occasion? What would be your preference?
8.What would you change to make this training system about social media better?
9.Name the things you enjoyed the most in this training, and the things you did not like.

If you have answered Yes to Q.8 (received training on cybersecurity)

1.Can you tell me more about the training course that you attend about cybersecurity? (Content, format, was it mandatory, satisfaction rating etc.,)
2.Did the training system content meet your original expectations? 'Why or why not?'/ Would you take a training like this again without it being mandatory? Why or why not?
3.Do you see that the training topic was relevant to you? Or was the training relevant to your needs?
4.Did you face any challenges with this training e.g., difficulties in engaging, problems in understanding some terms, hardness in adapting with the system, challenges in following

up, or disliking the methods/approaches used to deliver information while applying this training system?

5.Do you feel that your knowledge or skills have improved by taking this cybersecurity training? / Do you feel that your training needs have changed since then? Do you find yourself unsure at times about cybersecurity?

6.Did the training involve examples, videos, interactive games, group discussions, quizzes, posters, slogans, text description etc., for delivering information? Could you comment which (if any) you found useful?

7.Did the training take place regularly, or on a single occasion? What would be your preference?

8.What would you change to make the training system better?

9.Name the things you enjoyed the most in this training system and the things you do not like.

General questions about social media security and training preferences:

1.Have you experienced any incident while using social media such as loss of privacy, financial disclosure, loss of sensitive data, loss of reputation, hacking, or stealing your identity? If yes, can you provide more details about the incident and how you deal with it?

2.What do you like to learn more about social media security? / What areas in social media security topic do you need improvement on? Or you struggle with the most?

3.What training approach you like more in general, for example, online training, workshops, learning by games, focus activities, lectures, presentations, discussion, videos, tip sheets, posters, attending events, etc., And why? / What type of training you would like to attend even it was not mandatory? And why?

4.In your view, what factors can help in making the training system more effective? /When can you say that this training is effective? / When would you recommend the training system to your colleagues/ friends? E.g., the trainer is skilled, the topic attractive or relevant, the objectives are important, or may be the time or duration is suitable for you?

5.Imagine you want to train about social media security, what do you think is the most appropriate training approach and delivering information methods for social media security topic? And why?

6.In your view, what are the opportunities that should the social media security training

system provides?

7.In your opinion, how can management improve their employee's social media security awareness in an organization? / Imagine you own a company, and you want to control your employees' behavior on social media. What would you do about that?

8.Do you think that having social media policy in organizations is a good idea to control employees' behavior online? Why and why not?

9.In your opinion, what is the best method to measure the effectiveness of social media security training? / How can management measure the effectiveness of social media security training?

10.In your opinion, how can employees adapt to the training system more effectively? E.g., formatting different training for different groups, using methods to attract them, etc.,

Social Media Cybersecurity Diagnostic Test

Dear Participants

This project examines social media security risks and existing training approaches that help users address these risks more effectively.

We do not anticipate any risks associated with your participation, but you have the right to stop the participation or withdraw from the project at any time.

Thank you for agreeing to be part of this experimental study. Ethical procedures for academic research undertaken from UK institutions require that participants explicitly agree to be interviewed and how the information contained in their study will be used. This consent form is necessary for us to ensure that you understand the purpose of your involvement and that you agree to the conditions of your participation.

Would you, therefore, read the accompanying information:

-The assessment will be in English and translated into Arabic for all the questions.

-The second step of your participation will be a training session tailored uniquely to you, and the training session will be held in Arabic by the author (Fai Bensalamah),

-The outputs of the survey and the training feedback will be analysed by (Fai Bensalamah) as a research investigator.

-Post-training assessment will be held with the same initial quiz. Along with another short online survey to assess your feedback.

-Access to the data transcript will be limited to the supervisory team, who might collaborate

as part of the research process,

-Any summary content, or direct quotations from the training session, will be anonymized so that you cannot be identified; it will be taken to ensure that other information in the training that could identify yourself is not revealed.

-All recordings will be deleted once they have been transcribed.

-You have the right to withdraw after two months of your participation only.

Email Address:

Section one: Target group

1-Please, select from the list below the sector in which you are currently working (choose as many as apply):

	Education , Training, and Libraries
	Healthcare support
	Leadership and Management
	Business and Financial operations
	Arts, Design, Entertainment, Sport and Media
	Office and Administrative Support
	Military such as, the Army and Police
	Others, pls specify...

2-Are you responsible for the social media accounts within your current company?

3-Your gender?

4-How old are you?

5-Your Education Level?

6-How many years of experience do you have in your field?

7-How much time do you spend on social media per day approximately?

Section Two: Generic cybersecurity questions

1-Asuming you are visiting your social media website from your browser, what should you do before you login with your email and password?

	Send an email to the IT staff of the website
	Check the website URL
	Check the contact details on the website
	Check the Wi-Fi connection I am connected to
	None of the above
	I don't know

2-Which of the following social media account passwords would you prefer? (You can choose more than one option)

	Password123456$$
	Luke1985
	Password@Password
	Jelly22fi$h
	GladiatorPoolGeese
	None of the above options
	I don't know

3-What tool could you use to create strong, unique, long, and hard-to-guess passwords? (You can choose more than one option)

	Your company's VPN
	Google forms
	Using a safe password manager
	Antivirus software
	None of the above options
	I don't know

4-What is the correct definition for Two-Factor authentication (2FA)?

	Authentication mechanism based on the assumption that the number of failed logins for suspicious users increases by a factor of two in comparison to legitimate login requests.
	Authentication mechanism based on two biometric data inputs at the beginning and end of each session.
	Authentication mechanism, where users are requested to provide two pieces of evidence to prove their identity
	None of the above options
	I don't know

5-Have you enabled two-factor authentication feature on your social media accounts yet?

-Yes

-No

-I don't know

If you answered no, can you tell us why not?

6- Your social media account can be compromised (hacked) if you are on a compromised network.

-True

-False

-I don't know

7- Which of the following best describes what you would do first, when realising that your social media account has been hacked?

	Restart your device and clear app history
	Turn off the network and stop using the device
	Notify your friends your account has been hacked and ask for their help
	Reset your password and enable 2FA
	None of the above options
	I don't know

8-Some internet browsers have security weaknesses that might make you vulnerable to hacking on social media.

-True

-False

-I don't know

9-Suppose you find someone on social media pretending to be something or someone that doesn't exist. What should you do?

	Ignore it; nothing wrong will happen.
	Report it to the social media platform
	Contact him to double-check
	None of the above options
	I don't know

10-You should check that you are using the latest version of your social media accounts to prevent hacking?

-Yes

-No

-I don't know

Section Three: Training Preferences

1-Which of the following best describes your training preferences on social media cybersecurity? (Choose as many as apply)

	Workshop/in-class training
	Online training
	Posters
	Short presentations
	Video
	Games
	Social media posts
	Flyers
	Phishing tests
	Tip sheets
	Email
	Others (pls, specify)

Section Four: Social Media Usage

1-What is your preferred social media platform?

	Facebook
	Twitter
	YouTube
	Instagram
	Snapchat
	LinkedIn
	TikTok
	Tangler

Depending on their choices, participants will be led to each social media questions.

Assessing Facebook user's best practices (5 questions)

1-How could you know that your Facebook account had been hacked? (Please, select as many as apply)

	I can't open my device
	My email has been changed
	Battery draining quickly
	Friend requests have been sent to people you don't know
	Your birthday has been changed
	Non of the above
	I don't know

2-Is it possible to find who is looking at your Facebook profile and tracking you?

-Yes

-No

-I don't know

3- Can you select an audience for every post you share on Facebook?

-Yes

-No

-I don't know

4-You can report a fake account on Facebook by?

	Privacy and security section
	Clicking on the fake account profile and choose Report
	Calling Facebook
	Sending an email to my company's IT staff
	Non of the above
	I don't know

5-What should you do if you find that there is a Facebook account or Page pretending to be you?

	Contact the fake account directly and ask them to stop
	Getting in touch with the fake account by email
	Ignore it
	Report the incident to Facebook
	Non of the above
	I don't know

Assessing Twitter user's best practices- 5 questions

1-How can you report incidents on Twitter (choose as many as apply)?

	Calling the IT staff in your company
	Visit the Help Centre on the Twitter website
	Calling Twitter by phone
	Select the individual Tweet and click on Report
	Non of the above
	I don't know

2-How can you make the tweets that you post on Twitter 'Private'?

	By modifying the security options on your profile page
	By modifying the settings on the privacy page
	By visiting Twitter's Help Center
	I cannot make Tweets private
	Non of the above
	I don't know

3-How could you know that your Twitter account has been compromised (hacked)? You can select more than one option.

	When you notice your password is no longer working, and you are being prompted to reset it
	Your mobile phone switches off suddenly.
	You receive a notification from Twitter stating that your account information has changed, and you didn't change it
	Your battery goes down quickly
	You observe other account settings that you didn't choose (like following, unfollowing, or blocking)
	I don't know

4-How can you report that someone is impersonating you on Twitter?

	Report it to the IT staff in your company
	Report it to your specialist friend
	Select the account that is impersonating you and choose Report
	Send an email to Twitter team
	None of the above
	I don't know

5-To avoid phishing on Twitter, you should (choose as many options as apply):

	Avoid using Twitter for too long
	Limit the number of tweets you post
	Limit the number of tweets you like
	Check the spelling of URLs before clicking on them.
	None of the above
	I don't know

Assessing YouTube's users best practices- 5 questions

1-How could you know that your YouTube account has been compromised (hacked)? You can select more than one option.

	When you notice your password is no longer working, and you are being prompted to reset it
	Your mobile phone switches off suddenly.
	You receive a notification from YouTube stating that your account information has changed, and you didn't change it
	Your battery goes down quickly
	You observe other account settings that you didn't choose (like downloading's videos, or subscribing channels)
	I don't know

2-How could you change your video privacy settings on your YouTube account?

	By modifying your Privacy and Security options
	By modifying your Settings options
	By signing in then modifying your Content options
	None of the above
	I don't know

3-What should you do if you can't sign into your YouTube channel?

	Restart your device
	Reinstall the YouTube app
	Go to the account recovery page
	None of the above
	I don't know

4-What should you do if you find videos on YouTube that you think might be spam or phishing?

	Ignore them
	Report my friends
	Flag them for review by YouTube team
	None of the above
	I don't know

5-To avoid phishing on YouTube, you should (choose as many options as apply):

	Avoid using YouTube for too long
	Limit the number of videos you post
	Check the spelling of URLs before clicking on them
	Limit the number of subscribing videos
	None of the above
	I don't know

Assessing LinkedIn user's best practices- 5 questions

1-How can you protect your LinkedIn account? (Choose as many options as apply)

	Limit the contents of your posts
	Use a fake profile picture
	Avoid using public networks
	Avoid re-using the same password across different websites
	Avoid accessing LinkedIn from your PC
	None of the above
	I don't know

2-Is it important to update the phone number and email associated with your LinkedIn account for security reasons?

-Yes

-No

-Idon't know

3-How could you know that your LinkedIn account has been compromised (hacked)? (Choose as many as apply)

	When you notice your password is no longer working, and you are being prompted to reset it
	Your mobile phone switches off suddenly.
	You receive a notification from LinkedIn stating that your account information has changed, and you didn't change it
	Your battery goes down quickly
	You notice other account settings that you didn't choose (like following, unfollowing, or blocking)
	I don't know

4-How can you report an incident on LinkedIn? (Choose as many as apply)

	Report the incident to friends through any other communication methods
	Report the incident to the LinkedIn Team through their website
	Report the incident to LinkedIn by phone call
	Report the incident to LinkedIn through sending an email
	None of the above
	I don't know

5-What should you do if you find contents on LinkedIn that you think might be spam or phishing?

	Ignore it
	Report it to my company's IT staff
	Report it directly on the site
	Restart my device
	None of the above
	I don't know

Assessing Snapchat's users best practices- 5 questions

1-You can only report accounts but you cannot report stories that you see as inappropriate.

-True

-False

-I don't know

2-How can you report an incident on Snapchat?

	Through sending an email to Snapchat
	Through calling Snapchat by phone
	Through the snapchatter's name
	None of the above
	I don't know

3-How can you hide your location on Snapchat?

	Through the block option
	Through the custom option
	Through the ghost mode option
	Through the security & privacy option
	None of the above
	I don't know

4-How do you know if your Snapchat account has been compromised (hacked)? (You can choose more than one option)

	Your device switched-of suddenly
	You have had to continually re-log into the app
	The device battery drained fast
	A new contact has been added to your list without your permission
	None of the above
	I don't know

5-You must verify that the email and mobile number associated with your account are accurate to keep your Snapchat account secure.

-True

-False

-I don't know

Assessing Instagram's users best practices - 5 questions

1- What should you do if someone creates an Instagram account pretending to be you?

	Ignore it
	Report it to Instagram
	Change your password
	Report it to IT staff in your company
	None of the above
	I don't know

2- Is it important to update the phone number and email associated with your Instagram account for security reasons?

-Yes

-No

-I don't know

3-How can you report an incident on Instagram? (You can choose more than one option)

	Report through a phone call
	Report through SMS
	Report directly the post or message
	Report someone through their profile
	None of the above
	I don't know

4-Can you identify who has recently logged into your Instagram account?

-Yes,I can

-No, I can't

-I don't know

5-After making your account private, what can you do to prevent your followers from seeing your posts?

	Tell them to unfollow me
	Block them
	Report them as spam
	Ignore them
	None of the above
	I don't know

Assessing TikTok's users best practices

1-How can you limit the audience of your videos in TikTok?

	By modifying your privacy settings
	By modifying your home page settings
	By modifying your profile settings
	None of the above
	I don't know

2-Can you apply different privacy settings to each video you share on your Tiktok profile?

-Yes

-No

-I don’t know

3-What are the suspicious links and messages that you should be aware of and report immediately? (Choose as many as apply)

	Requests to follow someone else’s social media account
	Your friend asking to follow you
	Questionable links or content
	QR codes appearing in someone’s profile of video
	None of the above
	I don’t know

4-Can you report a comment you have come across on Tiktok?

-Yes

-No

-I don’t know

5-What should you do if you find contents on Tik Tok that you think might be spam or phishing?

	Ignore it
	Report it to my company’s IT staff
	Report it directly on the site
	Restart my device
	None of the above
	I don’t know