An Alternative Approach to Information Security Awareness Training to Reduce Human Errors

****

A project submitted to Middlesex University

in partial fulfilment of the requirements for the degree of

Doctor of Professional Studies (DProf)

(Computer Communications Engineering – Information Security)

Lukman Sharif

Institute for Work Based Learning

Middlesex University London

January 2022

Table of Contents

List of Figures & Tables

Abstract

Information security (InfoSec) is concerned with protecting the confidentially, integrity and availability of information and information systems. InfoSec has traditionally been considered a technology problem with much attention often focused on technical solutions. However, technology alone cannot deal with all InfoSec risks. Research shows that an overwhelming percentage of InfoSec breaches are caused by human errors. It is ultimately the end users in any organisation that are the primary line of defence.

Whilst security breaches can be attributed to a variety of factors, inadequate user awareness training always features prominently. Awareness training programmes are often identified as a key contributor to changing user behaviour in order to achieve optimum security. However, research shows that whilst many organisations implement such programmes, security breaches resulting from human errors are still rampant which calls into question the effectiveness of existing InfoSec awareness programmes. This encapsulates the phenomenon that is the focus of this study.

This phenomenological study investigated the shortcomings in existing InfoSec awareness training programmes (vis-à-vis human errors) based on a literature survey of internationally peer-reviewed books, professional practice literature, journal papers, articles, policy documents and global security surveys. In addition, semi-structured, in depth, open-ended interviews were conducted involving eight InfoSec academics and practitioners to understand their lived experiences and perspectives about the phenomenon in question. The research participants were encouraged to share their experiences of researching InfoSec threats and countermeasures as well as implementing and managing InfoSec awareness training programmes. The experiences shared by the participants offered valuable and practical insights into important issues surrounding human factors contributing to human errors, nature of security threats, the psychological aspects of human behaviour and factors contributing to the ineffectiveness (and effectiveness) of awareness training programmes.

Interpretive Phenomenological Analysis (IPA) was used to analyse participants' responses to interview questions in order to help answer the research question. The analysis culminated in the formation of valuable and practical guidelines, corroborated by academic, industrial, and professional practice research literature as well as my own professional knowledge and experience. The guidelines offered here will help to improve the processes and practices used to develop and implement effective InfoSec awareness programmes and can be built into future awareness programmes to reduce security breaches resulting from human errors. The guidelines will benefit a range of groups within my professional community including myself, InfoSec academics, InfoSec practitioners, organisational leaders, managers, chief information officers, chief information security officers, systems administrators, and end users. The outcome of this study contributes to the scientific knowledge and understanding of an important phenomenon and offers InfoSec researchers a springboard for further explorations into issues related to InfoSec awareness training and human behaviour. The essences of the experiences shared by research participants in this study also serve as a catalyst for further research.

Acknowledgements

The process of completing a project of this nature is rarely an entirely independent endeavour. I would like to take this opportunity to express my sincere gratitude to all the people who have helped me during this tremendous journey.

I am deeply indebted to Dr Mehmetali Dikerdem, my principal advisor, for his continued support, guidance, and kindness throughout the process. His encouragement and insightful feedback added tremendous value to this project.

I am very grateful to Dr Penny Duquenoy, my consultant, for her valuable feedback and guidance throughout this project.

I am immensely appreciative of all the research participants who took time out of their busy schedules to participate in this research. Without their enthusiasm, cooperation, and flexibility this project would not have been possible.

I would like to thank the DProf administration team for their support, especially Stephen Watt, for his cooperation and professionalism.

I am grateful to my family and friends who supported me and encouraged me to complete this project.

Finally, I am extremely grateful to my wife and children for their support, patience, and love during this journey.

Chapter 1: Introduction

Overview

This chapter provides a general background to this project, the proposed research problem and its importance within the wider research area and my professional field of practice. I briefly discuss my professional background and influential factors within my professional practice that have led to the emergence of the research question and the subsequent aim and objectives of this project. I also offer a reflection on the personal and professional significance of this project.

As an overview, chapter 2 provides a literature review, offering a theoretical framework that this research study is built on and that can be further extended to achieve the objectives of this project. Chapter 3 provides a critical discussion of the research methodology I have used in this project and my justifications for the choice of this particular methodology. My stance as an insider practitioner-researcher is considered and how this has affected my overall approach to this project, including the choice of research methodology. Chapter 4 details the project activity by applying the theoretical and philosophical principles of phenomenology from chapter 3 to describe the process of data collection (interviews) and data analysis. Chapter 5 attempts to make sense of the data gathered in the previous chapter and presents the findings through a discussion and interpretation of the results in light of relevant literature and my own professional knowledge and experience. Chapter 6 presents the findings in a coherent and meaningful way, in the form of guidelines intended to help improve the processes and practices used to develop and implement effective InfoSec awareness programmes. This chapter also discusses the value of the project, the applicability of the outcome to my field of practice and the stakeholders. The limitations of this project and recommendations for further research are also discussed. Finally, I reflect on the overall project journey and future directions and translation of the findings to a wider context within my field of practice.

1.1 Setting the Scene

In recent years, the field of InfoSec has received much attention, often as a consequence of an increasing number of security breaches that have resulted in major organisational and economic losses. Although in many cases technical solutions exist to counter such security breaches, technology alone cannot deal with all InfoSec risks (Cisco, 2021). InfoSec has traditionally been considered a technological issue with much attention often focused on technical solutions. However, since computers are operated by people, ultimately human behaviour will influence how people interact with information technology and the impact this will have on the security of such systems. Human behaviour is often described as the weakest part of a security system and users are often referred to as the weakest link in the security chain **(**Bada, Sasse and Nurse, 2019**).**

Human behaviour, beliefs, attitudes and their ultimate decisions represent a conundrum to be deciphered by cybersecurity experts (Cano, 2019). Consequently, human factors have become a major concern in the field of InfoSec. Human factors in cybersecurity represent the actions (and inactions) or events when human error results in a successful security breach (Hughes-Lartey *et al*., 2021).

In a sense, human factors are a side effect of the information technology success story. An ever-increasing number of businesses and households in the UK and all around the world make extensive use of information and communications technologies (ICT). With an increasing drive by governments around the world to move their services online, ordinary citizens without the technical knowhow are at risk of being deprived of the benefits offered by ICT. When it comes to technology, one thing we can be sure of is that nothing remains the same. Technology is always evolving to meet the ever-changing demands of a fast-paced society (Rock, 2018). Given the speed of technological change, it is hardly surprising that there is a knowledge and skills gap – both in terms of technology and specifically in terms of InfoSec. This gap affects individuals and organizations (Naden, 2021).

The role of InfoSec awareness training programmes is often highlighted as being crucial in promoting learning and participation that can be applied to manage human behaviour in organizations (Bada, Sasse and Nurse, 2019; Legárd, 2020; Cisco, 2021; Gardner and Thomas, 2014; Wilson and Hash, 2003). The focus of such programmes is on the need to educate and persuade users to think and act in a security-conscious way (CybSafe, 2021) since the people in any organization are the most critical line of defence (Brodie, 2008). This fact has been acknowledged in the international InfoSec management framework embodied in ISO/IEC 27001/27002 Requirement 8.2.2 (ISO/IEC, 2013), European General Data Protection Regulation (GDPR) Article 39:1:b (Art. 39 GDPR, 2018), National Institute of Standards and Technology (Wilson and Hash, 2003) as well as other related best practices. My own professional experience of more than fifteen years in the field has taught me that the security of an organisation is very much dependent on the knowledge and awareness of the end users and those who manage them.

Many of the high-profile security breaches world-wide in the recent past have been the result of simple human error (PwC, 2020; Ernest & Young, 2020; Deloitte, 2020; CrowdStrike, 2021; Cisco, 2021; ISACA, 2019). The real tragedy is that such security breaches will continue to take place due to the way the security industry has traditionally approached the problem. Despite the fact that huge sums of money are spent on IT infrastructure projects and state of the art security solutions, most organizations remain inherently vulnerable to the most basic of security threats (PwC, 2020; Deloitte, 2020). This is largely due to the fact that far too much attention is focused on the technology and comparatively little attention is given to the human factors (Legárd, 2020; Gardner and Thomas, 2014; Bada, Sasse and Nurse, 2019).

The Global Security Surveys carried out by Ernest & Young (2020), Deloitte (2020), PwC (2020), CrowdStrike (2021), Cisco (2021) and ISACA (2019) all highlight a growing appreciation and increased financial investments among organizations in security awareness training. Despite this fact, the surveys also reveal that security breaches involving human factors and insider user threats are still rampant. It is evident that issues persist with managing human behaviour despite the efforts of organizations to put in place suitable security awareness programmes.

This project investigates the shortcomings in existing information security awareness training programmes and seeks recommendations and solutions to address the shortcomings in order to reduce human errors.

This study aims to propose an alternative approach to InfoSec awareness training on the basis of a) literature survey of internationally peer-reviewed books, professional practice literature, journal papers, articles, policy documents and global security surveys b) engagement with InfoSec academics and practitioners to determine the shortcomings in existing awareness training programmes and offer recommendations and possible solutions to address these shortcomings.

This research will employ a qualitative (phenomenological) research approach to conduct interviews with InfoSec academics and practitioners involved in the research, design and implementation of InfoSec programmes. The contribution of academics and practitioners is crucial to the success of this project due to their expertise in this area of InfoSec.

The principal output of this project will be a set of guidelines that will help to improve the processes and practices used to develop and implement effective InfoSec awareness programmes and can be incorporated into future awareness programmes to reduce security breaches resulting from human errors.

The outcome of this study will benefit a range of groups within my professional community including myself, InfoSec academics, InfoSec practitioners, organisational leaders, managers, chief information officers, chief information security officers, systems administrators, and end users.

1.2 Project Background & Context

I have been working in the Computer Communications and Information Security industry for over fifteen years. During this period, I have worked in a variety of highly technical and leadership roles including Chief Technical Officer, Head of Training & Consultancy and Senior Network Consultant. This project will be undertaken within my current role as a Network Security Solutions Architect, Senior Trainer in InfoSec and a Researcher. The specialist focus of my DProf research project is in the field of Computer Communications Engineering and InfoSec.

The role of human factors in InfoSec has been a recurring theme in my career over the years (Appendix J) and it is an aspect of my professional practice that I intend to research and develop further. I have spent a significant part of my professional career trying to convince ICT users about the value of InfoSec awareness and adhering to good security procedures and practices in their everyday personal and professional lives. In my experience, the vast majority of users are sensible, honest and hardworking people who are all too willing to comply with security policies and procedures as long as they are given easy to follow guidelines and advice on the benefits of compliance.

This research project is an effort to consolidate and further enhance my understanding of the complex issues surrounding human behaviour and organisational InfoSec awareness training programmes. I believe that there is a need for an integrated approach to understanding human behaviour in this field as well as an understanding of how awareness training programmes can be improved to achieve the desired change in user behaviour. Such an approach is intrinsically transdisciplinary because it requires insights from InfoSec researchers, practitioners, computer scientists, communications engineers, psychologists, sociologists and philosophers, among others, to understand and address the human factors in InfoSec (Sasse et al, 2007).

I consider my own personal and professional experience, technical knowledge and research background (Appendix J) as an indispensable part of my DProf research. Kemmis (2010) quotes Eraut (1994) and Higgs, Titchen and Neville (2001) who suggest that professional practice knowledge can be described in terms of: 1: propositional, theoretical or scientific knowledge, 2: professional craft knowledge and 3: personal knowledge about oneself as a person and in relationship with others. I believe that my professional practice has elements of all three categories of knowledge, helping me to form my own unique perspective in my approach to this project.

The practitioner-researcher dual role is complex and requires conscious adoption of specific approaches. However, the insider practitioner-researcher role does not strive to make claims to objectivity as defined by standard positivist approaches to research. This approach is already committed to a certain kind of change (the impact I intend to make) and to research process integrity (transparency in the choice of appropriate methodologies and data collection) as well as the ethics of research and its outcomes.

As an InfoSec practitioner-researcher, I am part of the same professional community as the research participants and therefore I cannot consider myself to be a detached outsider during the research. My own experiential knowledge and beliefs constitute a vital part of the project. The insider practitioner-researcher approach takes into account the subjectivities which rise as a result of my own positionality, the values, perspectives, understandings (and misunderstandings) I bring into the research process (Holliday, 2002).

Although it is impossible for me to eliminate my own theories and beliefs during the research, I will focus on trying to reduce the impact of such validity threats on my findings by making my core values and research interests transparent and accountable.

From an ontological and epistemological perspective, my past professional and research practice has been predominantly rooted in a positivistic research paradigm (Appendix J), trying to understand various phenomena through mainly quantitative approaches. Costley and Armsby (2007) observe that practitioner-researchers tend to base their research in methodologies and epistemologies accepted and traditionally used within their professional field.

With an increasing recognition of the role of human behaviour, the field of InfoSec has sought insights from the social science domain. My own professional and research practice has followed a similar trend with a shift in focus from a predominantly technical approach to one that is more socio-technical in nature, recognising that InfoSec is both a human and technological problem.

This research project will be based on a qualitative (phenomenological) investigation and I would argue that this type of methodology is not commonly used in InfoSec research. I have decided to use this methodological approach as I believe it will allow me to unlock and understand the complex human behavioural contexts involved in this research.

I have chosen to pursue research in the above-mentioned area as I believe it will allow me to attain the knowledge and experience I need to make a personal contribution to my profession and community of practice.

1.3 Aim, Objectives and Outcomes

Given the background and context of this project, the following research question was formulated:

- *What are the main shortcomings in existing information security awareness training programmes and how can these be addressed in order to reduce human errors?*

The main aim of this project can be summarised as follows:

- *To propose an alternative approach to information security awareness training to reduce human errors.*

The research question, along with the aim, can be broken down into the following objectives:

1. *Establish the main shortcomings in existing InfoSec awareness training programmes (vis-à-vis human errors) on the basis of a literature survey and engagement with InfoSec academics and practitioners*
2. *Determine possible solutions to help make InfoSec awareness training programmes more effective (vis-à-vis human errors) based on engagement with InfoSec academics and practitioners*
3. *Assess the validity and reliability of the proposed solutions (that emerge from objective #2) by corroboration with existing literature and own experience*
4. *Derive practical guidelines that can be incorporated into future InfoSec awareness training programmes to reduce human error*

1.4 Personal and Professional Significance of this Project

This DProf project will be designed to inform and add value to my professional practice. The research carried out will be informed by a broad knowledge of computer communications engineering and InfoSec (Appendix J), beyond that of my community of practice. The project will allow me to attain the knowledge and experience that I need to make a personal contribution to my profession and community of practice.

As can be gleaned from the project objectives, the principal output of this project will be a set of guidelines that can be incorporated into future InfoSec awareness training programmes in order to reduce security breaches resulting from human errors. These guidelines will be derived from the collective knowledge, experiences and insights shared by InfoSec experts (academics and practitioners) and corroborated by academic, industrial, and professional practice research literature as well as my own professional experience.

As a professional practice-based project, this research is motivated by real business drivers. Consequently, the guidelines will be grounded in real business needs and concerns and are expected to have an immediate, direct and tangible impact on my profession and community of practice. It is possible that some of the recommendations may require further deliberations in accordance with the unique business contexts and therefore implementation and impact of the research findings is expected to take place over an extended timescale.

The proposed guidelines will help me to make a significant contribution to my community of practice. The personal learning that I will achieve will be fed back into my professional practice in order to enhance my expertise in the field of InfoSec and to create a more defined niche for myself within my community of practice.

The DProf project will give me the opportunity to improve my scholarly abilities and skills both academically and professionally. The personal learning and the findings of the project will be disseminated through academic and professional journals and seminars in order to engage with a range of current issues and debates in the field of InfoSec awareness training and professional practice. The research findings will also form the basis for future InfoSec awareness training courses that I will be able to offer as part of training and consultancy services.

I feel privileged to be able to bring to the programme my own mix of skills and experience to work with in order to develop my research and have the opportunity to make a positive contribution to my community of practice. I believe that the rigorous and challenging process of undertaking a DProf will give me a competitive edge and greatly improve my career prospects. It will also give me the opportunity to further develop myself and play a strategic thought leadership role in my chosen area of InfoSec research.

1.5 Project Audience & Stakeholders

The outcome of this study will benefit a range of groups within my professional community including myself, InfoSec academics, InfoSec practitioners, organisational leaders, managers, chief information officers, chief information security officers, systems administrators, and end users (at home and at work).

InfoSec academics: This group will participate in the data gathering phase of this project, making them an obvious audience and stakeholder. InfoSec academics are professionals working in a variety of academic and research-oriented environments such as universities, research institutes and laboratories. InfoSec academics keep up to date on the latest developments in information security threats and investigate and analyse their capabilities. They also attempt to understand the cybersecurity threat landscape, predict latest trends and attack vectors and develop and recommend appropriate security responses and standards. A particularly crucial aspect of their role is research into human factors of InfoSec and psychological models of human behaviour to identify potential factors that could lead to the success/failure in changing user behaviour. Consequently, they are ideally placed to offer valuable insights into how security awareness training can help to manage human behaviour more effectively.

InfoSec practitioners: This group will also participate in the data gathering phase of this project, making them an obvious audience and stakeholder. InfoSec practitioners provide strategic, tactical and operational oversight of an organisation's InfoSec operations. Their role includes ensuring that the business understands the importance of security and adherence to policies as well as identifying weaknesses in existing efforts and ensuring that adequate resources and processes are in place to continually update and strengthen safeguards against internal and external security threats. InfoSec practitioners can assume a variety of job titles including InfoSec specialist, InfoSec architect, InfoSec analyst, InfoSec awareness training specialist and chief information security officer (CISO). The implementation of robust and effective organisational InfoSec awareness training programmes is an integral part of their role.

Organisational leaders, managers, chief information officers (CIO): This group is in charge of securing the assets of their organisations and institutions. They have the authority to sanction security awareness training initiatives, to ensure that security policies are enforced, and regular monitoring systems are in place. CIOs generally assume a very strategic role, reporting directly to the CEO and often have a seat on the executive board.

Chief information security officers (CISO) and systems administrators: The CISOs tend to assume a high-level role and are responsible for all things security in the organisation. Their responsibilities include developing and managing an organisation's security program and providing training to all staff on security protocols. The role of systems administrators includes management and support of the IT infrastructure at multi-user organisations to ensure availability, performance and security of all systems in order to meet users' needs.

End users: Most people in developed countries and a rapidly growing number in developing countries have Internet access, either at home, work, or through providers such as Internet cafes, etc. End users (at home and at work) are always at risk from viruses, intruders and hackers when connected to the Internet. In order to manage human factors effectively, all stakeholders need to be involved in the design and operation of security systems. All parties need to communicate effectively about security risks and their roles and responsibilities in managing and enhancing security.

Summary

This chapter offered a general background to this project along with the proposed research problem and its importance within the wider field of InfoSec. I briefly discussed my professional background and important factors within my professional practice that have led to the emergence of the research question and the subsequent aim and objectives of this project. I concluded the chapter by reflecting on the personal and professional significance of this project.

Chapter 2: Literature Review

Overview

The purpose of this chapter is to provide a theoretical framework that this research study is built on and can be further extended to achieve the objectives of this project. This chapter offers a discussion of InfoSec ontology and awareness training as a crucial and evolving aspect of InfoSec. The field of InfoSec is vast and therefore it is important to establish the boundaries of this project. For the purpose of simplicity and coherence, this chapter has been divided into two main sections. The scope of each section is outlined at the start of the section.

The research topic of this project is vast and evolving and this literature review is not intended to provide an exhaustive discussion on every aspect of this area of research. As a practice-based doctorate, this project will endeavour to focus on only the specific research area and texts that are relevant to my professional practice-based approach.

Traditionally, the aim of the literature review is to reflect the current state of play in the chosen area of research in order to identify limitations and help the researcher to pinpoint a gap which the proposed research question can then address. As such, traditional research studies tend to incorporate substantive review and acknowledgement of how existing research has informed what is to be studied.

Within academic and professional practice literature, the scope and the position of a literature review in a phenomenological study has been the subject of some debate. According to Vagle (2014: 73), the role of theory (in the form of a literature review) in phenomenological studies has been tenuous. In stark opposition to positivism, Husserlian phenomenology espouses a vision of a foundation for all social sciences that strongly resists the idea of theory testing and theoretical explanations and predictions. Vagle (2014: 74) points out that the Husserlian approach regards the human experience as too complex and fluid to be captured or constrained by a theory. As such, no theory, regardless of how well constructed or agreed upon in a scholarly field, should be used as the basis to determine how the human participants experience the world.

Smith, Flowers and Larkin (2009:112) assert that in IPA studies, the research question (and any subsequent interview questions derived from it) are not usually theory driven. The literature review in IPA studies attempts to provide a big picture of the major issues related to the research area / phenomenon. Consequently, this kind of literature review is short and aims to introduce readers to the field, the phenomenon of interest, what useful contribution the study can make and how the phenomenon will be examined (Smith, Flowers and Larkin, 2009: 43).

Smith, Flowers and Larkin (2009:42) argue that in IPA studies, there is a commitment to a degree of open-mindedness during the data collection (interviews) stage which necessitates suspension of researcher's preconceptions. The aim is to facilitate the participants to communicate their concerns and make their claims on their own terms. Although, it is acceptable to have some idea of what form such claims are likely to take, an exhaustive literature review of the phenomenon prior to data collection phase is likely to jeopardise the open-minded approach called for.

Vagle (2014: 71) notes that whilst it is in the researcher's interest to be familiar with the relevant literature, it is not advised to 'read too much' existing literature as 'knowing much' about the very phenomenon can make it hard for the researcher to 'see something new'.

According to Dahlberg, Dahlberg, and Nystrom (2008), there is a concern that an exhaustive review of literature could compromise the researcher's openness to what might be learnt from the phenomenological inquiry. Vagle (2014: 71) warns that in phenomenological studies, a thorough literature review could 'settle' matters before the study is even conducted.

Whilst from a traditional research perspective, it makes sense to conduct a thorough literature review, in phenomenological studies (such as IPA), it could jeopardise the researcher's 'philosophical and methodological commitment' to remain open to the phenomenon (Vagle, 2014: 72).

Whilst bracketing preconceptions and theories in data collection and early analysis is a non-negotiable commitment in all phenomenological traditions, Vagle (2014) argues that researchers should also bring important theoretical understandings from their scholarly fields (e.g. InfoSec awareness training) to weigh in during the later data analysis and writing up phases. During this phase of an IPA study, there is a change of register, and the research findings are placed in a wider context by engaging in a dialogue between the findings and the existing literature. In other words, there is a return to the literature (this chapter) in order to understand how existing work sheds light on what has been found. How do the findings illuminate or problematize what other studies in this field say? (Smith, Flowers and Larkin, 2009:112)

However, given the nature of IPA studies, it is likely that the outcome of interviews and analysis leads into unanticipated territory e.g., the emergence of themes which were not anticipated by the interview schedule. Smith, Flowers and Larkin (2009:113) point out that this will require additional literature at this stage in order to frame the new angles that have emerged. As such, there is no issue with introducing some literature for the first time during the qualitative write-up phase. However, this engagement with new literature is very selective. Vagle (2014: 74) argues that this engagement with data by returning to theories is an acknowledgement that the work of a researcher is to contribute to ongoing theorising.

In summary, whilst bracketing preconceptions and theories is an integral part of data collection and early analysis in a phenomenological study, using the same bracketed theories (literature review) during later analysis and discussions in order to situate the work in wider context is equally important.

Based on the above discussion about the scope and the position of a literature review in a phenomenological study, I agree that a literature review of some sort is necessary to help shed light on the phenomenon of interest. However, I feel that an exhaustive literature review at this stage of the project will distract me from the important task of exploring the phenomenon.

Following Vagle’s (2014: 72) advice, I have opted for a partial review of the literature in order to strike a balance between the customary research practice (of exhaustive literature review) and not constructing a priori explanation of what the phenomenon ‘is’ or ‘should be’ according to pre-existing theoretical explanations.

My focus is therefore on providing a literature review that attempts to offer a ‘big picture’ of the major issues related to InfoSec awareness training programmes and makes connections across the broad related areas to enable the reader to develop a sense of the phenomenon of interest and the significance of the research.

This literature review draws upon up-to-date InfoSec research publications, books, journals, conference proceedings, articles, industry surveys as well as professional practice literature, making use of electronic database journals, such as JSTOR, Springer, IEEE, Science Direct, Emerald and ACM.

As mentioned briefly in the previous chapter (and discussed in greater detail in the next chapter), this study seeks to understand the phenomenon of the effectiveness (or lack thereof) of InfoSec awareness training programmes as experienced by InfoSec professionals (academics and practitioners) through interpretative phenomenological analysis (IPA). The goal of the research is to understand the participants’ individual meanings that develop after reflecting on their role as it relates to InfoSec awareness programmes and other interrelated themes.

I am confident that the literature review presented here is adequate and effective in establishing familiarity with the current research in the area as well as professional practice concerns in order to help place this study within the context of existing literature and making a case for further research in this area. Specifically, this chapter will help to highlight the point that shortcomings persist in existing InfoSec awareness training programmes and the fact that this issue has not been adequately addressed in existing academic and professional literature.

This chapter concludes with a problem statement, confirming that a real problem exists, it is important, this research is necessary, and that the research design is viable and will help to solve the problem.

Section 1

This section sets the scene by providing a general overview of the InfoSec landscape and the most widely known security standards. The subtle differences between human factors and human errors are highlighted and Reason's classification of human errors along with the main categories of human errors considered in the InfoSec literature are briefly discussed.

A more focussed discussion of human errors follows with specific examples of some of the most common examples of human errors in InfoSec. This leads to a general outline of the most common security breaches followed by specific examples of some recent high profile security breaches resulting from human error.

A discussion of the various costs (loss of revenue, regulatory fines, loss of customer confidence, reputational damage) associated with security breaches resulting from human error is provided with up to date supporting statistics from the highly regarded Ponemon Institute, the UK Department for Digital, Culture, Media and Sport (DCMS) Cyber Security Breaches Survey and the Kaspersky Security Risks Survey. These surveys also reveal insights into the most common human factors contributing to security breaches as well as the most common attack vectors used by cybercriminals, confirming the fears of many organisations that their own users are their greatest vulnerability.

The section concludes with a brief discussion of the human error perspective in the wake of the Covid-19 pandemic and the unique security challenges faced by organisations as a result.

2.1 The Cybersecurity Landscape

The terms computer security, network security, information assurance, InfoSec and cybersecurity are commonly used interchangeably and are frequently interrelated and aim to achieve the same common goals of protecting the confidentially, integrity and availability of information or data. However, there are some subtle differences, in particular between cybersecurity and InfoSec.

National Institute of Standards and Technology (Kissel, 2013: p:58) defines cybersecurity as the "ability to protect or defend the use of cyberspace from cyber-attacks." Cybersecurity and Infrastructure Security Agency (CISA) (CISA, 2019) defines cybersecurity as the "art of protecting networks, devices, and data from unauthorized access or criminal use" whilst ensuring the integrity, confidentiality and availability of information. The ISO (ISO, 2021) refers to the "preservation of confidentiality, integrity and availability of information in the cyberspace". Cybersecurity concerns any and all types of attacks from the inside or outside of an organization. It aims to provide a framework for protecting and securing data that is in digital form that is vulnerable to attacks or unauthorized access (Fasulo, 2020).

NIST (Wilson and Hash, 2003) define information security as the protection of "information and information systems from unauthorized access, use or destruction in order to provide integrity, confidentiality, and availability". This definition of InfoSec is more comprehensive and covers information and data regardless of its form. In other words, data can be in a digital or physical (e.g., paper) format.

Today, it seems that everything relies on computers and the internet in one way or another. This seems to be the case in all spheres of our lives including communication (email, smartphones), entertainment (social media, movies, games), transportation (navigation systems), shopping (online shopping, online payments) and so on. It seems that much of our daily life relies on technology and the internet in some form (NIST, 2018).

As such the term cybersecurity seems to capture this reality more succinctly. However, for the purpose of our discussion both terms (cybersecurity and InfoSec) will be used interchangeably throughout this study.

2.1.1 InfoSec Standards

The aim of InfoSec standards is to set forth techniques that can facilitate the protection of the cyber environment of a user or organization. The term cyber environment in this context is comprehensive and covers the users, devices, networks, devices, applications, software, services, information in all forms as well as systems that are directly or indirectly connected to networks (Scarfone, Benigni, and Grance, 2009).

The primary goal of such security standards is reduction of security risks as well as prevention or mitigation of cyber-attacks. These InfoSec standards are available in published form proving a collection of guidelines, security concepts, policies, tools, risk management techniques, user training, best practices, information assurance and technologies (InfoSec, 2021).

Some of the most pertinent InfoSec industry standards are discussed below.

ISO/IEC 27000

This is family of InfoSec standards jointly published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). This broad series of standards offers a best-practice approach that helps organizations manage InfoSec by addressing people, processes and technology. As such this series of standards covers areas of privacy, confidentiality and technical cybersecurity issues, providing best practice recommendations within the context of a comprehensive InfoSec management system (ISMS) (ISO/IEC JTC 1, 2013).

Within the ISO/IEC 27000 family, the ISO/IEC 27001:2013 (ISO 27001) and ISO/IEC 27002:2013 (ISO 27002) are particularly relevant in the context of InfoSec. ISO 27001 offers a framework for implementing a comprehensive InfoSec management system (ISMS) in order to bring InfoSec under explicit management control and to ensure the confidentiality, integrity, and availability of all data. ISO 27002 is a reference guide for implementing security controls as part of an ISMS and serves as a guidance document, offering best-practice guidelines for applying the controls encompassed in ISO 27001 (Bird, 2013).

NIST Cybersecurity Framework

Developed by the National Institute of Standards and Technology, NIST Cybersecurity Framework (CSF) provides guidance to help all stakeholders of organizations to manage and reduce cybersecurity risks. Based on existing standards, practices and guidelines, it offers tailor-made organization-specific activities for managing cybersecurity risks (Gordon, Loeb, and Zhou, 2020). NIST CSF is popular with a wide range of businesses and organization since it offers a high-level classification of cybersecurity outcomes and a strategy to assess and manage those outcomes (NIST, 2018). It provides organizations with guidance on how to protect critical infrastructure and protections for privacy (Moss, 2019).

Cyber Essentials

Launched in 2014 by the UK Department for Business, Innovation and Skills, Cyber Essentials is an information assurance scheme managed by the National Cyber Security Centre (NCSC). It is a collaborative standard developed in partnership with the Information Assurance for Small and Medium Enterprises Consortium (IASME), the British Standards Institution (BSI) and the Information Security Forum (ISF) (Moore, 2020). Cyber Essentials comprises of an assurance framework and a basic set of security controls to help protect information from security threats originating from the internet. Its principal goal is to help organizations to adopt good practice in InfoSec (Curtis, 2014).

GDPR

General Data Protection Regulation (GDPR) is a standard introduced by the European Union (EU) in 2018. One of the main goals of this standard is provide data protection of all the users. GDPR defines a set of key principles designed to offer guidance on how user's data can be handled. Integrity and confidentiality are a key principle that stipulates that personal data must be protected against unauthorized access, accidental damage, loss or destruction. In order to be fully compliant with the requirements of GDPR organizations must put in place appropriate InfoSec protections to guards against hackers and data security breaches (GDPR, 2018).

Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS is an InfoSec standard specifically designed to help organizations to handle credit cards from the major card networks such as Mastercard, American Express, etc. The PCI standard is implemented by all the major card brands and administered by the PCI Security Standards Council. The main motivation behind the creation of this standard was to tackle credit card fraud by improving controls around cardholder data (PCI DSS, 2018).

2.1.2 Technological Advances in InfoSec

Information security has traditionally been considered a technological issue with much attention often focused on technical solutions. Much of the research and development in the field of InfoSec has been oriented towards providing technology-based solutions. There have been some remarkable advances in the field of InfoSec and the level of technical sophistication makes it very difficult for security breaches to take place, at least on a technological level.

Today there is a wide variety of technologies such as authentication systems, encryption, firewalls, VPN, intrusion detection and anti-malware protection systems available to successfully protect organizations from an array of threats. Such security technologies are undoubtedly invaluable weapons in an organizations' InfoSec armoury. However, technology alone cannot deal with all InfoSec risks. Since computers are operated by people, ultimately human behaviour will influence how people interact with information technology and the impact this will have on the security of such systems. It is ultimately the users in any organization that are the primary line of defence (Parsons et al, 2010).

InfoSec is ultimately about people. Much of the research into how attackers manage to compromise IT systems clearly illustrates that the human element is always crucial to the majority of successful attacks (Hughes-Lartey *et al*., 2021). Although technical solutions are very important, unfortunately, they do not address the ignorance or omission on the part of the people using IT systems.

2.2 Human Factors & Human Errors

Human factor is an overarching term for the study of human performance in specific environments. From an organizational and more specifically InfoSec perspective, human factors describe the relationship between users and the technology they operate as well as the environment, knowledge and information that is available to them (Edkins, 2021). Perhaps more importantly, human factors are about user interactions with other humans. In other words, human factors are conditions that without proper management can result in human errors.

The terms human factor and human error are quite often used interchangeably. However, there are some important differences between the two terms. Human error is what a user commits as a consequence of their action (or inaction). Human factors on the other hand can be described as the reasons why such errors take place.

Some examples of human factors in the InfoSec context include fatigue, physical or mental stress, personal issues, distractions, work pressures, familiarity with the task, experience and training and awareness. It is evident that an understanding of human factors is crucial to understanding why human errors occur and how they can be addressed.

Human error is a term that is intuitively understood by most people and one that has become part of the common vernacular in many industries. It is a generic term that encompasses all the occurrences when a planned activity or task fails to achieve its intended outcome. Although the exact definition may vary according to the industry, the term refers to the consequences of human action (or inaction), deliberate violations or the causal factor of an accident (Hansen, 2006).

Human errors are not restricted to any particular industry, profession, gender or culture. Everyone can make errors regardless of the level of training, experience, professionalism and motivation. On the bright side, research has shown that experts at given tasks are better positioned than novices at predicting errors and taking appropriate corrective action to mitigate their effects (Edkins, 2021).

Errors do not simply occur randomly; there are almost always reasons for their occurrence. Generally, human errors can be divided into two main categories: unintentional or intentional actions (Edkins, 2021).

Unintentional Actions

This covers instances where the right intention or action is carried out incorrectly or even where the user fails to carry out an action. These actions can occur as a result of attention or memory failures during familiar tasks and include slips (e.g., sending sensitive documents to the wrong recipients) and lapses (e.g., forgetting to back up important data). These types of errors often occur during highly-trained repetitive tasks where the user does not need to fully concentrate on the task at hand. These types of error cannot simply be eliminated by training but require improved system design to mitigate the likelihood of their occurrence (HSE, 2015).

Intentional Actions

This covers instances that involve conscious choices on the part of the user and can be traced back to factors such as poor judgment or motivation. These types of error are often mistakes or judgement and decision-making errors (e.g., plugging an insecure USB device to company network) where the intended actions taken by the user are wrong whilst believing it to be right. This commonly occurs in situations where the user does not know the correct way to carry out a task because it's new, unexpected or they simply have not received the proper training (HSE, 2015). In such situations users often resort to rules from similar scenarios which may not necessarily be applicable. These types of errors can be addressed with appropriate user training.

Violations

Another category of human errors that is related to intentional actions is violations that often result from non-compliance, taking shortcuts or circumventions and work-arounds. These actions are intentional in nature since the user deliberately fails to carry out the procedure correctly. However, such actions are often well-meaning and rarely malicious, often resulting from a desire to complete a task efficiently and promptly. Factors that give rise to violations include poor system design, impractical rules, work expectations and work pressure (HSE, 2015).

Violations can also be classed as routine and exceptional. Routine violations tend to be habitual actions (not malicious) on the part of the user and are generally tolerated by the organization to some extent. Exceptional violations are isolated and extreme departure from the accepted norms and are rarely condoned or tolerated by management. (Shappell and Wiegmann, 2001).

Reason's Classification of Human Error

In recent times, human error has become the subject of research in almost every industry ranging from, aviation, road and rail transport, health care, nuclear power plants as well as communications networks and InfoSec. Norman (1983), in his research on cognitive engineering introduced the classification of human error that was later expounded and expanded upon by Reason (1990) and Liginlal et al. (2009). Reason (1990, p:7) defined human error as “the failure to achieve the intended outcome in a planned sequence of mental or physical activities when failure is not due to chance”. Reason (1990) postulated levels of behaviour that may be used to distinguish the different types of human error. The latter can be summarized as skill-based errors and decision-based errors.

Skill-based Errors

This type of behaviour is automatic and unconscious and the type of errors consist of slips and lapses that typically occur when performing familiar tasks. The user has knowledge of the correct course of action but fails to act correctly due to a temporary lapse, mistake or negligence. The reasons for this kind of behaviour on the user’s part could be tiredness or being distracted.

Decision-based Errors

This type of behaviour occurs under attentional control when the user makes a faulty decision. One of the main reasons for this could be the user not having the required level of knowledge to perform the task, or not understanding of the circumstances and not realising that their inaction also has consequences.

Insider Threats and IT Sabotage

The Cybersecurity and Infrastructure Security Agency (CISA) defines an insider as “any person who has or had authorized access to or knowledge of an organization’s resources, including personnel, facilities, information, equipment, networks, and systems” (CISA, 2020).

Insider threat refers to an insider who uses authorized access to an organization to cause harm to that organization. The harm can include intentional and malicious acts that adversely affect the integrity, confidentiality, and availability of the organization and its assets including data, personnel and facilities (CISA, 2020).

IT sabotage is a type of criminal action often associated with insider threats. Sabotage is in theory a violation and is defined as any situation where a current or former employee, contractor, or business partner deliberately exceeds and exploits authorized access to networks, systems, or data in order to cause harm to an organization, its data, personnel, facilities or daily business operations (King, 2010). Insider threats and IT sabotage is a vast area of research in its own right and beyond the scope of this study.

2.3 Human Errors in InfoSec

In the context of InfoSec, a human error could be described as any unintentional action (or inaction) by users that can bring about, spread or allow a security breach to take place (Georgescu, 2021). This is a rather comprehensive definition and encompasses a wide range of activities and actions. Consequently, the topic of human errors in InfoSec is vast and difficult to tackle.

We live in an age when a rapidly increasing number of people have access to computers in their personal and work environments. The vast majority of these people possess limited technical knowledge and their use of computers is restricted to basic necessities such as web browsing, emails, word processing and use of job-specific applications. Consequently, most people do know or understand the importance of security measures such as firewalls, anti-virus software and regular security updates and patches. Such users are prone to commit errors that render them easy targets of malicious software and hackers, resulting in security breaches that can have catastrophic consequences for organizations.

Computer systems can also be compromised due to design faults or security loopholes that can be exploited by hackers to gain control of such systems. In a majority of cases, once a loophole has been found it can be rectified through software updates and patches. However, the system administrator or the user may not apply such patches due to a lack of training, or sheer negligence and carelessness.

Careless and untrained inside users present some of the greatest threat to organizations. Careless user behaviour can manifest itself as writing passwords on sticky notes on screens, accessing harmful links or websites and blatantly ignoring and failing to follow proper security policies and procedures. Careless and untrained users can also fall prey to social engineering attacks resulting in major losses for businesses.

Human error and the associated security breaches is a problem that has existed since the advent of computers. Human error can take place at home, involving individual users and their personal devices and data as well as employees within organizations. In the latter case, the consequences for organizations can be catastrophic (Georgescu, 2021) in terms of financial costs, loss of revenue, loss of clients and partners, system down-time, reputation and possible penalties due to regulatory noncompliance (BEQOM, 2021).

2.3.1 Examples of Common Human Errors in InfoSec

- Clicking on email links or attachments without paying attention and verifying
- Improper handling of sensitive data: accidentally deleting sensitive data, not backing up important data
- Publication of confidential data on public websites by mistake
- Email mis-delivery: sending sensitive documents to the wrong recipients
- Using weak passwords or unreliable storage of passwords, e.g., using sticky notes on computer screens
- Use of outdated software, unauthorized downloads, ignoring software update reminders
- downloading compromised software
- Use of insecure public Wi-Fi networks without a VPN
- Misconfiguration of assets to allow unwanted access
- Plugging in insecure devices, e.g., USB storage devices to company network

2.3.2 Security Breaches vs Data Breaches

The terms security breach, data breach, security threat, security incident and cyber-attack are often used interchangeably and for most part refer to the same thing. According to (Kaspersky, 2021; Symanovich, 2019) a security breach is any incident that culminates in unauthorized access to a computer network, data, applications or devices. Typically, an intruder manages to circumvent the normal security measures gaining unauthorized access to information (a data breach). A security breach is like a burglar smashing a window and climbing into your home. If the intruder snatches your personal documents and devices and manages to climb back out and escape, that would be akin to a data breach (Symanovich, 2019).

The terms security breach and data breach are often used interchangeably. Typically, a security breach occurs first and may or may not be followed by a data breach.

Some examples of security breaches are as follows:

Viruses, Spyware, and Malware

Cybercriminals make use of viruses, spyware, and other types of malware (malicious software) often sent through email or downloaded by users in order to break into protected networks. For example, a user receives an email with an attached image, audio or video file. When the user opens the attachment, their computer becomes infected and in the case of a virus can also spread to other computers on the network (Symanovich, 2019).

Social Engineering

Social engineering involves deceiving users into giving away access or confidential information (Gardner and Thomas, 2014). For example, a cybercriminal phones an employee and pretends to be a member of the IT support staff, thereby tricking the employee into revealing their password and other confidential information that the cybercriminal later uses to gain access to company information.

Ransomware Attacks

In essence, this is a form of malware used to encrypt a victim's files and documents. The cybercriminal demands a ransom (usually in the form of money) in exchange for the encryption key that can restore access to the data.

Exploits / Bugs

Systems that are out of date or have not been updated with the latest security updates and patches are vulnerable to this type of attack. Cybercriminals can exploit bugs and security loopholes to break into an organization's network.

Impersonation / Phishing attacks

Cybercriminals can send out convincing emails to employees that appear to originate from a company executive urgently requesting employee records, login information and other confidential information. The employee is convinced that the email is genuine and is all too eager to divulge the information to cybercriminals. This form of attack is very common in the financial industry where the goal of the attacker is to gain access to the user's financial accounts. This type of attack is known as phishing or spearfishing when it specifically targets a specific person (Symanovich, 2019).

Denial of Service Attacks

Cybercriminals can make an organization’s website or other important public resources unavailable to legitimate users by flooding it with traffic. This type of attack can overwhelm an organization’s security devices and prevent normal business operations.

The above-mentioned breaches are some of the most common examples. The list is by no means exhaustive and there are many other types of security breaches.

2.3.3 High-Profile Security Breaches Involving Human Factors

A number of major studies (PwC, 2020; Deloitte, 2020; Ernst & Young, 2020; Cisco, 2021; CrowdStrike, 2021; ISACA, 2019) in the recent past have shown that an overwhelming percentage of InfoSec breaches are caused by human factors. Depending on the nature of the industry, security breaches could result in catastrophic losses. Consequently, the human element cannot be ignored in any organizational security risk analysis (Cano, 2019).

Human error is a common thread in all of the examples below.

Yahoo

In 2013 three billion user accounts were compromised as a result of phishing attempts that culminated in hackers gaining access to Yahoo’s network and stealing user data such as account names, dates of birth, telephone numbers, email addresses, hashed passwords and unencrypted security questions and answers (Perlroth, 2017).

Facebook

In 2018, the company lost 29 million users' personal data due to internal software flaws. The personal data stolen by hackers included usernames, gender, and hometowns linked to a user’s profile page (Rodriguez, 2018).

Equifax

In May 2017, one of the largest consumer credit reporting agencies in the world experienced a data breach exposing the personal information of more than 145 million Americans. The breach was the result of a third-party software exploit for which a security patch was available but Equifax failed to update on their servers. Personally Identifiable Information (PII) including names, dates of birth, addresses, social security numbers and driver’s license numbers were stolen exposing millions of Americans to the risk of identity theft (Posey, 2019).

Misreporting of Covid-19 Cases

In October 2020, Public Health England (PHE) failed to report approximately 16,000 Covid-19 cases due to a Microsoft Excel error. This was caused by PHE’s developers using the incorrect Excel file format that limited each template to about 65,000 rows of patient data instead of the one million-plus rows that Excel can accommodate (Kelion, 2020).

Citigroup

In August 2020, employees in the credit department wired almost $1 billion to Revlon Inc.'s lenders as a result of a clerical error. The bank blamed human error for the blunder. Whilst some of the lenders returned the money sent to them, around 10 lenders refused and the bank filed a lawsuit to recoup approximately $501 million (Martinuzzi, 2020).

The Overpaid Australian Worker

Between July 2017 and January 2018, Australia's Northern Territory government departments made a number of overpayments to employees and contractors. One employee that was meant to receive a salary of approximately $5,000 discovered almost $500,000 in his account, more than 100 times his normal salary. An internal investigation concluded human error as the cause after it was discovered that a decimal point had been misplaced during processing (BBC Business, 2018).

2.4 The Cost of Human Errors in InfoSec

The cost of security breaches resulting from human errors is generally significantly lower than the costs associated with security breaches instigated by malicious insiders and hackers. Nevertheless, the consequences of human errors committed by normal users should not be underestimated (Ekran System, 2019). In the United States, the cost of data breaches could be in hundreds of millions of dollars in the form of regulatory fines, mandatory compensation to affected parties as well as loss of revenue due to breach of customer trust.

There are a number of organizations that keep track of major security breaches and the associated costs. The Ponemon Institute is one such organization that dedicates almost all of its efforts and budget to track costs of major data breaches.

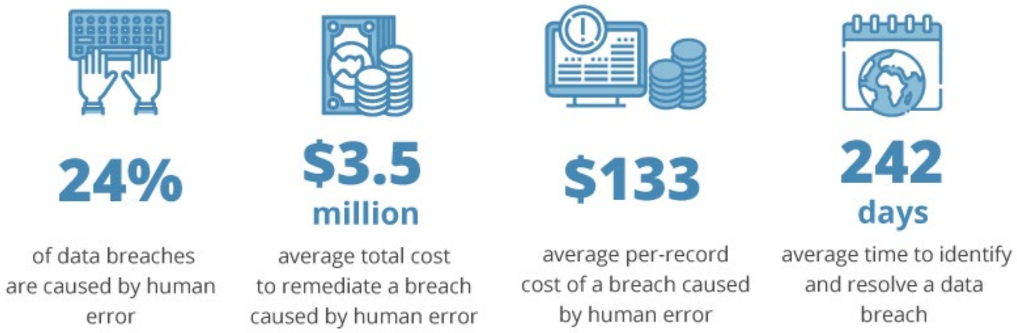


Figure 1: Ponemon Institute: 2019 Cost of a Data Breach Report

The 2019 Cost of a Data Breach Report by the Ponemon Institute (IBM Security, 2019) was compiled from a survey of 507 organizations that had experienced a breach in the previous year as well as interviews with 3,211 individuals with knowledge of the breaches within these organizations.

The report found human errors committed by employees or contractors to be the root cause for 24% of security breaches. The human errors typically resulted from compromised users as a result of phishing attacks or infected, lost or stolen devices. The average cost to remedy a breach was estimated at $3.5 million, whilst the average per record cost was $133. The survey estimated that it took organizations an average of 242 days to identify and rectify a breach resulting from human error (IBM Security, 2019).

In the UK, the Department for Digital, Culture, Media and Sport (DCMS) commissioned the 2021 Cyber Security Breaches Survey (DCMS, 2021) of 2,284 businesses, charities and education institutions as part of the National Cyber Security Programme. It is an effort to help organizations understand the cyber threats they face and what is being done by other organizations to stay safe. The survey also supports the UK government in future policy formation in accordance with the National Cyber Security Strategy 2016–2021.

The survey revealed that almost 4 in 10 (39%) of businesses and a quarter (26%) of charities reported having experienced a security breach in the past 12 months. Within this group of organisations, more than a quarter (27%) of businesses and almost a quarter (23%) of charities reported that such breaches occur at least once a week.

The most common attack vectors used by cybercriminals were reported to be phishing attacks (83% of businesses and 79% of charities) followed by impersonation attacks (27% and 23% respectively).

The average cost of a security breach experienced by UK businesses in the past 12 months is estimated at £8,460, whilst the combined average cost for medium and large organizations is at £13,400.

It is noteworthy that the figure of 39% of businesses identifying security breaches is lower than the previous year (2020) when it was 46%. This reduction could be due to the COVID-19 pandemic and the resulting economic downturn affecting normal business activities.

Nevertheless, some qualitative and quantitative data also suggests that the security risks to organizations is potentially greater as many businesses struggled to institute robust security measures during the pandemic. This is evident from the fact that only 35% (vs. 40% last year) of businesses make use of security monitoring tools whilst only 32% (vs. 38% last year) use any kind of user monitoring. This data also indicates that many organizations are simply not as aware as before of the growing security threats faced by their users.

In a world with an ever more sophisticated and a growing cyber threat landscape, there is an increasing realization amongst organizations that their own users are their greatest vulnerability. According to Kaspersky (2018), 57% of businesses expect that their security will become compromised at some point, whilst 52% believe that the careless actions of their employees is their biggest weakness.

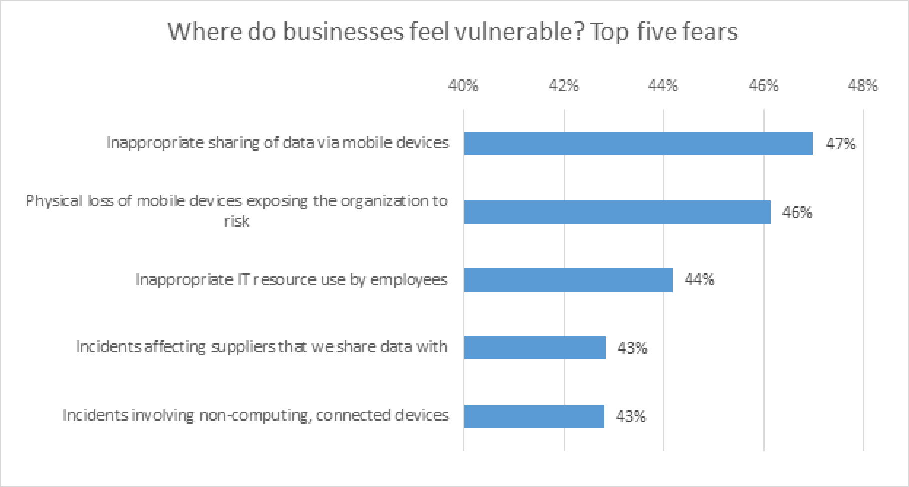


Figure 2: Source: Kaspersky Security Risks Survey 2017

The fear of insider threats amongst organization is evident from the above survey. The top three worries reported by organizations, namely sharing inappropriate data via mobile devices (47%), physical loss of mobile devices with business data (46%) and inappropriate IT use (44%) are all fears related to human behaviour and human error.

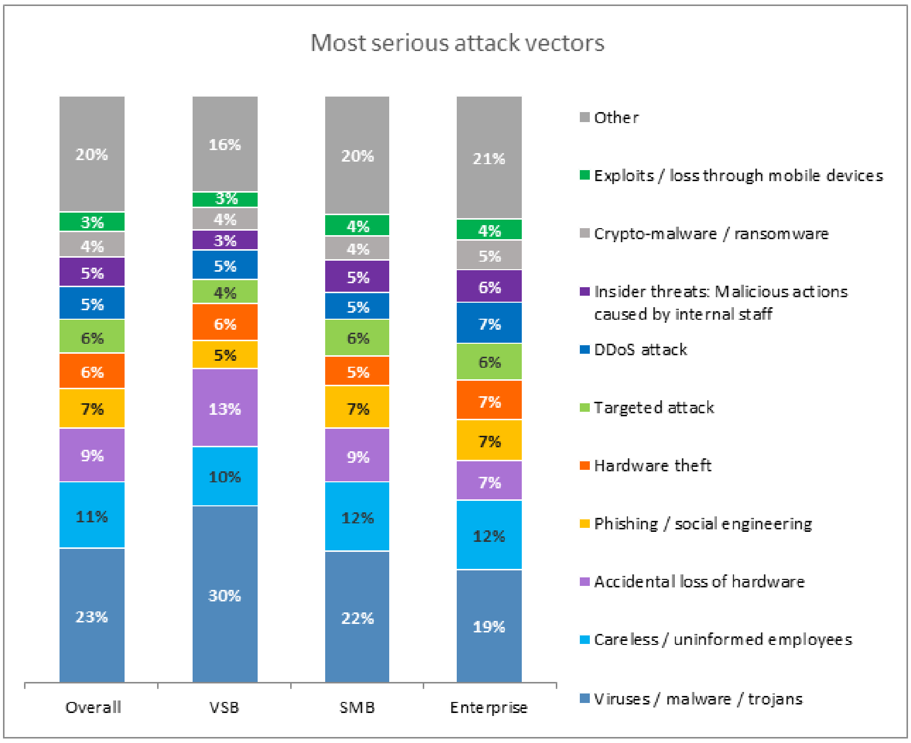


Figure 3: Source: Kaspersky Security Risks Survey 2017

The survey (Kaspersky, 2018) also revealed that amongst all the businesses that experienced security breaches in the past 12 months, more than 1 in 10 (11%) of the serious incidents involved careless users as the main cause. Other major causes of security breaches such as malware (23%), accidental loss (9%), social engineering (7%) and ransomware (4%) all have a human element in one form or another.

Employee carelessness, phishing attacks, social engineering and malware are all attack vectors that have increased in frequency and intensity over the recent years. It is evident that there is a significant user contribution in most of the serious attack vectors. Although the human element in the vast majority of such threat scenarios may be unintentional, organizations need to take serious protective measures to address the risks.

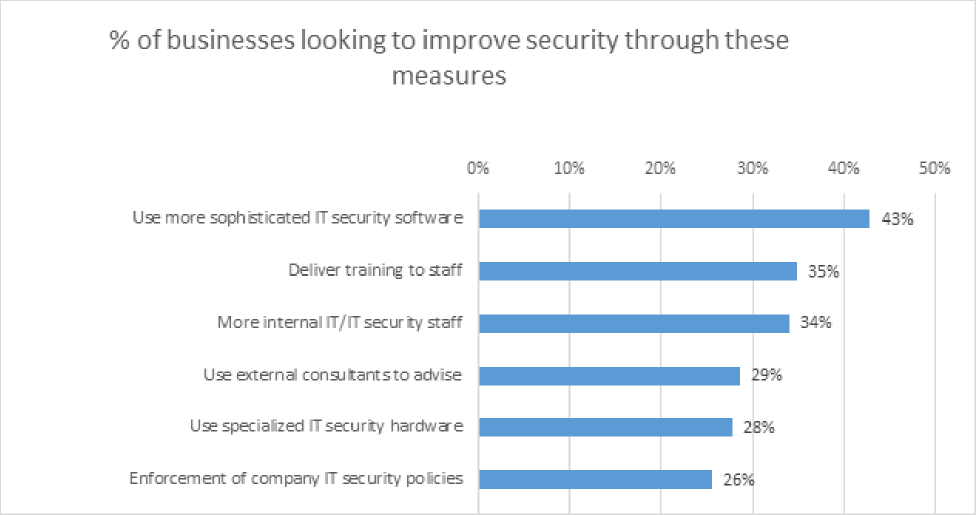


Figure 4: Source: Kaspersky Security Risks Survey 2017

When the same organizations were quizzed (Kaspersky, 2018) about their plans to address security threats, the use of sophisticated security software and staff training featured at the top of their priority list. This shows that there is some level of understanding amongst organizations about the important role that users play in the organization’s overall security.

The data proves that businesses have good reasons to be worried about employee behaviour. Human factors such as carelessness and lack of awareness can lead to serious user errors that could jeopardize the security of the entire organization. User-focused training to raise awareness is essential in motivating employee to be mindful of the plethora of cyberthreats and possible countermeasures. Protective measures such as password management, security updates and anti-malware protection are all an integral part of a comprehensive user awareness programme.

2.5 Human Error in the Wake of COVID-19

The Covid-19 pandemic has created unique security challenges for businesses around the world. Despite an unprecedented global pandemic, cybercriminals have made it amply clear that they’re not taking a break (Panetta, 2020). As discussed previously, human error is already a major factor in most security breaches and the potential for human error is greatly intensified during such uncertain times. The fears and social pressures around maintaining personal safety and well-being and dealing with a new surge of threats whilst countering the traditional cyber threats, gives rise to a uniquely challenging threat landscape for organizations and users (USecure, 2021).

In an age of social distancing, most businesses around the world have had to adjust to remote working in a way never experienced before. Many of these organizations have been forced to switch to this new way of operating with little preparation. Cybercriminals have wasted no time in exploiting the atmosphere of fear, anxiety and curiosity; as a result, users are at a significantly greater risk of yielding to online threats. According to Bannister (2020), an astounding 90% of organizations worldwide witnessed an increase in the frequency of cyberattacks during the first 6 months of the pandemic.

Employees without prior experience of working from home suddenly found themselves in situations where they were having to deal with issues such as poor internet connectivity, babysitting children and pets as well as other household chores. In the midst of all the distractions, security often dropped to the bottom of the priority list (USecure, 2021). According to the VMware Global Threat Report (VMware, 2020), 85% of chief information security officers (CISO) and chief technology officers (CTO) did not feel that their workforce was properly equipped for remote work whilst 91% of executives reported that remote work had led to a rise in cyberattacks (VMware, 2020).

Employees working from home often found themselves outside of the careful watch and management of the IT department (USecure, 2021). Without the readily available technical support, users found themselves struggling to deal with simple tech-related issues and cyber threats. IT departments were forced into situations where they had to rely on the end users to carry out essential security updates and maintain security of their home networks and internet connections.

There has been a sharp rise in the number of malware, ransomware and phishing scams reported during the pandemic (Panetta, 2020). Cybercriminals have deployed COVID-19 themed lures to deposit malware and ransomware on user devices and networks by exploiting people's fears and anxieties (Ferbrache, 2020). According to Coker (2021), phishing scams impersonating UK's tax and customs authorities grew by a staggering 87% during the pandemic. Cybercriminals employed creative themes such as offers of government assistance and tax rebates during the pandemic to lure users into downloading malicious software.

While there are technical solutions such as intelligent spam filters to protect users from the threat of malware and phishing attacks, due to the sheer number of threats and a host of different systems and technologies used by modern day employees to accomplish their work, the role of human error remains the biggest risk factor that must be addressed in order improve security (VMware, 2020).

Section 2

This section starts with a brief introduction to InfoSec awareness training, it’s role and the benefits for organisations. The current state of awareness training across the InfoSec industry is discussed in some detail. This section draws on empirical data from numerous global InfoSec surveys to highlight the increased appreciation for the importance of awareness training amongst organisations. The positive trend of increasing InfoSec awareness training budgets across the industry is also highlighted.

A problem statement draws on the main threads from both sections to firmly establish (from the literature) that whilst human error is by far the greatest cause of security breaches, InfoSec awareness training remains perhaps the most cost-effective means to change user behaviour.

Research also suggests that most security awareness programmes fail to demonstrate a positive change in user behaviour. Consequently, the discussion concludes by asking the question: why do security awareness programmes fail to deliver? In essence, this is also the research question of this project. The literature brings to light wider questions about the methods used to communicate security messages, current approaches to managing human behaviour, making awareness programmes meaningful and establishing suitable evaluation and feedback mechanisms. The section concludes by preparing the ground for the qualitative (phenomenological) data collection phase of the project where the answers to all such questions are sought from InfoSec professionals (academics and practitioners) through in-depth semi-structure interviews.

2.6 The Role of InfoSec Awareness Training

Much of the research (ISO/IEC, 2013; Wilson and Hash, 2003; NIST, 2018; ISACA, 2019; GDPR, 2018; CISA, 2020; ENISA, 2010) into InfoSec standards and best practices identifies InfoSec awareness training as a form of management control intended to achieve prevention and mitigation of security breaches and is regarded as a key contributor to achieving optimum security.

According to the Global State of InfoSec Survey (PwC, 2018) carried out by PriceWaterhouse Coopers, most serious security breaches are due to multiple failings in people, processes and technology. However, the survey identifies the failure to invest in educating staff about security risks as the root cause.

Ultimately, the protection of an organization’s information is the responsibility of all staff. InfoSec awareness training is probably the greatest non-technical measures available to achieve this (CybSafe, 2021).

My own professional experience of more than fifteen years has taught me that the security of an organization is very much dependent on the knowledge and awareness of the end users and those who manage them. As such awareness training programmes provide a crucial layer of protection against security attacks and breaches. It is important to integrate security issues and requirements into normal business behaviour to develop a security culture since many insider threats are rooted in ignorance rather than malicious motivation (Gardner and Thomas, 2014).

2.6.1 What is Security Awareness Training?

As discussed previously, the vast majority of security breaches are the result of human error, rendering the employees or users in an organization the weakest link in the InfoSec chain. Regardless of what technological controls are put in place, users will always be targets of security threats such as malware and phishing attacks. End users are one of the most effective entry points for cybercriminals to gain access to an organization's systems and data (Reciprocity, 2021).

Security awareness training aims to address the weakest link in the security chain: the users. In essence, security awareness is about changing user behaviour in order to reinforce good security practices by thinking and acting in a security conscious way. It seeks to empower users to take personal responsibility for protecting the organization's data (Gardner and Thomas, 2014). It is also a process by which an organization's workforce is educated about cybersecurity issues, best practices as well as regulatory compliance (Reciprocity, 2021). In essence, a security awareness training programme is a vehicle for communicating information required by users (and managers) to do their jobs (Wilson and Hash, 2003).

A security awareness training programme seeks to train users about the potential threats to an organization's data and ways to avoid situations that could jeopardize the security of an organization by enforcing the policies and procedures in place to protect data (Gardner and Thomas, 2014). Policies and procedures are put in place to govern and protect an organization's data and could include computer use policies, remote access policies, internet use policies, etc. (Vlandan, 2020).

2.6.2 Benefits of a Security Awareness Programme

Apart from the most obvious benefit of helping to prevent security breaches and attacks, a successful security awareness programme also offers many other benefits.

With the aid of security awareness training, organizations can foster a culture of security whereby security values are built into the fabric of the business. The knowledge and situational awareness that employees develop can also be transferred to their personal lives. This in turn empowers the employees to mitigate and respond to risk, acting as a crucial first line of defence.

Technological controls are in an integral part of any organization's security. However, technological defences still depend on interaction and input from humans and without appropriate security awareness training, they cannot fulfil their potential (CybSafe, 2021).

Consumer confidence is an important indicator of the level of trust placed in a business, affecting customer loyalty and ultimately business revenues. Consumers are increasingly more aware of the various cyberthreats and expect to feel safe and secure. According to a recent survey by Arcserve (Security Magazine, 2020), 70% of consumers believe that businesses need to do more to ensure cyber security. Security awareness training demonstrates to the consumers that the business is responsible and takes cybersecurity seriously.

Businesses are increasingly being required to comply with their industry specific data security standards, such as GDPR and PCI-DSS with security awareness training almost always being an integral condition of compliance (Reciprocity, 2021).

2.7 The State of Security Awareness Training

The global disturbance caused by the COVID-19 pandemic has opened up a whole new world of sinister opportunities for cybercriminals. The curiosity surrounding latest COVID-19 developments combined with unprecedented disruptions to daily life such as lock-downs, home-schooling and remote working created an atmosphere of fear, stress and anxiety that rendered users even more susceptible to mistakes. Cybercriminals thoroughly exploited the opportunity by targeting already vulnerable users with COVID-themed lures to gain access to sensitive organizational data (ProofPoint, 2020). In 2020, organizations around the world witnessed a rapid surge in phishing and ransomware attacks, with up to two-thirds reporting successful attack or infection (ProofPoint, 2021).

According to the 2021 State of the Phish annual report, 92% of UK organizations required most of their employees to work from home due to the pandemic. This in itself was a huge challenge as many organizations found themselves ill-prepared (Cosgrove, 2021) for this new mode of operation.

Many organizations recognized the situation as a wake-up call and in response instituted security awareness training or propped up their existing awareness training programmes. In particular, many organizations conducted COVID-specific security awareness training. According to (ProofPoint, 2021), 80% of organizations reported a reduction in phishing susceptibility as a result of awareness training. Although it is encouraging to see that more organizations are putting in place user awareness training, it is also striking that it took a global crisis to compel organizations into rethinking their priorities (Cosgrove, 2021).

According to numerous global InfoSec surveys (ProofPoint, 2021; ISACA, 2019; DCMS, 2021; IBM Security, 2021; Kaspersky, 2021; PwC, 2020; CrowdStrike, 2021), there has been a steadily increasing appreciation of the importance of security awareness training amongst organizations in the recent past. According to State of Security Awareness Training survey (CybeReady, 2020) carried out by CybeReady, 58% of the decision-makers questioned believe security awareness training to be superior to technological solutions, especially when dealing with rampant threats like phishing.

Almost 98% of organizations surveyed (ProofPoint, 2021) have a security awareness training programme of some sort. The figure of 98% is astounding and taken at face value, it would suggest that the majority of organizations have got it right. However, when probed further, of the 98%, only 64% conduct formal awareness training for their users whilst nearly 30% rely solely on simulated phishing attacks to train their users. Only around 52% of the organizations surveyed conduct company-wide training, whilst around a third (36%) provide training only for specific departments and job roles.

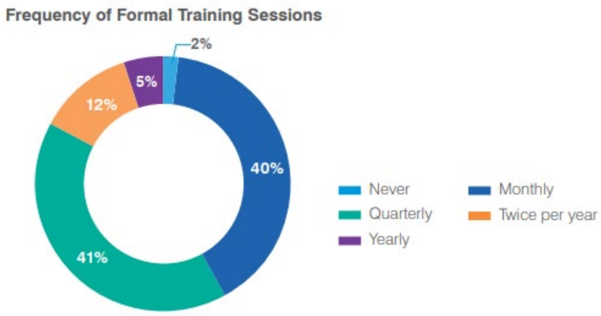


Figure 5: Source: ProofPoint: 2021 State of the Phish Annual Survey

The annual survey by ProofPoint also asked organizations about the frequency and duration of formal awareness training. Around 80% reported that they conduct training at least quarterly, whilst 12% of respondents reported delivering training bi-annually.

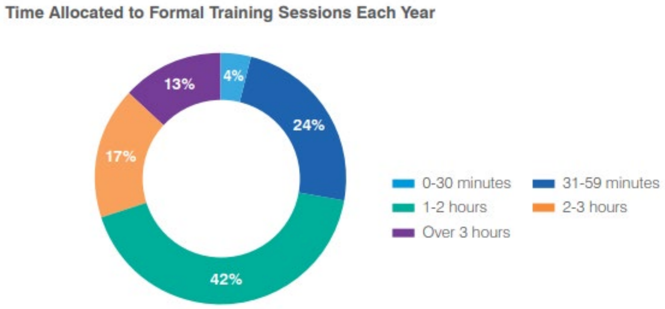


Figure 6: Source: ProofPoint: 2021 State of the Phish Annual Survey

In terms of the duration of the training delivered, at least 72% of organizations deliver training that lasts at least one hour or more whilst 13% delivering training lasting more than 3 hours. Research conducted by Osterman (2019) also revealed a significant increase in the amount of monthly security awareness training time received by users: an average of 17.6 minutes in 2018 to 26 minutes in 2020.

2.7.1 Increases in Security Budgets

Research also reveals that security budgets for a great majority of organizations have been steadily increasing over time. (CybeReady, 2020; Osterman Research, 2019). As a general rule, security budgets can vary widely depending on the nature of business, the size and geographical distribution of the workforce as well as the risk appetite of upper management.

More pertinently, per-employee security awareness training budgets have been increasing at a faster rate than overall security budgets (Osterman Research, 2019).

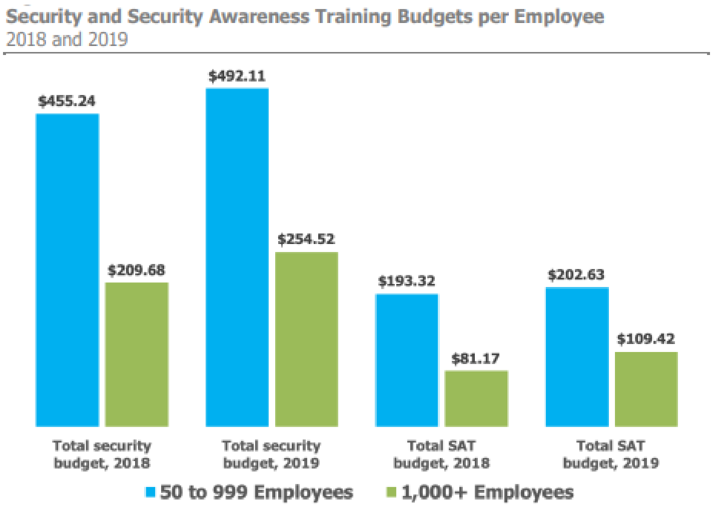


Figure 7: Source: Osterman Research 2019 – The ROI of Security Awareness Training

Osterman Research revealed that the average security budget per-employee for both small and large organizations increased from $332 (2018) to $373 (2019), representing a 12% increase. On the other hand, the average security awareness training budget per-employee for both small and large organizations increased from $137 (2018) to $156 (2019), representing a 14% increase.

It is also worth noting that the per-employee overall security budget and per-employee security awareness training budget for smaller organizations was significantly higher than the equivalent per-employee budgets for larger organizations, both in 2018 and 2019. This is expected as larger organizations are able to reduce their per unit costs due to economies of scale (Osterman Research, 2019).

On the surface, the statistics related to the uptake of security awareness training seem very encouraging. However, the prevalence of security awareness training on its own is not a true measure of success. There is a significant difference between delivering a security awareness training programme and delivering an effective security awareness training programme (CybeReady, 2020; Cosgrove, 2021).

2.8 Why Security Awareness Programmes Fail to Deliver

As discussed in the previous section, human error is by far the greatest cause of InfoSec breaches. Security awareness training aims to address the weakest link in the security chain: the users. It is one of the most cost-effective means to reduce the risk of security breaches resulting from human error. In essence, security awareness seeks to change user behaviour in order to reinforce good security practices by thinking and acting in a security conscious way.

As noted in the previous sections, there has been an increasing appreciation of the importance of security awareness training amongst organizations. A survey by ProofPoint (2021) reported that almost 98% of organizations have a security awareness training programme of some sort. At the same time security awareness training budgets as well as the average user training time have been increasing steadily over the recent years. With more employees working from home due to the pandemic, cyber-attacks are on the rise. Research by Barracuda Networks

(Touchstone Security, 2020) reported a 667% surge in COVID-19 themed email attacks, from January to February 2021 alone.

The primary goal of security awareness training is to change user behaviour (Winkler and Manke, 2013). It is a very frustrating scenario when the IT security team works tirelessly to implement and maintain advanced security defences, while the end users carelessly click on dubious links and reply to phishing emails, jeopardizing the entire security of the business. A great deal of problems experienced by security professionals could be solved if the end users acted differently. If only the user didn't click that email link or download that free software or choose such a simple password, our lives would be so much easier; these are familiar comments made by security professionals (Patterson, *et al.*, 2007).

Most users know that emails and social media messages from unverified senders can contain dangerous links but they still click on them (FAU, 2016). Despite the significant investments made by organizations in security awareness training and the repeated warnings by security professionals about cyberthreats, the ever-increasing breach statistics demonstrate that many users are simply not following through on what has been taught to them.

According to CybeReady (2020), most security awareness programmes fail to demonstrate a positive change in user behaviour. From an organization's perspective, a failure to change user behaviour could ultimately mean a failure of the whole security awareness programme (Spitzner, 2012).

2.9 Problem Statement

Human error is by far the greatest cause of InfoSec breaches. Security awareness training aims to address the weakest link in the security chain: the users. It is deemed to be one of the most cost-effective means to reduce the risk of security breaches resulting from human error. Security awareness seeks to change user behaviour in order to reinforce good security practices and induce users to think and act in a security conscious way.

Research points to an increasing appreciation of the importance of security awareness training amongst organizations. Multiple industry surveys confirm the existence of security awareness programmes within most organizations, with statistics as high as 98% of organizations with an awareness training programme of some sort.

The COVID-19 pandemic has prompted many organizations to re-evaluate their security posture and in response institute pandemic-specific user security awareness training as well as propping up their existing awareness programmes. It is encouraging to see such positive measures being taken by organizations. However, it is probably too early to assess whether these measures are well-considered sustainable policy-based decisions or simply a knee-jerk reaction to a global pandemic.

Research also indicates steady increases in overall security budgets. More pertinently, security awareness training budgets as well as the average user training time has been increasing steadily over the recent years. All of the crucial indicators seem to point to a state of security awareness training that is robust and fit for purpose. However, most recent global security surveys reveal that human behaviour remains probably the single greatest threat to InfoSec and security breaches resulting from human error are still rampant.

In light of the findings of the literature in this field, it seems that issues persist with managing human behaviour despite the efforts of organizations to put in place suitable awareness programmes. Research findings seem to suggest that awareness training does not automatically lead to the desired user behaviour. This raises wider questions about the effectiveness of awareness training programmes and how such programmes could be made more meaningful and contextualized with suitable evaluation and feedback mechanisms to ensure continuing currency and relevance.

The methods used to communicate security messages to persuade users and the way that users process and respond to such messages are also important considerations for the success of such awareness programmes. The research also raises issues relating to current approaches to managing human behaviour in InfoSec and how these could be improved to effect change in user behaviour. There are also questions surrounding the role of organisational culture in changing user behaviour. These are some of the more obvious issues and concerns that emerge in light of the literature review. It is expected that more pertinent issues will transpire during the course of the research.

This research project is an effort to gain a better understanding of the issues involved in existing security awareness training programmes and why they fail to effect change in user behaviour as their intended purpose. It is also an attempt to explore the possible remedies to the aforementioned problems and to elucidate the findings in the form of practical guidelines that can be incorporated into future organisational security awareness training programmes to reduce InfoSec breaches resulting from human error.

The role of human factors in InfoSec has been a recurring theme in my career over the years and this project is also an effort to consolidate and further enhance my understanding of the complex issues surrounding human behaviour and organisational InfoSec awareness training programmes. I consider my own personal and professional experience, technical knowledge and research background as an indispensable part of this project. I believe that there is a need for an integrated approach to understanding human behaviour in this field in order to design and implement effective awareness programmes that can truly achieve the desired change in user behaviour. Such an approach is intrinsically transdisciplinary since it requires insights from InfoSec researchers, practitioners and psychologists among others. It is for this reason that I have employed a multi-faceted research approach that draws upon a robust literature survey and in-depth phenomenological interviews with InfoSec academics and practitioners in order to gain valuable and practical insights into the issue at hand.

The problem statement can be summarized as follows:

A problem exists

Human error is arguably the greatest cause of InfoSec breaches. Security awareness training seeks to bring about better security through a positive change in user behaviour. Consequently, awareness training programmes form a crucial part of an organization's overall security posture. However, despite their prevalence and increased take up amongst organisations, security breaches caused by human error are on the rise.

The problem is important

Security breaches resulting from human error can have potentially catastrophic consequences for organisations in the form of financial losses (loss of revenue, regulatory fines, mandatory compensation), loss of consumer confidence and damage to reputation.

This research is necessary and will help to solve the problem

Existing research shows that security awareness training is probably one of the most cost-effective ways to mitigate the risk of security breaches resulting from human error. However, there is a need for a better understanding of why security awareness training programmes fail to effect the desired change in user behaviour. The findings of this research will offer possible remedies in the form of practical guidelines that can be incorporated into future organisational security awareness training programmes to reduce InfoSec breaches resulting from human error.

The research design is viable in order to help solve the problem

A multi-faceted research approach draws upon a robust literature survey and in-depth phenomenological interviews with InfoSec academics and practitioners in order to gain valuable and practical insights into the issue at hand.

Summary

This chapter provided the theoretical framework that this research study is built on through a detailed discussion of InfoSec ontology and awareness training as a crucial and evolving aspect of InfoSec. For the purpose of simplicity and coherence, the chapter was divided into two main sections. Section one provided a general overview of the InfoSec landscape with a brief discussion of well-known security standards, differences between human factors and human errors and the main categories of human errors considered in the InfoSec literature. Section two provided a brief introduction to InfoSec awareness training, its role and benefits to organisations. The current state of awareness training across the InfoSec industry was discussed. The increased appreciation for the importance of awareness training amongst organisations and the positive trend of increasing InfoSec awareness training budgets across the industry was highlighted. This chapter concluded with a problem statement, confirming that a real problem exists, it is important, this research is necessary, and that the research design is viable and will help to solve the problem.

Chapter 3: Project Research Methodology

Overview

This chapter provides a critical discussion of the research methodology I have used in this project and my justifications for the choice of this particular methodology. My stance as an insider practitioner-researcher is considered and how this has affected my overall approach to this project, including the choice of research methodology. The details of the chosen methodology and research design are presented here, including sampling method, sample size, research instrument and data collection. The issues of researcher bias, validity and reliability of the research are discussed as well as triangulation as a means to reinforce credibility. This chapter also provides a discussion of how issues of confidentiality and research ethics have been dealt with.

This project employed a qualitative research methodology using interpretive phenomenological analysis (IPA) to explore the lived experiences of InfoSec academics and InfoSec practitioners in order to answer the research question: *What are the main shortcomings in existing InfoSec awareness training programmes and how can these be addressed in order to reduce human errors?* The participants (InfoSec professionals) represent the unit of analysis for this study. As such, the analysis is intended to gain an understanding of the participants' meanings developed after reflecting on their roles and past and current experiences as it relates to InfoSec awareness training programmes.

I will begin by reaffirming that in any discussion about human learning, the nature of knowledge (epistemology) and the nature of reality (ontology) are closely intertwined, whereby one inevitably affects the other. It is rather like a circular journey where reality influences human knowledge which in turn has an impact on human reality (Allison and Pomeroy, 2000). Before delving into a critical discussion of the methodological issues related to this project, it is important for me to clarify my own ontological and epistemological position and how it has evolved over time. This will help me to identify and construct an appropriate research paradigm for this project. In other words, I was able to put together a paradigm based on my professional context and one which is related to the change impact I wish to accomplish, as already indicated above. Consequently, I was able to 'pick and mix' what works for my context and practice, constructing a methodology (rather than picking one off the shelf) with the appropriate data collection tools fit for the purposes of my aims and objectives.

With a background in computer communications engineering and InfoSec, much of my previous research experience is based on a positivistic research philosophy. According to Guba & Lincoln (2005) this approach to research treats reality as objective and knowable. It is based on the premise that the only authentic knowledge is scientific knowledge that can only come from positive affirmation of theory through strict scientific methods. A positivistic research paradigm also implies that the researcher is independent and external to the research. This paradigm favours a quantitative methodology where the unit of analysis could be reduced to the simplest form.

Over the years, the field of InfoSec has witnessed a steady shift in focus towards a more qualitative research paradigm coinciding with an increasing recognition of the role played by human and social factors in this field. My own professional and research practice has followed a similar trend with a shift in focus from a predominantly technical approach to one that is more socio-technical in nature, recognising that InfoSec is both a human and technological problem.

The introduction of human subjects into any research context renders a traditional positivistic approach rather rigid and hence unsuitable. Instead, the research focus tends to shift towards generation of new theory and knowledge by understanding how social phenomena develop in particular social contexts (Easterby-Smith *et al*., 2002). The latter lends itself to a more interpretivist constructivist research paradigm where reality is seen as being subjective and individually and socially derived (Guba & Lincoln, 2005).

Interpretive methodology emphasises that social phenomena be understood "through the eyes of the participants rather than the researcher" (Cohen *et al*., 2007: 21). As such the phenomenon of interest must be understood within the context of the participants. The interpretivist-constructivist researcher relies upon the research participants' views of the context being studied with an implicit recognition of the impact that their own background and experience will have on the research (Creswell, 2013). As a researcher, I would be engaging with the opinions, ideas and lived experiences of the research participants and therefore would be seen as an involved participant rather than a detached and neutral outsider.

Crotty (1998) expounds that all knowledge and therefore all meaningful reality is dependent on human practices and their interactions with the world. With this frame of reference, constructivism regards truth and the construction of meaning to be derived from human engagement with the realities around them; subject and object working in tandem to generate meaning. It follows therefore that meaning is ultimately constructed and different people will create meaning in different ways since human beliefs and ideals are inevitably influenced by cultural perspectives (Crotty, 1998).

An interpretivist-constructivist approach seeks to analyse data inductively. As a researcher, rather than start with a particular theory, I would attempt to discover patterns in the data which can be gathered under broad themes to understand the phenomenon and inductively generate theory or patterns of meanings (Creswell, 2013).

Interpretivist-constructivism is the theoretical framework or 'lens' I will use through which I will examine the research data. The 'lens' will help me to 'sharpen my focus' on the phenomenon of interest (Polit & Beck 2006).

An interpretivist-constructivist paradigm is appropriate for this project since from an ontological perspective, reality is subjective and socially constructed by participants of the research. It follows therefore that the phenomenon of interest (InfoSec awareness programmes and human errors) is best understood from the point of view of the participants that are directly involved in the activities and behaviours that I am seeking to study.

Whilst much is known to me about InfoSec awareness training programmes and the varied professional views in this field, I seek to further add to my existing knowledge and experience by carrying out a deeper investigation of current practice within a more expert group from my community of practice. A constructivist research paradigm favours dialogue in trying to gain an authentic understanding of the reality as perceived by the participants. In essence, it avoids treating responses like some quantifiable entities that can be described but instead problematizes the whole process of constructing relevant 'facts' (Allison and Pomeroy, 2000). As a researcher, I would learn to read and contextualise the responses and interpret them in a way they can be used as `fact' or `evidence' for future developments and innovation in professional practice.

Since the research question focuses on establishing what the participants think is going on, a qualitative research methodology will be most appropriate. Qualitative methods provide an integrated view by focusing on understanding the social setting rather than making predictions about it. In qualitative research, the researcher becomes a research instrument and is therefore required to have appropriate skills to observe participant behaviour and to conduct face-to-face as well as online (e.g., Skype) interviews. This type of research allows room for identifying the role of the researcher and their biases (Janesick, 1994). Although researcher bias is an inevitable part of qualitative research, there are techniques that can be used to reduce its impact and will be discussed later in this section.

3.1 Phenomenological Investigation

The central research question of this study seeks to explore the shortcomings in existing InfoSec awareness programmes and possible remedies to improve the effectiveness of such programs in order to reduce security breaches resulting from human errors. As previously highlighted, within academic and professional literature, InfoSec awareness training is consistently and almost unanimously hailed as one of the most effective measures to counter the security threat emanating from human factors. However, despite an increased appreciation of and investments in InfoSec awareness programmes by organisations, security breaches resulting from human errors are rampant and on the rise.

This study seeks to understand the phenomenon of the effectiveness (or lack thereof) of InfoSec awareness training programmes as experienced by InfoSec professionals through interpretative phenomenological analysis (IPA). The goal of the analysis is to understand the participants' individual meanings that develop after reflecting on their role as it relates to InfoSec awareness programmes. For these professionals dealing with InfoSec awareness training programmes and related issues such as the effectiveness of such programmes in preventing human errors is a normal everyday occurrence. This requires an appropriate approach to facilitate and guide the study participants in the reflection process, in order to draw out useful meanings from their lived experiences.

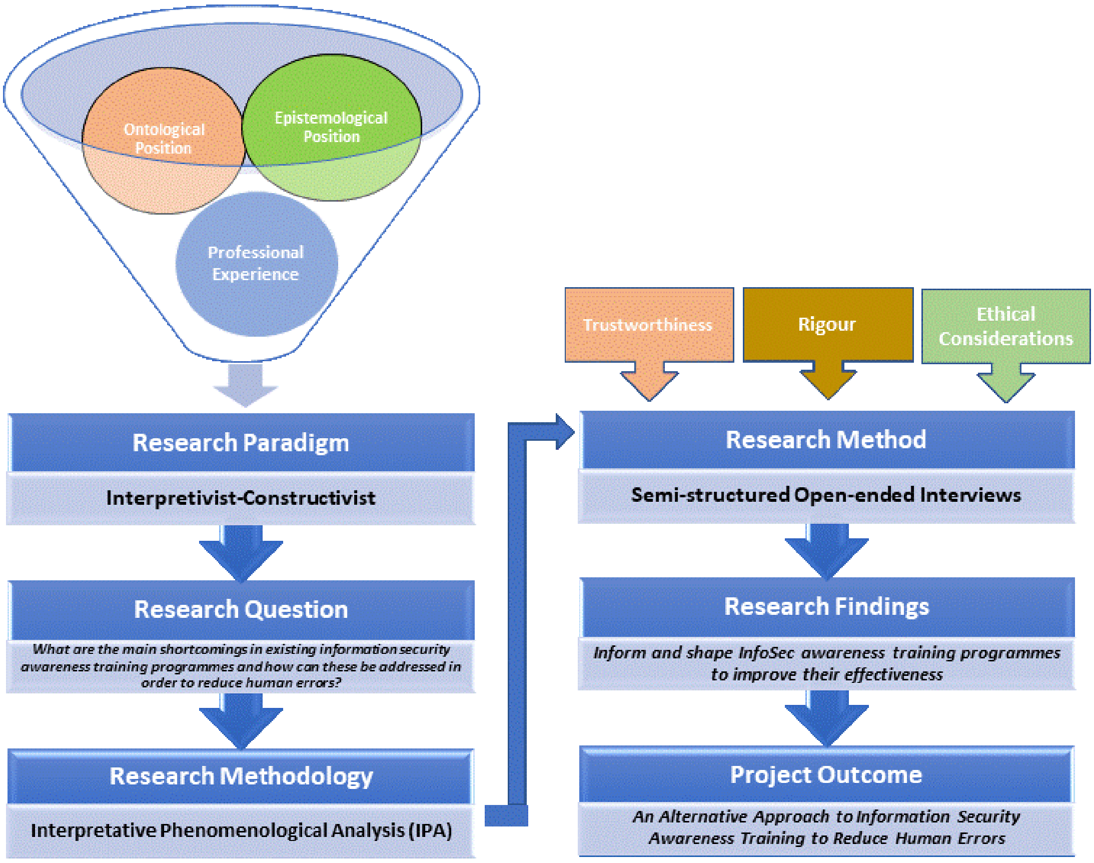

Ontological Position
Epistemological Position
Professional Experience
Trustworthiness
Rigour
Ethical Considerations
Research Paradigm
Interpretivist-Constructivist
Research Question
What are the main shortcomings in existing information security awareness training programmes and how can these be addressed in order to reduce human errors?
Research Methodology
Interpretative Phenomenological Analysis (IPA)
Research Method
Semi-structured Open-ended Interviews
Research Findings
Inform and shape InfoSec awareness training programmes to improve their effectiveness
Project Outcome
An Alternative Approach to Information Security Awareness Training to Reduce Human Errors

Figure 8: Research design for the project

As a qualitative research methodology, IPA offers the exploratory capacity to investigate, interpret, and make sense of the problematic issues outlined above. Qualitative research is conducted when there is problem or issue that needs to be explored. A phenomenological study is an appropriate approach to get to the root-cause of the phenomenon (Creswell, 2013). According to Creswell (2013), a phenomenological approach expresses the common meaning for the research participants of their lived experiences of a phenomenon. IPA is an interpretive process in which the researcher interprets the meaning of the lived experiences.

The idea of finding meaning in lived experiences is not an unconventional concept; indeed, it's an instinctive practice that humans engage in continuously. However, drawing meaning from such experiences materialises when humans use appropriate language to enhance and reconstruct these experiences that would otherwise remain unexplored and unrefined, stored away as everyday events (Merleau-Ponty & Landes, 2012).

The process of reflection is an integral part of phenomenology. IPA seeks to provide detailed examination of personal lived experiences in an attempt to understand the authenticity of the meaning given to the experience through reflection on the experience. IPA is essentially an interpretative endeavour which recognises that humans are sense-making organisms (Smith, Flowers and Larkin, 2009). IPA seeks to construct an account of lived experiences in its own terms rather than relying on one dictated by any other pre-existing theoretical presuppositions.

This study involved in-depth open-ended semi-structured online interviews with InfoSec professionals (academics and practitioners), working in academic and business environments respectively. Each interview was designed and conducted to help the participants to reflect on their unique experiences of research into InfoSec human factors and InfoSec awareness training programmes and to elucidate the meanings derived from those experiences. These InfoSec professionals are ultimately responsible for protecting and enhancing the value of an organization's assets.

InfoSec practitioners provide strategic, tactical and operational oversight of an organization’s InfoSec operations. Their role includes ensuring that the business understands the importance of security and adherence to policies as well as identifying weaknesses in existing efforts and ensuring that adequate resources and processes are in place to continually update and strengthen safeguards against internal and external security threats. InfoSec practitioners can assume a variety of job titles including InfoSec specialist, InfoSec architect, InfoSec analyst, InfoSec awareness training specialist and chief information security officer (CISO). The implementation of robust and effective organizational InfoSec awareness training programmes is an integral part of their role. As a result of their experience with InfoSec awareness training programmes, interaction with upper management as well as end users and first-hand encounters with a wide variety of security breaches, InfoSec practitioners are ideally placed to offer rich and meaningful insights into the phenomenon under investigation.

InfoSec academics are professionals working in a variety of academic and research-oriented environments such as universities, research institutes and laboratories. InfoSec academics keep up-to-date on the latest developments in information security threats and investigate and analyse their capabilities. They also attempt to understand the cybersecurity threat landscape, predict latest trends and attack vectors and develop and recommend appropriate security responses. A particularly crucial aspect of their role is research into human factors of InfoSec and psychological models of human behaviour, in order to identify potential factors that could lead to the success/failure in changing user behaviour. There is no doubt that with their knowledge, understanding and experience, InfoSec academics will be able to offer indispensable insights into the phenomenon under study.

My own position in this study is that of an InfoSec practitioner-researcher seeking an in depth understanding of the relevant issues. I have worked in academia and industry in very similar roles and firmly believe that the InfoSec academics and practitioners selected for this research are in a position to provide me with first-hand and thorough account of practical concerns and offer possible remedies in relation to the state of InfoSec awareness programmes.

A phenomenological approach is generally considered to have two perspectives as far as the perception of lived experience is concerned: the participants who are living through the phenomenon and the researcher who has an interest in the phenomenon (Smith, Flowers and Larkin, 2009; Giorgi, 1985; Patton, 1990). IPA is a research tradition that seeks to interpret and amplify the lived experiences of research participants (Creswell, 2013). However, in order to make sense of their lived experiences, the researcher (interpreter) must have a deeper understanding of the participants' lived experiences by putting themselves in the shoes of the participants (Smith and Osborn, 2004).

As an insider-researcher, I am familiar with the professional practice field concerned and have engaged with it for many years. This will provide me with contextual insights for judging and evaluating the responses, teasing the meanings out of these individual experiences. As a practitioner-researcher with knowledge and experience in the same field as the research participants, I can relate to their lived experiences and it is inevitable that my own experiences will be infused into the interview and data analysis stages since my own professional practice is also a part of the research object under consideration. I will make my professional values, positions and beliefs that will ultimately inform my interpretations transparent and explicit (Smith, Flowers and Larkin, 2009; Spinelli, 2005 & Groenewald, 2004).

This research culminates in the formulation of a set of practical guidelines that can be built into future awareness training programmes from the outset in order to reduce security breaches resulting from human errors. In constructing a research methodology for this project, my focus was on generating 'emergent data' reflecting the mind-sets, attitudes, overt and tacit knowledge of the professionals in the field which informed their professional practices. This is characteristic of a qualitative methodology and brings me closer to a constructivist-phenomenological research paradigm since I am dealing with the professional opinions, perceptions and suggestions of my community of practitioners. As an InfoSec practitioner-researcher I am a part of the same professional community as the participants and therefore I cannot consider myself to be a detached outsider during the research.

I am seeking to understand the practical concerns that the participants and their organizations have in relation to InfoSec awareness training programmes; in particular, why security breaches, especially those involving users, still occur despite the implementation of internal security awareness programmes.

The research participants are engaged in complex professional practice involving research, design, implementation and evaluation of organisational security awareness programmes. I am seeking to capture this complexity in my findings rather than reduce their experiences to simple terms. Therefore, I feel that a phenomenological investigation is most appropriate for this purpose. With phenomenology, the aim of the researcher is to describe as accurately as possible the phenomenon, remaining true to the facts and refraining from any preconceived notions (Smith, Flower and Larkin, 2009; Spinelli, 2005; Groenewald, 2004).

This approach also helps to seek commonalities and highlights the differences between the various cases in order to understand the reasons and causes for the concerns regarding the current approaches to InfoSec awareness programmes and to find ways to mitigate their reoccurrence.

Groenewald (2004) notes that in applying phenomenology, a researcher is concerned with the lived experiences of the people involved with the issue being researched. Since my research aims to understand the issues surrounding InfoSec awareness programmes from a technical and human perspective, a phenomenological approach provides a rich picture of the phenomena. It helps to tap into the opinions, ideas and experiences of the participants in a way that helps to generate new theory and knowledge that will ultimately benefit my community of practice.

3.2 Comparison of other possible Qualitative approaches

As discussed in the previous section, due to the constructivist characteristics of the proposed research, quantitative approaches were deemed unsuitable. Quantitative research generally relies on the testing of hypothesis in order to generate new knowledge (Creswell, 1998). Since this DProf project aims to understand the issues surrounding InfoSec awareness programmes based on the experiences of InfoSec professionals, it is not appropriate to begin with a hypothesis.

From an ontological and epistemological perspective, interpretive qualitative research approaches such as IPA aim to study the impacts of observations and experiences on the human condition (Smith, Flower and Larkin, 2009). Qualitative research approaches seek to evaluate emotions, experiences, decisions, and other forms of non-numeric data. Qualitative inquiry is better suited for the goals of this study since the focus is on understanding the experiences of InfoSec professionals. Qualitative research approaches are deemed to be less restrictive and more inductive than quantitative approaches. They offer a holistic approach to a research problem by looking at the bigger picture and seeking an understanding of the whole (Bogdan and Biklen, 2006).

Alternative qualitative research approaches were also considered for this project and the most pertinent approaches are discussed in this section.

Narrative inquiry is a form of qualitative research often employed in human sciences. It involves gathering and analysing participants' stories about their experiences and their interpretations (Haydon, Browne, & Van der Riet, 2018). However, this research approach is not suitable for addressing the research question of this study which is concerned with how security awareness programmes can be made more effective to reduce human errors rather than personal stories of the participants.

Ethnography is a popular qualitative research approach often used by social anthropologist (O'Reilly, 2005). Similar to phenomenology, it also involves in-depth interviews of participants as well as observations and informal interviewing over a substantial period of time. In my case, participant observation is not really appropriate as the focus of the research is the opinions and perceptions of the participants rather than their behaviours. Also, since the participants are busy professionals, interviews would need to be scheduled in advance rather than conducting informal interviews. Due to the restricted timescale of the project, it would not be possible to conduct interviews over a prolonged period of time as is often the case with ethnography research.

Developed in the 1960s, grounded theory (GT) is an established qualitative research approach. GT has been around a lot longer than IPA and is often considered the main alternative to IPA. GT seeks to develop theoretical-level account of a phenomenon of interest, often requiring sampling on a considerably larger scale when compared with IPA. There is significant overlap between what GT and IPA can offer since both employ a predominantly inductivist approach to research. A GT approach to the research question of this project is likely to require a larger sample leading towards more of a conceptual level understanding that would draw on individual participant accounts to justify the resulting theoretical claims. IPA on the other hand has the capacity to offer a more detailed and nuanced examination of the lived experiences of a smaller research sample, with greater emphasis on the convergence and divergence between the individual participants (Smith, Flowers and Larkin, 2009: 202). IPA's focus on the analysis of the individual experience is a crucial factor in its suitability for this research project.

3.3 Sampling Methods

Sampling is a technique that allows a researcher to select a subset of the population to help make inferences from them about the characteristics of the whole population (Bogdan and Biklen, 2006). Sampling methods are of two main types: probability sampling and non-probability sampling.

With probability sampling the researcher sets the selection criteria and selects members of a population randomly, with all members given an equal chance of being part of the sample. In non-probability sampling, members of the population do not have an equal chance of being selected. Purposive sampling and convenience sampling are two types of non-probability sampling methods used for this research. The choice of these sampling methods will be explained in this section.

The research population consisted of 8 InfoSec professionals (4 InfoSec academics and 4 InfoSec practitioners). The participants for this qualitative research study were selected using purposive sampling. This sampling method requires that the researcher use their best judgment to select only the participants that are deemed suitable and capable of answering the research question. The selection of participants using purposive sampling is also consistent with the IPA research tradition. According to Creswell (2013), in any qualitative study, the researcher must select the participants that can best help them in understanding the main phenomenon. Utilizing purposive sampling allowed me to directly identify the target population for this study. As a result, participants were selected based on their experience of the phenomenon of interest (InfoSec awareness training programmes). The InfoSec academics and practitioners were uniquely placed to provide insights and rich descriptions of their experiences relating to InfoSec awareness training programmes within their organizations. Samples are selected purposively since they can offer the researcher insights into a particular experience. Purposive sampling is suitable for this study since the intention is not to generalize the findings across a population (Smith, Flowers and Larkin, 2009).

It is important that there is homogeneity amongst the selected participants in order to gain a better understanding of the perceptions among their lived experiences. Creswell (2013) goes further to emphasize that all participants should have similar lived experiences of the phenomenon under study. I was able to achieve this by putting in place a strict selection criterion and only selecting the participant that met the criteria.

In order to gain an in depth understanding of the phenomenon of interest, a phenomenological study is required to interview a sufficient number of research participants (sample size) to be able to attain a degree of credibility. In academic literature, the recommended sample size for an IPA study varies from 6 to 20 (Ellis, 2016). Creswell (1998) recommends long interviews with up to 10 participants for a phenomenological study whereas according to Boyd (2001), anywhere from 2 to 10 research participants is sufficient to reach saturation. The sample size provides an indication of the intended size and scope of this research study. A small sample size was appropriate for this study in order to focus on the depth of participants' experiences. Due to the homogeneity amongst research participants and the small sample size, IPA research studies are expected to be rich and descriptively deep in the analytical process, allowing the researcher to investigate convergence and divergence in detail (Smith, Flowers and Larkin, 2009).

IPA is primarily concerned with detailed accounts of individual experiences so the focus is on quality rather the quantity of the sample. Given the complexity of most human experiences, an IPA study is more likely to benefit from vigorous focus on a small number of cases (Smith, Flowers and Larkin, 2009). Patton (1990) believes that there are no strict criteria for a sample size in qualitative studies, since judgments about usefulness and credibility are ultimately left to the researcher and the reader. Given the practical issues such as time and lack of access to participants due to a global pandemic, I feel that a sample size of 8 research participants is adequate and acceptable. In keeping with the tradition of qualitative research and due to the practical implications of a global pandemic, a convenience sample was used.

Since this study seeks to obtain insights from InfoSec academics and InfoSec practitioners, there will inevitably be some variations in how the two groups experience the phenomenon of interest. Furthermore, other people within an organisation, such as CEOs, CIOs and end users may also be able to offer their input about the phenomenon of InfoSec awareness training.

In IPA, the focus is on the emic perspective whilst recognising that the emic perspective itself is an interpretation of the lived experience, necessitating that the researcher applies their own interpretation to the subject's interpretation (Smith and Osborn, 2004). As a practitioner-researcher with knowledge and experience similar to that of the research participants, it is inevitable that my own experiences will be infused into the data collection (interview) and data analysis stages and my own explicit beliefs will ultimately inform my interpretations (Groenewald, 2004). For this reason, I believe that it would not be possible for me to achieve the same depth of focus, verification, interpretation and validation of data in dealing with other groups of potential participants (e.g., CEOs, CIOs, end users). Furthermore, phenomenological research does not seek or claim to be generalizable. Participants are selected because of their ability to offer the researcher access to a particular perspective of the phenomenon. In other words, they represent a particular perspective rather than a population (Smith Flowers and Larkin, 2009). As such the research sample is not required to be representative of all groups that have experienced the phenomenon.

3.4 Research Instrument: Interviews

The most common methods of qualitative data collection are observations, focus groups and interviews. Each method is discussed here briefly with a particular focus on semi-structured interviews.

In qualitative research design, the researcher becomes the research instrument, i.e., the researcher is the primary method of data collection whether through observations, focus groups or interviews. This necessitates that the researcher has the ability to observe behaviours and conduct interviews.

Observations are a useful data collection tool to gain insights into a particular setting or behaviour. Qualitative observations are generally of two main types: participant or non-participant. In a participant observation, the observer/researcher becomes part of the observed setting whilst in a non-participant observation, the observer/researcher is an outsider 'looking in', not taking part in the setting/situation so as not to influence the setting (Bogdan and Biklen, 2006).

Being aware that they are under observation, the behaviour of a subject could change and affect the results. Observer bias in the form of selective perception of the observer could also distort the data. Qualitative observations tend to be expensive and time consuming in practice with the researcher having little control over the situation. The participants in this project are busy professionals and it would not be practical to carry out lengthy observations within their places of work due to the restricted timescale of the project. More importantly, observations would not the yield the rich insights into the InfoSec professionals' opinions and experiences to help me answer the research question.

Focus groups are a particularly useful data collection tool in qualitative research, allowing multiple voices to be heard within one sitting. It is a form of group interview that takes advantage of interaction between participants in order to generate data. However, the multiplicity of voices and interactional complexities during a focus group make it very difficult to develop and infer the phenomenological aspects of IPA (Smith, Flowers and Larkin, 2009: 71).

Smith, Flowers and Larkin (2009) advise caution in using focus groups in IPA studies and state that it can be quite difficult to use such settings to elicit experiential narratives. Groups discussions within focus groups are more likely to bring out attitudes and opinions about a given topic rather than provide detailed descriptions of individual participant's lived experiences. Smith (2004) posits that it is unlikely that research participants will be able to discuss their personal experiences in sufficient details and intimacy in the presence of other group members.

IPA as a research approach is best suited to a data collection method that will allow participants to provide rich, detailed, first-person accounts of their experiences. The term 'rich data' suggests that participants are given a chance to speak freely and reflectively to express their concerns thoroughly (Smith, Flowers and Larkin, 2009: 56). In depth interviews are commonly considered as the best method to allow participants to offer detailed accounts of their experiences.

Qualitative research interviews will almost always have some sort of structure to the way they are conducted. Unstructured interviews are generally preferred for conducting long-term field work as they allow participants to express themselves in their own ways and at their own pace. However, this form of interviews is closer to a conversation than an interview and tends to be skewed towards the interests of the interviewer (Gray, 2009).

In contrast, semi-structured in-depth interviews are often preferred in IPA studies as they allow participants to answer pre-set open-ended questions. For this project, the use of in-depth semi-structured interviews of InfoSec professionals that are involved in or affected by InfoSec awareness training / programmes offers me a rich picture of the phenomena. A phenomenological approach based on in depth open-ended semi-structured interviews helps to probe into participants responses and provides an opportunity for them to elaborate and clarify their responses. Interviews are regarded as 'introspective' techniques since they involve participants reporting on themselves, their views, beliefs and feelings. As a practitioner-researcher, a phenomenological approach allows me to put aside my own preconceptions and biases in order to gain a deeper understanding of the participants' subjective experiences, motivations and actions (Creswell, 1998). It also gives me an opportunity to expose any limitations in current understanding of the issues and develop alternative perspectives based on my own professional expertise.

Qualitative methodology is key to understanding the lived experience of research participants and face-to-face interview is the method of choice for generating qualitative data (Creswell, 2013). Indeed, face-to-face interviews are regarded as the 'gold standard' of qualitative research (Novick, 2008).

However, the COVID-19 global pandemic has demonstrated that in an era of social distancing, lock-downs and travel restrictions, face-to-face interviewing is not always feasible. As a result, for this research study, all of the interviews were conducted online via Skype and Zoom.

The use of online interviews in qualitative research is not a new phenomenon (Cooper, 2009; Turney and Pocknee, 2005). Whilst online interviews offer many benefits and a range of possibilities for the qualitative researcher, there were a number of practical, methodological and ethical considerations that needed to be taken into account.

One of the most obvious considerations is the use of technology and ensuring that the participants are able to access and comfortably use the chosen online platforms (Skype & Zoom). Technical difficulties such as sound and video quality and the speed of the internet need to be considered. Internet connectivity issues can interrupt the interview session, frustrating the participants and causing them lose focus and become disengaged (Ownsworth *et al.*, 2020). The latter could affect the flow of the interview and the rapport between the researcher and participant, making it difficult to obtain the detailed accounts sought by a phenomenological inquiry. Participants may also need to be assisted with setting up the camera to ensure that their face and torso is in full view in order to aid the researcher in observing any non-verbal expressions and cues (Archibald *et al.*, 2019).

In order to reduce the potential impact of technical issues, I provided participants with generic guidance on using the online platforms. I also provided the participants with a contingency plan to use an alternative platform in case they encountered problems with the main platform. I was able to mitigate most of the anticipated technical problems through brief practice sessions prior to the interviews to ensure that technology worked as required. I was also fortunate that the research participants themselves were high skilled, tech-savvy professionals that were proficient in the use of such technologies.

During face-to-face interviews the researcher is able to standardize the environment and create a positive atmosphere for the participants. The use of online interviews meant that as a researcher I had little control over the physical environment surrounding the participants. A disruptive environment has the potential to shift the focus from the interview (Deakin & Wakefield, 2014).

Conversely, online interviews could offer the participants an environment conducive to their everyday needs and may actually offer greater privacy for the interview process (McCoyd & Kerson, 2006). In order to mitigate issues related to participant attention and concentration, participants were offered guidance on how to set up an appropriate environment prior to the interview.

One of the primary goals of phenomenological research is to obtain authentic and rich data from the participants. For the researcher, it is crucial to build a rapport with the participants in order to facilitate open dialogue and to elicit authentic data (Creswell, 2013). The participants in turn must feel comfortable when describing their lived experiences, particularly when discussing sensitive topics such as InfoSec awareness training. However, in the absence of a face-to-face interaction the quality of the researcher-participant connection could be compromised, resulting in a loss of the richness of interaction (Archibald *et al.*, 2019).

In order to mitigate some of the aforementioned issues associated with online interviews, I employed certain strategies to build rapport and exhibit sincere interest in the participants and their experiences (Ownsworth *et al.*, 2020). This was achieved by informally communicating with the participants before the interviews. Although it is difficult to maintain eye contact during an online interview, I made sure to focus on the camera rather than the screen when speaking, in order to mimic virtual eye-contact (Ownsworth *et al.*, 2020).

Wiederhold (2020) points out that the exponential increase in the use of video-calling and virtual meeting platforms during the pandemic has shed light on the exhausting nature of such technologies. I was very conscious of the increased risk of the participants being fatigued during the online interviews. Although I could not rely on easily observable nonverbal body cues available during face-to-face interviews, I still remained vigilant to any signs of fatigue. I highlighted this risk to the participants and encouraged them to inform me when they felt tired and offered breaks where appropriate.

Online interviews are considered to be more cost and time efficient compared to face-to-face interviews since the need for travel is eliminated and there are opportunities for more expansive recruitment of participants (Seitz, 2016).

(Ownsworth *et al*. (2020) point out that although it is very easy and convenient to arrange online appointments, there is also a tendency on the part of the participants to cancel and reschedule interviews just as easily. This could be due to participants perceiving an online appointment to be less formal than a face-to-face appointment. I made sure to maintain frequent contact with the participants and reminded them about the interview along with an option to cancel / reschedule the appointment.

3.5 Researcher Bias

Due to the nature of qualitative research, the researcher is a central part of the research and researcher's biases could have an impact on the research. Creswell (1998) notes that in phenomenological research, a researcher is also the instrument for the research and brings his/her own experience relevant to the research area that inevitably colours their ability to develop theory from the data.

Strauss & Corbin (1990) describe theoretical sensitivity as the attribute of having insight and the ability to give meaning to data. They note that everyone comes to the research situation with varying degrees of sensitivity, depending on previous reading and experience relevant to the area.

Phenomenological research in particular requires that a researcher should be transparent and make their personal biases and values known to the readers in reporting research findings. This enables the reader to make an informed judgement about the work (Creswell, 1998; Strauss & Corbin, 1990).

I approached this research project with two main biases resulting from my industry and research experience. I have been working in the Computer Communications and InfoSec industry for over fifteen years. During this period, I worked in a variety of highly technical and leadership roles including Chief Technical Officer, Senior Network Consultant, IT Security Solutions Architect, Technical Instructor and Researcher.

In particular, I have worked in a similar role to that of the research participants, providing strategic and operational oversight of organizational InfoSec operations and ensuring that adequate resources and processes were in place to safeguard against internal and external security threats. In addition, I conducted independent research into the area of organizational security policies and the role of security awareness training programmes in reducing risk of security breaches.

My professional background presented a significant challenge as I tried to remain impartial and objective during the interview process. Whilst this type of bias is an inevitable part of qualitative research, I have tried to implement the techniques suggested by Strauss and Corbin (1990) to reduce the impact. This includes adopting an attitude of reflection and scepticism during the interviews and periodically stepping back and asking: what is going on here? I needed to be my own critic and had to consider alternative interpretations wherever possible (Strauss & Corbin, 1990).

3.6 Research Trustworthiness

I understand that as a researcher I must be able to demonstrate the validity and reliability of my research to the wider research community. Qualitative research is often criticised as being sloppy, subjective, observational, and lacking in rigour (Lincoln & Guba, 1985). However, the traditional concepts of validity and reliability (as used in quantitative research) cannot be addressed in the same way in qualitative research. A number of measures have been put forward to address the issue. In particular Guba's (1981) constructs have been widely accepted and were used as a basis to address the issue of research trustworthiness.

In quantitative studies, researchers often use traditional terms such as internal validity, external validity, reliability and objectivity to assess the rigour of quantitative research studies.

Guba's constructs correspond directly to the criteria employed in quantitative research (i.e., internal validity, external validity, reliability and objectivity):

- Credibility (to address: internal validity)
- Transferability (to address: external validity/generalisability)
- Dependability (to address : reliability)
- Confirmability (to address : objectivity)

Credibility

In qualitative terms, credibility seeks to ensure that the study measures or tests what is actually intended. I made the following provisions to address this:

- The adoption of a well-established research methodology (IPA), data collection and analysis methods that have been successfully utilised in previous comparable studies (Smith, Flowers and Larkin, 2009; Spinelli, 2005 & Groenewald, 2004; Hycner, 1999; Lester, 1999; Somasundram, 2007; Ridoutt, 2008; Hanna, 2020).
- Prolonged engagement with participants to build rapport and gain familiarity with the participants and their organisations before data collection. This helped to establish a relationship of trust (Lincoln & Guba, 1985).
- Data triangulation by selecting participants from different personal, professional and organizational backgrounds so that viewpoints and experiences can be crosschecked and verified.
- Ensured participant honesty by giving opportunities to refuse participation. This helped to ensure that data collection involved only those genuinely willing to take part.
- Utilised my own background and experience as a major instrument of data collection and analysis (Patton, 1990).
- Peer debriefing checks (critical friends) – used work colleagues, supervisor and consultant to critically review research design, data collection and data analysis stages

- Member checks - asked the participants to read the interview transcripts before data analysis to verify that their views had been captured accurately. Also, after data analysis, I sought input from the participants about the preliminary findings.
- Related my findings with previous studies and existing body of knowledge.

Transferability

In qualitative terms, this refers to the extent to which the research findings of one study can be applied to other situations (Merriam, 1998). This is very difficult to achieve in phenomenological research since the findings will always be very specific to particular participants and context (Erlandson et al, 1993).

Stake (1994) argues that although each qualitative study may be unique, it is also a subset of a broader group, and therefore there is a case for some transferability. Although it would be difficult to make any explicit transferability inferences, it is believed that by providing sufficient contextual information, readers can ultimately determine how far they can apply the findings to their own / other situations (Lincoln & Guba, 1985). The findings of this research will ultimately inform my professional practice and the positive outcome of this project will be disseminated to my community of practice. In this way, I will be making a contribution to my professional practice.

Dependability

In qualitative terms, this seeks to determine the extent to which other studies would obtain similar results if the research were to be repeated, in the same context, with the same methods and the same participants.

It is difficult to satisfy such conditions in qualitative research. As Marshall & Rossman (1999) point out that the nature of the phenomena being studied in qualitative research is very fluid and the researcher's observations and interpretations are always closely tied to the particular situation under study.

Lincoln & Guba (1985) argue that dependability is closely tied with credibility and a demonstration of the latter automatically ensures the former. In order to address the dependability requirement, a detailed account of the research process was provided in the previous sections to enable future researchers to repeat the work. In particular, details of the research design, data gathering stages as well as a reflective appraisal of the project has been provided in this report.

I acknowledge that threats to reliability cannot be completely eliminated. In order to further strengthen the reliability of the project, I requested one of my professional colleagues to act as a 'critical friend' during the data collection and analysis phases. I found it very useful to have someone from within my own professional practice to offer constructive criticism and useful suggestions and guidance to address the issues of reliability.

Confirmability

This is the qualitative researcher's equivalent of objectivity. The use of triangulation techniques discussed earlier helps to reduce the effect of researcher's own biases. An account of my own beliefs and assumptions about the research topic has been provided as well as recognition of any shortcomings in the methods employed (Shenton, 2004). An audit trail of how the data was gathered, processed and resulted in the formation of new theory has been provided in a diagrammatic form.

3.7 Triangulation

Triangulation is a strategy employed to establish the credibility of qualitative research in order to ensure that the findings are rich, comprehensive and robust. It seeks to mitigate weaknesses and biases linked to single method, single observer, single theory studies (Bogdan and Biklen, 2006). Triangulation provides a mechanism for crosschecking and testing out arguments and perspectives from different viewpoints in order to strengthen evidence for support of particular claims when studying the same phenomenon.

Polit & Beck (2006) describe four main types of triangulations in order to confirm the consistency of the findings. Method triangulation uses multiple data collection methods; data triangulation employs different data sources within the same method; investigator triangulation makes use of more than one researcher/analyst to review the findings during data collection and analysis stages whilst theory triangulation focuses on multiple theoretical perspectives to analyse and interpret the data.

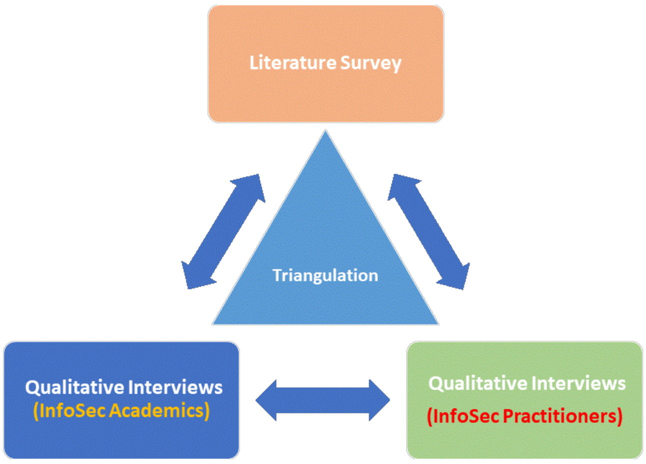


Figure 9: Data Triangulation

For this research project, I utilised data triangulation, using different data sources (literature survey, qualitative interviews with InfoSec academics and InfoSec practitioners) to understand the phenomenon of InfoSec awareness programmes and human errors and to verify the significance of the issues from multiple sources. This allowed me to increase external validity by comparing and crosschecking the data derived from the different sources using the same qualitative method. I was able to compare the perspectives of InfoSec academics with those offered by InfoSec practitioners during the interviews and relate these back to the literature survey.

Data triangulation is also helpful in corroborating the perspectives of the different participant types with my own professional experience (Smith, Flowers and Larkin, 2009). Yin (2009) asserts that data triangulation also addresses the issue of construct validity since multiple sources of data basically provide multiple measures of the same phenomenon.

I also employed aspects of investigator triangulation as I was fortunate to have a supervisor and two professional colleagues to offer valuable technical and research related input to this project.

The two types of triangulations mentioned above helped to ensure that this research was not biased from single method, single observer and single theory studies during data collection, analysis and interpretation stages of the project.

3.8 Ethical Considerations

Ethical practice is an integral part of qualitative research and must be observed throughout the data collection and analysis stages. A number of ethical issues could arise during the course of this research study and will be considered in this section.

It could be argued that for a study with a small sample size, it would be sufficient to obtain verbal informed consent from the participants for the online interviews. However, when conducting phenomenological research involving participants that have experienced a particular phenomenon, written permission should be obtained from the participants (Creswell, 2013). There may be a tendency on the part of the participants to underestimate the implications of giving their consent.

A Participant Information Sheet (PIS) was prepared (Appendix C) and given to the potential participants in order to give them some generic background to the study. This allowed the potential participants time to carefully think about any concerns they may have had about taking part in the research. It was also ensured that unnecessary information about the nature of the research was not given away that could potentially bias the results. In addition to obtaining written informed consent from the participants for data collection, consent is also required for the likely outcomes of data analysis. This is particularly relevant for an IPA study since verbatim extracts from participants are included during the analysis stage (Smith, Flowers and Larkin, 2009).

It is common in qualitative research studies to offer participants the option to withdraw at any time. However, this is something that needs to be clarified to the participants, perhaps by offering the option to withdraw up to a certain point. Clearly, it would not be possible for a participant to withdraw from a study once the data has been analysed and the finding published. Based on the recommendations by Smith, Flowers and Larkin (2009), participants were offered the option to withdraw from the study up one month after the initial interview, combined with the opportunity to review the interview transcript for accuracy.

Due to the fact that this study was based on an IPA approach with in-depth interviews with the participants, the participants were informed about how much time would be required from them as well as a broad overview of the type of information being sought. InfoSec is an extremely sensitive topic and there is generally mistrust by security professionals of any attempts to seek information about their practices and behaviours. As Kotulic & Clark (2004) point out that many previous studies in InfoSec have experienced poor response rates due to the intrusive nature of the subject.

Due to the online nature of the participant interviews, privacy and confidentiality was of particular concern. The use of online platforms (Skype and Zoom) means that there is potential to record interview conversations, save online data and track participant identity and location (Archibald *et al.*, 2019). In making use of these online platforms, I took extra steps to ensure that online connections were secure. I made use of VPN software to establish encrypted internet connections before using the interview platforms and also advised all participants to do the same. In addition, when setting up virtual meetings for the interviews, a password was used for each new online meeting. I also made sure to communicate the potential security risks of online interviews with all the participants.

I exercised caution in wording the interview questions so as not to appear too intrusive and to ensure that the participants felt comfortable in their responses. This was also important because if the participants inadvertently revealed some sensitive information about their organization, they could become agitated and refuse to participate in any future research. I ensured that participants did not feel compelled or pressurised to take part in this research. As a researcher it was important to be mindful of issues relating to power relations and vested interests. It was important to avoid being perceived as steering the research in a particular direction or expecting certain type of responses from the participants.

I was conscious of the fact that after having built a rapport and a relationship of trust with the participants, there is likely to be a tendency for the participants to speak freely about their professional practice, sometimes unintentionally revealing information that was not intended for the interview. In such situations, I would be very careful not to exploit the participant's candour and possible vulnerability. I would bring the matter to their attention and assure them that the unintentionally revealed information would not be used in the research in any way.

During the course of the interviews, some participants expressed their opinions about their colleagues and other individuals in the organization, attributing blame to them for certain failures and for being barriers to success in previous projects. This was dealt with in a sensitive manner and the anonymity and confidentiality of the participants was protected.

I also needed to agree with the participants the extent to which their identity and confidentiality needed to be concealed and had to make a judgement about the appropriate balance between revealing such information and remaining faithful to the research.

Smith, Flowers and Larkin (2009) refer to the concept of 'representation', arguing that some participants may be delighted to have their experiences represented within a professional or academic forum. However, they emphasise that this should not be at the expense of their anonymity. I feel that the issue of anonymity is particularly crucial for the participants in this study due to the sensitive nature of InfoSec and the potential adverse effects this could have on the participants and their organisation's reputation.

I took care to ensure that confidential information such as participant names, addresses and other personally identifiable information (PII) was stored in a safe and secure manner.

As a practitioner-researcher conducting research in the same area of professional practice as the participants themselves, I inevitably had my own personal views on the issues discussed during the interview. I was very careful not to be distracted and get drawn into debates. This also required me to act cautiously and reflectively in balancing the needs of the research and the need to maintain a professional relationship with the participant.

As a practitioner-researcher I was also mindful of the issue of conflicts of interest in the sense that the participants could regard the research area as threatening their interests or could feel that they were being exploited for my personal interests.

Another possible issue that could arise is due to the dual purpose of this research that is my own professional development and the need to fulfil the requirements of the DProf programme. I was aware that I could be perceived as an external change agent with no particular responsibility towards the participants after the project is completed. To address this, I assured the participants that their views and input was valued and would be incorporated into the research findings. I also explained that as a practitioner-researcher I have a professional interest and stake in the success of this research study as well as our community of practice. As a qualified professional I am bound by the ethics of my profession and reputation in the field.

Summary

This chapter provided a critical discussion of the research methodology employed in this project along with my justifications for the choice of this particular methodology. My stance as an insider practitioner-researcher was also considered and how this has affected my overall approach to this project, including the choice of research methodology. The details of the chosen methodology and research design were presented here, including sampling method, sample size, research instrument and data collection. The issues of researcher bias, validity and reliability of the research as well as triangulation as a means to reinforce credibility were also considered. Finally, a discussion of issues of confidentiality and research ethics was also provided.

In the next chapter, I will apply the theoretical and philosophical principles of phenomenology as described in this chapter to describe the process of data collection, data analysis and the construction of meaning from the collected data.

Chapter 4: Project Activity

Overview

This chapter is divided into three main sections. The first section starts with a self-reflection process through the concept of epoche, whereby I clarify any preconceptions and judgments toward the phenomena in question.

In the second section, I apply the theoretical and philosophical principles of phenomenology as described in the previous chapter to describe the process of data collection (interviews) as well as my reflections on this process. As part of this section, the selection of research participants, the formation of interview questions, their evaluation by an expert panel, pilot test interviews and the actual interviews are described. This section concludes with a reflective account of the data collection process and a brief account of important issues related to management and security of research data.

In the third section, I again apply the theoretical and philosophical principles of phenomenology as described in the previous chapter to describe the process of data analysis and the construction of meaning from the collected data. The different stages of phenomenological analysis are described in detail and a reflection on the data analysis and construction of meaning is also offered. The diagram below illustrates the various stages of the project activity.

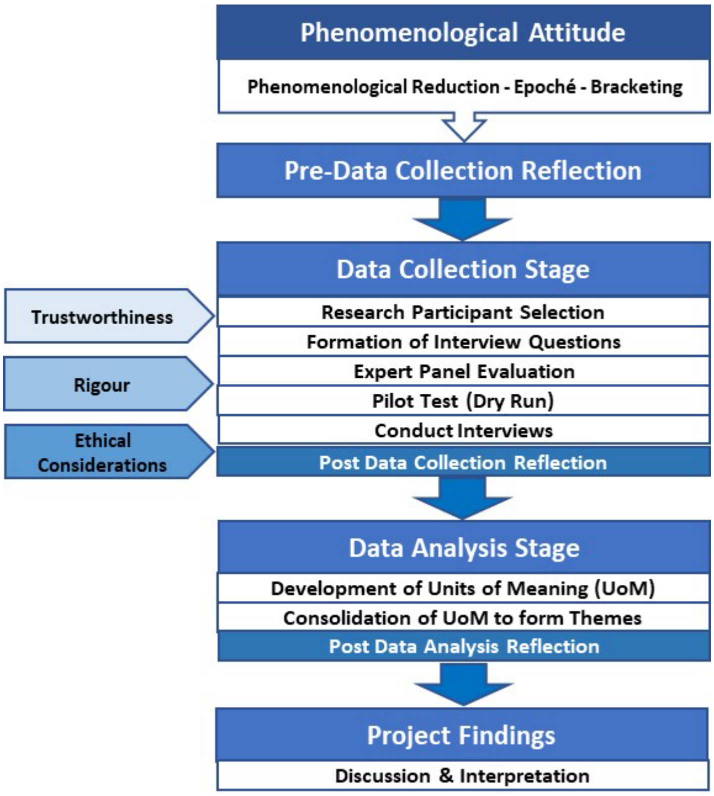

Phenomenological Attitude
Phenomenological Reduction - Epoché - Bracketing
Pre-Data Collection Reflection
Data Collection Stage
Trustworthiness
Research Participant Selection
Formation of Interview Questions
Rigour
Expert Panel Evaluation
Pilot Test (Dry Run)
Ethical Considerations
Conduct Interviews
Post Data Collection Reflection
Data Analysis Stage
Development of Units of Meaning (UoM)
Consolidation of UoM to form Themes
Post Data Analysis Reflection
Project Findings
Discussion & Interpretation

Figure 10: Project activity stages

4.1 Pre-Data Collection Reflection

Research in phenomenological tradition is often characterized by the researcher's motivation and commitment to bring about a change in the status quo and a 'willingness to reflect upon the consequences of this commitment' (Smith, Flowers and Larkin, 2009: 42). Although the IPA researcher is not required to have an 'insider' status, it is important to consider the extent to which the researcher can relate to the concerns, claims and experiences of the participants. In a sense, the researcher is required to be able to imagine what an insider status could entail (Smith, Flowers and Larkin, 2009: 42).

Subjectivity and interpersonal experiences play an important role in qualitative research. It follows therefore that as a researcher I should provide a personal reflective account of any previous knowledge and experience in the participants' field of practice so the reader can see for themselves the journey that this research study has undergone (Alase 2017). Smith, Flowers and Larkin (2009) point out that the issue is not about how much of the previous knowledge should be declared but simply that the researcher should be candid about the possible ramifications of their preconceptions (fore-structure of knowledge). Although the researcher may not be able to access and name all their preconceptions at the start of the research, it is nevertheless useful to reflect on what is accessible. Alase (2017) asserts that IPA is a participant-oriented interpretative approach that requires the researcher to be in a state of constant self-reflection, with a sense of 'one-self' and a perception that one is intruding into the participants' private space.

As an insider practitioner-researcher with knowledge and experience in the same field of practice as the participants, I can relate to their lived experiences, and this inevitably forms an impression in my mind about the participants and the phenomenon under study. However, I will endeavour to suspend my judgements until all the data (interviews) has been gathered. It is impossible for me to completely detach my personal interpretations from something that is personally interesting to me, having engaged in the same field of practice for many years. Therefore, I will revisit my assumptions and contextual insights during the data analysis stage to help me judge and evaluate the participants' responses in order to elicit the meanings from their individual experiences. I view the participants as my co-researchers in this research project (Pope, 2020), sharing a common phenomenon related to InfoSec awareness programmes that we explore together in the course of constructing meaning in order to answer the research question. My experience will inevitably be infused into the data analysis stage since my own professional practice is also a part of the research object under consideration.

Smith, Flowers and Larkin (2009) warn that in IPA studies, data collection (interview) stage is the only time when the researcher must keep their preconceptions out of the process so as not to distort or bias the research findings. This is especially pertinent to a study of this kind involving an insider researcher scenario. I endeavoured to make my personal biases, preconceptions and judgments towards the phenomenon transparent and explicit by assuming a 'phenomenological attitude' (Ngulube, 2017). This attitude required me to observe the phenomenon (InfoSec awareness programmes) whilst withholding my judgement about it (using personal experience or existing literature), stripping away any presumptions and biases, essentially reducing the lived world down to its bare essence so that I could study and freely question everything about it. This phenomenological reduction is referred to as epoché and involves 'bracketing' off other perspectives of the lived world so that one can focus on the essence of the phenomenon. My goal was to create an open and unbiased environment for the participants, where I could understand the phenomena from their perspective, without impinging on their narrative.

I also went through a period of focused introspection in which I transcribed my thoughts, feelings, motivations and expectations through a series of self-reflective questions:

- Why am I pursuing a doctorate in this field? How does it benefit me, the participants, and my professional practice?
- What do I expect from the participants?
- What are my own views on this topic? How would I answer the same interview questions if I was a participant?
- What contribution do I expect to make to the field? How significant is it likely to be?
- Do I have another agenda?

I revisited the DPS 4520 Review of Professional Learning module, which led up to the present project phase, to help me reflect on my journey and the experiences that have shaped my professional practice. I assumed a reflexive attitude in order to discover my own sense of being and question my motivations, expectations, beliefs, and values in pursuing a DProf. I reflected on different facets of my personal and professional life; as a student, InfoSec professional, lecturer, researcher, author, and doctoral candidate to help me clarify my assumptions and judgements about the field of InfoSec and awareness training. I have provided a brief account below.

I developed an interest in computers from an early age when I would spend a lot of time experimenting with hardware and software components. I chose to study Computer Science at university but dropped out at the end of the first year as I became very disillusioned with the degree programme. I found that there was a lot of theory and abstract concepts but not much emphasis on practical application of this knowledge. This made me question the degree's worth and applicability in the real world.

I continued my journey through self-study and experimentation and developed an interest in computer networking and InfoSec. I completed several specialised InfoSec certification courses and took up an exciting and life changing role with a consultancy firm specialising in networking and InfoSec. I decided to pursue this role by taking time out from my studies, against the advice of family and friends. This role proved to be an amazing experience as I gained invaluable professional experience working with high profile corporate customers on large scale projects, implementing some of the leading-edge technologies in the field.

I later returned to my studies, equipped with real life practical experience, and completed a BSc in Computer Networking with a specialist focus on InfoSec. I hugely enjoyed and excelled in my studies as I was now able to appreciate the correlation between theory and practice. I pursued this degree programme whilst maintaining a role in the industry. As a result, for my final year project, I was able to conduct an industry-based research project with a practical and tangible impact for my employer. This was also my first exposure to practice-based research that helped me to develop essential collaboration, project management, analytical and research skills that formed an excellent foundation for a later career in the industry. This was a challenging but hugely satisfying and rewarding part of my early career.

After graduation, equipped with a First-Class Honours degree and practical experience in a specialised field, I returned to industry with a renewed zeal to advance even further. I held a variety of roles in which I designed, authored, and delivered numerous highly specialised InfoSec courses for various clients. Having gained specialised practical experience and an academic qualification, I was able to deliver these courses with great confidence and authority.

As I acquired more experience in my specialist area, I assumed more project management and team leadership responsibilities, providing consultancy and training services to large corporate clients. I excelled in these roles and after a period successfully applied for the post of Chief Technical Officer (CTO) with another IT organisation. Once again, InfoSec was a major focus in this role. I acquired invaluable skills and experience, gaining valuable insights into the way large organisations operate and the skills required to provide strategic leadership. This was also a period of considerable personal growth and professional development for me. I had the opportunity to complete various training and development courses. In addition to specific technical training, I completed Project Management, Time Management, Strategic Visions, Negotiation Skills and Leadership and Decision-Making courses. It was a steep learning curve that gave me more confidence in my abilities and prepared me to deal with new challenges ahead.

Having acquired considerable professional experience in my field, I reflected on my journey and felt a strong desire to make a positive contribution and give something back. It was with this intention that I decided to join a University as a Technical Instructor and Network Security Architect. During my early university days, I had been frustrated due to the lack of emphasis on practical application of technical knowledge. I joined academia with a strong grasp of computer networking and InfoSec, extensive technical experience, and strong strategic and business knowledge. In this role, I designed and revised several postgraduate courses to incorporate up-to-date practical and industrially relevant content and research project work. I really enjoyed working in this environment and found it particularly fulfilling to work with students, providing advice and guidance for their future careers.

Working in an academic environment also sparked an interest in me for further study. After a period of intense deliberation and having evaluated my skills and experience, I recognised that although I had a wealth of practical experience, I needed to enhance my academic knowledge and skills in my chosen field. I decided to pursue a Master’s degree specialising in InfoSec in order to consolidate my past practical experience and personal interest in a way that could enhance my future career prospects. The Master’s degree was an excellent learning opportunity that greatly broadened my knowledge and understanding of the field of InfoSec. I had the opportunity to engage in various academic writing activities that further reinforced my analytical and research skills. I participated in various mini research and development projects as part of small teams. I learnt a great deal about the importance of cultural differences and how social and educational background tends to affect people's outlook. The overall experience and personal reflection helped me to analyse my own behaviour, motivations, and personal values.

As I pursued my postgraduate studies, I moved to another role in the higher education sector, as a senior lecturer and head of training and consultancy that afforded me greater flexibility and freedom to plan my studies around work. I taught various networking and InfoSec modules. As with my previous roles, the emphasis was on delivering industrially relevant content to equip students with the necessary professional and technical skills to pursue a career in the InfoSec industry. In this role, I also had the opportunity to focus on my research interests in the field of InfoSec, resulting in numerous publications in international peer-reviewed journals.

As outlined above, InfoSec has been a constant thread throughout my professional practice. As I headed into the next major part of my DProf project, I brought with me extensive knowledge and expertise in the field of InfoSec acquired over a period of more than 15 years. The central theme of this project therefore is an area of InfoSec that I have engaged with both in academic and work-based contexts.

The role of human behaviour in InfoSec represents a conundrum that researchers and practitioners have tried to grapple with since the early days of computers. InfoSec awareness training programmes are undoubtedly crucial in mitigating security threats and breaches. However, I believe that there has not been sufficient attention focused on the human element for it to be effectively integrated into awareness programmes to manage human behaviour. I believe that the approach taken in seeking a viable solution to the human problem in InfoSec must be transdisciplinary with insights from other disciplines such as psychology, sociology as well as InfoSec academics, researchers, and practitioners.

Using the latter as my frame of reference, this project is an effort towards finding a viable solution to the human problem in InfoSec using insights from two of the aforementioned disciplines: InfoSec academics and practitioners. In order to bring about any change or improvement in the status quo, it is necessary to hear the authentic experiences of these professionals so that the essence of the issue could be understood, and possible solutions could be proposed. I believe that the research problem of this project is of great importance for organisations and more broadly for a world that is increasingly reliant on internet technologies.

In summary, I have outlined the essence of my unique experiences and any preconceived notions about the phenomenon. As I outlined and reflected on some of the most relevant themes, I realised that there was a great deal that needed to be bracketed off before commencing the data collection phase of the project. I found the above process of self-reflection extremely valuable and at the end of this reflective journey, I feel that I am sufficiently equipped with a phenomenological attitude to commence the process of data collection.

4.2 Data Collection Stage

The aim of an IPA interview is to enable an interaction that allows the participants to tell their stories, in their own words (Smith, Flowers and Larkin, 2009). IPA is a participant-oriented research approach in which a researcher develops bonds with the participants through interpersonal and interactive relationships, facilitating smooth information gathering and subsequent analysis (Alase, 2017). Smith, Flowers and Larkin (2009) assert that the researcher and the participant engage in a dialogue during the interview process such that the initial questions may be adapted in light of participant's responses, allowing the researcher to explore other interesting areas which may arise during the dialogue.

As the main researcher, I was the primary instrument for the data collection phase of this research project. In qualitative research, conducting on-to-one interviews with participants is an established method of data collection that provides each participant the opportunity to reflect and share their experiences. In particular, semi-structured interviews allow the researcher to focus on key features of the phenomenon in question through coordinated questions to seek out greater detail (Smith, Flowers and Larkin, 2009).

What follows is a description of the main stages of the data collection process.

4.2.1 Research Participant Selection

The population for my research study was InfoSec professionals (academics and practitioners) with extensive research-based theoretical and experimental knowledge as well as applied, hands-on experience of InfoSec threats and awareness training programmes.

InfoSec practitioners provide strategic, tactical and operational oversight of an organization's InfoSec operations, ensuring that businesses understand the importance of security and adherence to policies to safeguard against internal and external security threats. InfoSec practitioners assume a variety of job titles including InfoSec specialist, InfoSec architect, InfoSec analyst, InfoSec awareness training specialist and chief information security officer (CISO). InfoSec practitioners are involved in the design and implementation of the organisation's InfoSec awareness programmes with strategic or tactical level oversight.

InfoSec academics work in a variety of academic and research-oriented environments such as universities, research institutes and laboratories. InfoSec academics keep up-to-date on the latest developments in information security threats and investigate and analyse their capabilities. They also attempt to understand the cybersecurity threat landscape, predict latest trends and attack vectors and develop and recommend appropriate security responses. Their research into human factors of InfoSec and psychological models of human behaviour are particularly useful in understanding the role of human behaviour in the success/failure of InfoSec awareness programmes.

The combination of research-based and practical experience offered by the research participants offers me rich and meaningful insights into the phenomenon under investigation.

A combination of email, social media and telephone inquiries as well as referrals using professional contacts I had built through many years of experience in the field were used to find suitable InfoSec academics and practitioners within different organizations and institutions. I also applied a snowball strategy to help attract more participants for this research. This was achieved by soliciting help from the participants who had already agreed to take part in the research. These participants were able to recommend suitable candidates for this research.

In the first instance, the appropriate senior management for each organization was identified in order to seek their approval for this research. The latter acted as the gatekeepers responsible for allowing access to the relevant InfoSec academics and practitioners within the organisations. A gatekeeper is typically an employee or member of the same organisation, without any particular relationship with the researcher, that can facilitate the potential candidates to participate in the study (Peticca-Harris, deGama, Elias, 2016).

The gatekeeper in each organisation was requested to forward my initial email invitation letter (Appendix A) and the pre-screening questionnaire (Appendix B) to potential candidates. The criteria used to assist the gatekeepers in identifying suitable candidates for the research included the aforementioned descriptions of the roles of InfoSec practitioners and InfoSec academics.

The eligibility criteria for the organisation included:

- Small to medium-sized enterprise (SME) with fewer than 250 employees
- Engaged in professional, technical or scientific activities
- Maintains a chief information officer (CIO) and/or a chief information security officer (CISO) or someone with equivalent responsibility and authority
- Has implemented and manages an InfoSec awareness training programme
- Engaged in research and development in the area of latest InfoSec threats and attack vectors with a particular focus on the role of human factors in InfoSec

Gatekeepers enjoy a position of trust and understanding with other employees of the organisation which they can leverage to ensure smooth coordination between the researcher and the research participants (Amundsen, Msoroka, & Findsen, 2017). I made use of the gatekeepers to assist me in gaining access to suitable participants for the study. The gatekeepers were able to evaluate the eligibility of potential participants using the aforementioned criteria and offer a list of potential participants. InfoSec awareness training is often considered to be a sensitive topic and organizational leaders are generally reluctant to allow access to qualitative data such as interviews. However, I believe that the use of gatekeepers greatly improved and aided the process of participant recruitment. Using the gatekeeper as an intermediary, I was able to allay any concerns and fears expressed by the senior management and the potential participants themselves.

A pre-screening questionnaire (Appendix B) was designed to gather basic information about the potential participants to ensure that the eligibility criteria was met for the research study. The information requested included name, age, gender, education level, professional certifications, research publications, current job title, employment status / history, size of the organisation (no of employees) and number of years of experience in InfoSec. It was clarified to the potential candidates that the completed questionnaire would be screened to determine eligibility and that participation was not automatically guaranteed.

A total of 31 potential research candidates were contacted and 19 candidates responded positively to my initial recruitment efforts. Based on the information obtained from the pre-screening questionnaire, 4 of these candidates were deemed ineligible for participation in the research. Another 3 of the candidates were withdrawn from the selection process due to long lapse in communication whilst 1 candidate withdrew voluntarily. From the remaining pool of 11 respondents, a total of 8 candidates were selected (4 InfoSec practitioners and 4 InfoSec academics) for interviews and all of them approved and agreed to the use of subsequent interview transcripts for this research. The remaining 3 candidates were kept as reserves and were also used in the expert panel evaluation and pilot testing of interview questions. The reserve participants were not needed for the data collection stage as saturation was reached with 8 interviews and additional interviews were not expected to improve or change the results.

Total No of Potential Candidates Contacted	31
Positive Responses	19
Deemed Ineligible	4
Withdrawn (lack of communication)	3
Withdrawn (voluntarily)	1
Candidates Selected for Interviews	8
Reserve Candidates	3

Table 1: Research participant selection

The information provided on the pre-screening questionnaire (Appendix B) was used to determine if potential participants met the inclusion criteria for this study. Patino and Ferreira (2018) assert that inclusion / exclusion criteria is an essential component of qualitative research. It allows the researcher to set constraints in order to seek out the participant attributes that are important to answer the research question. Conversely, the exclusion criteria bring to attention participant attributes that are likely to have a negative impact on the success of the research. I established an inclusion criterion which combined with my own professional experience and judgement helped me to focus my efforts on selecting the most data-rich participants with a confirmed history of lived experiences. The main features of the inclusion criterion are as follows:

- Must be willing to share InfoSec related professional experiences
- Education level (see table below)
- Research publications
- Professional certifications (see table below)

- Current job title / responsibility / experience
    - As an InfoSec practitioner, must occupy a leadership position with responsibility for implementing/oversight and maintaining InfoSec awareness programmes
    - As an InfoSec academic, must have a senior research role with an established track record of peer reviewed academic publications in the areas of InfoSec threats, human factors and InfoSec awareness training
- The organisation has an InfoSec awareness programme in place
- The organisation is an SME (small to medium enterprise) with fewer than 250 employees

In order to simplify the eligibility criteria, various qualification categories were created for both InfoSec practitioners and academics.

For InfoSec practitioners:

Category 1:	InfoSec practitioners with at least 10 years of experience in InfoSec (one or more organisations) and a bachelor's degree.
Category 2:	InfoSec practitioners with at least 5 years of experience in InfoSec (one or more organisations) and a Master's degree or higher.
Category 3:	InfoSec practitioners with at least 5 years of experience in InfoSec (one or more organisations) and a minimum of two industry recognised InfoSec related professional certifications.

Table 2: Selection criteria for InfoSec practitioners

For InfoSec academics:

Category 1:	InfoSec academics with at least 10 years of experience in InfoSec (one or more organisations), a minimum of three peer-reviewed publications in InfoSec (threat vectors, human factors) and a bachelor's degree or higher.
Category 2:	InfoSec academics with at least 5 years of experience in InfoSec (one or more organisations), a minimum of three peer-reviewed publications in InfoSec (threat vectors, human factors) and a Doctorate.

Table 3: Selection criteria for InfoSec academics

Creswell (2013) emphasizes the importance of homogeneity amongst participants in IPA research studies in order to provide a rich and descriptively deep understanding of the perceptions among their lived experiences. Consequently, all 8 of the research participants were recruited from within the UK to ensure homogeneity of experience and access to rich and detailed accounts whilst allowing comparative analysis of experiences.

The selection criteria were restricted to small and medium-sized enterprises (SME) with fewer than 250 employees. SMEs account for over 99% of all UK businesses and are enormously important to the UK economy (GOV.UK, 2020). The selection process focused on organisations engaged in professional, technical and scientific activities. In addition, I gave preference to organisations that maintained a chief information officer, a chief information security officer, or someone of equivalent responsibility with the authority to implement and enforce InfoSec policies and awareness training programmes. In case of InfoSec academics, the selection process was focused on potential participants with research experience of the latest developments in information security threats, trends and attack vectors with a particular focus on the role of human factors in InfoSec.

All of the participants were engaged in InfoSec roles (academic or industry), with a minimum accumulated experience level of 6 years in any combination of roles. This provided me with a homogenous pool of experience to draw from, facilitating capture of common features between different experiences and offering a deeper understanding of the participants' lived experiences. The table below lists the selected participants using participant ID codes, along with their relevant professional experience.

Participant ID Code	**Experience as an InfoSec Professional**
ISA1	8 Years / PhD / 5 peer-reviewed publications
ISA2	12 Years / PhD / 10 peer-reviewed publications
ISA3	6 Years / MSc / 8 peer-reviewed publications
ISA4	9 Years / MSc / 11 peer-reviewed publications
ISP1	13 Years / BSc / CCISP, CISM, CCSP
ISP2	6 Years / MSc / Security +, CEH
ISP3	11 Years / CISSP / CCSP / Security +
ISP4	8 years / BSc / CISSP / CCNP Security

Table 4: Participants' professional experience and qualifications

Research participants with more experience are expected to be in management / leadership positions with decision-making authority. More experienced participants are also more likely to hold professional certifications such as Certified Information Systems Security Professional (CISSP) and Certified Information Security Manager (CISM) which require advanced knowledge and a minimum level of InfoSec experience before they can be awarded.

4.2.2 Formation of Interview Questions

The central research question of this project is: *What are the main shortcomings in existing information security awareness training programmes and how can these be addressed in order to reduce human errors?*

From the literature review, it has already been established that human error is one of the main causes of security breaches in InfoSec. It has also been determined that InfoSec awareness training is perhaps the single most important measure to mitigate security breaches by seeking to bring about better security through a positive change in user behaviour. However, as discussed in chapter 2, despite increasing awareness training budgets and rapidly growing rates of implementation of awareness programmes within organisations, security breaches caused by human error continue to rise. This raises numerous questions about the efficacy of awareness training programmes and how such programmes could be made more effective to achieve the desired change in user behaviour. The research question encapsulates this phenomenon.

The literature review revealed several important themes that have been helpful in the formation of interview questions. In forming the interview questions, the research question and the objectives were carefully aligned to ensure that each interview question effectively addresses an objective and the overall research question. I also had to carefully consider how to analyse the participants' responses to the interview questions so that the objectives and the overall research question is appropriately addressed.

Since the data gathering method of this project was semi-structured interviews, it was important to have some kind of interview schedule to assist with the process. This also served as a loose agenda, helping to prepare me for the likely content of each interview. The list of interview questions was not meant to be prescriptive or to be followed in the exact order. I tried to keep questions as open and expansive as possible to facilitate the participants to engage with the topic at some length. The intention was to allow the participant's narrative to be as self-directed as possible. Depending on the topic and the type of participant (InfoSec academic or practitioner), I used filter probing questions when needed. The list of interview questions also served as a virtual map that I could refer to in case things became difficult during the interview. This preparation allowed me as the interviewer to remain engaged and to listen attentively to the participants.

In forming the interview questions, I endeavoured to go beyond my own experiences and preconceptions as an InfoSec professional and a researcher. In trying to remain true to the phenomenological process, my intention was for the interviews to be as open as possible to allow for different kinds of responses, allowing each participant to present their unique narrative. The intention was to understand the phenomenon from the participants' point of view and in their own terms. The interview questions placed emphasis on the participants' account of the benefits, shortcomings, and barriers to implementing InfoSec awareness programmes within their organisations. The participants were encouraged to speak freely about their experiences and were given full assurance of anonymity and confidentiality.

Smith Flowers and Larkin (2009) state that phenomenological interviews typically move between narrative and descriptive accounts to those that are more analytic and evaluative. In order to help ease the participants into the interview process, I started with questions that required participants to provide fairly descriptive accounts of their experiences and gradually moved towards questions requiring more analytical responses. In phrasing the questions, I tried to keep the formulation open, avoiding assumptions about the participants' experiences or leading them towards particular answers. As a practitioner-researcher with similar experiences, I consciously avoided questions that could be perceived as over-empathetic and/or manipulative. The table below provides a list of questions used during the interviews. Since this research involved two categories of participants, the table illustrates which questions were asked to each category. The table also highlights the corresponding objective (s) that each question attempts to address. Objective #3 of the project is addressed in chapter 5, as part of the discussion and interpretation of the findings.

Interview Question	**Respondent (ISA / ISP)**	**Corresponding Objective (s)**
What do you perceive as the biggest challenges to building an InfoSec awareness program for organisations?	ISA, ISP	1, 2
Can you describe your feelings towards building your InfoSec awareness programme? What failures and pitfalls did you face?	ISP	1, 2
What were the major internal / political obstacles you experienced in implementing the InfoSec awareness programme and how did you deal with them?	ISP	1, 2, 4
What are your thoughts on the role of senior management in the success of an InfoSec awareness programme? Did you feel supported? How can you gain their support?	ISA, ISP	1, 2, 4
What would you describe as your main successes in implementing the InfoSec awareness programme?	ISP	2, 4
Why do you think phishing and other social engineering attacks are so widespread and successful?	ISA, ISP	1, 2, 4
From your experience, how do you think InfoSec awareness programmes can be improved to change human behaviour for the better?	ISA, ISP	2, 4
What InfoSec awareness strategies have you found to be most effective to prevent human error and to promote the protection of organisational information systems and data?	ISA, ISP	2, 4

How has the implementation of an InfoSec awareness programme affected the frequency and severity of security breaches in your organisation, especially those related to human errors?	ISP	1, 2, 4
How do you establish what InfoSec concepts are most important in your organisation's InfoSec awareness programme?	ISA, ISP	2, 4
How do you determine that your users have been adequately trained through InfoSec awareness strategies to protect your organisational information systems and data?	ISA, ISP	2, 4
In your opinion, what is the best training frequency and what teaching and learning styles are most effective?	ISA, ISP	1, 2, 4
How do you measure the success of an InfoSec awareness programme?	ISA, ISP	2, 4
What evaluation mechanisms / metrics have you found to be useful for measuring the effectiveness of InfoSec programmes?	ISA, ISP	1, 2, 4
What constitutes an effective InfoSec awareness programme in your opinion?	ISA, ISP	1, 2, 4
What advice would you offer to other professionals wishing to build their own InfoSec awareness programme?	ISA, ISP	2, 4
ISA = InfoSec Academic ISA = InfoSec Practitioner		

Table 5: List of guide interview questions

4.2.3 Expert Panel Evaluation

In order to improve the quality and focus of the interview questions, they were tested on a two-member panel of InfoSec professionals (one InfoSec academic and one InfoSec practitioner).

The panel provided me with some valuable feedback and comments to help make the questions more understandable and focussed to ensure that I would be able to elicit the data that I needed from the research participants. I made use of the reserve research participants from the participant selection phase of the project.

4.2.4 Pilot Test (Dry Run)

Creswell (2013) points out that qualitative research is iterative in nature with to-and-fro between the data collection and analysis stages to bring about revisions and improvements to the approach where necessary. Using pilot interviews is an example of the iterative nature of qualitative research, whereby aspects of the interview (the format, interview questions, sound

/ video quality, etc) can be tested with a small number of participants and evaluated and revised accordingly. I pilot tested the interview questions with two of the reserve participants.

Based on the advice of Creswell (2013), I followed the same procedures for the pilot interviews as those planned for the main project. In other words, the participants were selected using the same eligibility and selection criteria, the interview protocol (PIS) was clarified to the participants and informed consent was received from them before the pilot interviews commenced. Conducting the pilot interviews gave me the opportunity to practice my interviewing techniques, familiarise myself with the online interview format and resolve any technical and research related issues early on. Based on my experience of the pilot interviews, I was able to make the necessary amendments and adjustments before conducting the main interviews.

Alase (2017) points out that there are many elements of unpredictability that could arise during the interview sessions and it is not possible for the researcher to be able to anticipate exactly what to expect in an interview. IPA researchers are advised to be prepared to expect the unknown vis-à-vis actions and/or inactions of the participants. A pilot test could help to bring to light some of these elements.

4.2.5 Conduct Interviews

Once I received a positive response to my initial email invitation letter (Appendix A) and a completed pre-screening questionnaire (Appendix B) from potential candidates, their eligibility to participate in the research was determined. The potential participants that met the eligibility criteria were sent a copy of the Participant Information Sheet (PIS) (Appendix C) and Participant Informed Consent (Appendix D) to sign and return.

In order to ensure that the research is ethically sound, a Participant Information Sheet (PIS) (Appendix C) was prepared to provide potential participants with the necessary information about the research. The PIS assured potential participants that their anonymity would be maintained and all responses would be kept confidential.

Based on Bailey's (1996) recommendations, the following key points were conveyed in the PIS:

- That the participant is taking part in a research study
- The purpose of the research and the procedures involved
- The possible risks and benefits of the research
- The voluntary nature of research participation
- The participant's right to stop the research at any time
- The measures taken to protect participant and organizational confidentiality (including compliance with the UK Data Protection Act, 2018).

The potential candidates that agreed to participate in the research were asked to sign a Participant Informed Consent (Appendix D). Any participant who did not wish to sign the informed consent was not pressured to participate in the study. Only the participants that were in agreement with the PIS contents and signed the consent document were selected to take part in the research. The contents of the PIS were also explained to each participant at the beginning of each interview.

The participants were provided information about the research area for this project, but the central research question was not shared. Bailey (1996) cautions that deception in research may be counter-productive. However, not revealing the central research question to the participants is not regarded as deception, since this could potentially jeopardise the entire study. An example of this could be in the form of response effect where the participants tailor their responses to what they think the researcher is expecting. In general, deliberate deception hinders genuine insights, whereas honesty combined with confidentiality reduces suspicion and promotes sincere responses (Bailey, 1996).

Once the signed Participant Informed Consents was received, confirming the participants' willingness to voluntarily participate in the research, I started the process of establishing contact and building a professional relationship with the participants. In cases where I did not receive the signed consent forms in a timely fashion, email reminders were sent to the participants. The process of interviews did not commence until I had received the signed consent forms from all of the participants. I then proceeded to arrange a suitable date and time for the interview.

All the participants were given the opportunity to ask questions or raise any concerns by email before the interviews commenced. I also offered the participants an opportunity to have a pre-interview chat to discuss any areas of concern to make sure that they understood what was involved and felt comfortable to proceed.

The most important thing for a qualitative interview is for the researcher to build a rapport with the participant; establishing trust with participants is a crucial factor in obtaining participant consent (Smith Flowers and Larkin, 2009). I reminded the participants about the importance of their participation for this research and how their contribution was valued and that the findings would benefit our common professional practice.

I endeavoured to establish and maintain a strong professional relationship with the participants, one founded on trust and transparency. In an effort to build trust with the participants, I followed the recommendations by Moser and Korstjens (2017) who emphasise the need for prolonged pre-interview engagement to ensure the comfort of participants and to convey a sense of true concern for their interests as well as appropriate allocation of time to prepare for interviews, maintaining transparency through every phase of the interview.

Moser and Korstjens (2017) also emphasise the importance of transparency to foster trust between the researcher and the participants. During the interview scheduling stage, I reiterated and clarified the purpose of the research and the interview process by referring back to the PIS. I emphasized the robust mechanisms in place to maintain participants' anonymity and to protect their privacy to ensure that they would feel assured and satisfied to commence the interview.

In-depth interviews informed by the phenomenological approach were conducted with the participants that were focused on their experiences, feelings, beliefs and convictions (Welman & Kruger, 1999) about the theme of InfoSec training and awareness programmes. The central research question was: *What are the main shortcomings in existing InfoSec awareness training programmes and how can these be addressed in order to reduce human errors?*

The participants were in a position to assess the relevant issues from an academic, professional and organisational point of view and were able to offer insights from their personal experiences. The emerging themes were important in framing my thinking and also offered a crucial reference point during data analysis and theory generation stages, acting as a form of triangulation.

I found the pre-interview engagements to be quiet valuable in helping me to build a strong rapport with all the participants. As a result, all the participants and I felt relaxed before and during the interview sessions. I started the interviews with some generic icebreaker questions, such as:

- What aspects of InfoSec interest you the most?
- What kind of InfoSec related tasks do you perform on a typical day?

Although the nature of the interviews was semi-structured, I had a clear idea of the type of questions to ask. Interview questions were focused on the practical concerns and issues that the participants and their organisations had in relation to InfoSec awareness programmes.

I found the 5-step interview guidelines offered by Rivard *et al* (2014) to be particularly useful during the interview stage. The steps consist of:

- ➢ Building rapport with the participants
- ➢ Avoid asking leading questions
- ➢ Avoid interrupting the participants
- ➢ Allow for pauses between and during questions
- ➢ Use follow-up questions to fill any gaps in participant responses

I allowed participants ample time to respond to each question. Follow-up questions were used as necessary to prompt participants to elaborate on their responses. The same protocol was used for all the interviews in order to maintain consistency and uniformity in the data collection process. Based on Rivard *et al's* (2014) recommendations, I asked a variety of questions such as non-leading, probing, follow-up, specifying, direct/indirect and interpreting questions. In addition, I utilised the following probes suggested by Asmussen and Creswell (1995):

- *Could you explain your response more?*
- *Tell me more. Please explain.*
- *I need more detail.*
- *What is an example of that?*

Based on Asmussen and Creswell's (1995) recommendation, I also employed an interview protocol (Appendix E) to clarify the process to each participant prior to the interview. The interview protocol combined with the interview questions helped me to organise my thoughts on the interview process, such as headings, starting and concluding ideas as well as making my own notes related to each interview.

Before I commenced each interview, I made brief notes on my personal feelings and impressions of each participant. Having established a good rapport with each participant as part of pre-interview engagements, I was able to reflect on the mental impressions I had formed about each participant. I felt it was important for me to jot down any presumptions I had formed about the participants, especially from a professional perspective, as I did not wish any preconceived biases to weigh in on the interview process in terms of how I conduct the interviews and deal with the participants.

As an example, I made some notes prior to conducting the interview with participant ISP3. Having studied the pre-screening questionnaire completed by the participant, I could see that he possessed extensive InfoSec related industrial experience as well as a number of highly regarded InfoSec certifications. However, the participant did not possess any formal academic qualifications. This is not something uncommon in the InfoSec industry. Typically, such individuals join the industry in entry level roles, often after completing specific vocational courses to gain the relevant knowledge and skills.

I have personally worked with many InfoSec professionals with similar backgrounds. They tend to be extremely hard working, focussed and experts in their fields, moving up the organisational hierarchy through many years of hard graft. In my experience, professionals in this category often tend to hold negative views about their senior management who are often themselves university graduates with broader management backgrounds. Senior management is often perceived by such individuals as being an imposed structure with no real understanding of the ground realities that InfoSec professionals face. I expected some of these feelings of resentment and frustration to come through in the interview. This also resonates with me as I have personally experienced similar situations in my career. I could almost imagine myself stepping into the participant's world and living through the experience that was being described to me. I felt that that there was a strong feeling of mutual trust, friendship, and affinity amongst us.

Although the interviews focussed on the participants' experiences, I maintained self-awareness of my own personal assumptions in order to minimize personal bias. I consciously sought to bracket off my preconceptions during the interviews to allow participants to express themselves and put forward their claims on their own terms (Smith, Flowers and Larkin, 2009)

All the interviews were conducted via video teleconferencing using Skype and Zoom platforms. I coordinated with each participant to arrange a mutually convenient time and appropriate location in order to ensure privacy and minimise disruptions during the interview.

I was mindful of technical issues such as connection problems, equipment failure, background noise and interruptions during the interviews that could seriously threaten the research (Easton et al, 2000). Before commencing each interview, I confirmed with the participants that they were satisfied with their location and offered them the opportunity to reschedule the interview if they anticipated any disruptions during the interview.

The interview questions were presented with emphasis placed on the participant's account of the benefits, shortcomings and barriers to implementing awareness training programmes within their organizations.

The intent was to understand the issues from the participant's point of view and in their own terms. The participants were encouraged to speak freely about their experiences and future expectations and were given full assurance of anonymity and confidentiality.

Although the participants being interviewed were the main unit of analysis, by treating each participant as a unique case, it was possible to consider group characteristics between the different cases. As such each participant was expected to have distinctive issues as well as common problems. The internal differences and consistencies between the cases were compared to reveal useful insights that could possibly have wider implications and result in new theory (Stake, 1994). This kind of data collection and analysis from participants with different backgrounds also provided a form of triangulation (literature, academics and practitioners) to make the data more reliable (Arksey & Knight, 1999).

The vast majority of interviews lasted between 60 to 90 minutes. Two of the interviews exceeded the 90 minutes threshold by approximately 10 minutes due to the need to ensure that all the topics had been saturated and the participants did not offer any new perspectives on the topic.

After the initial interviews, a further 15-20 minutes of participants' time was requested to review and validate the interview transcripts. This form of participant validation or member checking is an important provision to strengthen the credibility and validity of qualitative research (Shenton, 2004). The interview transcripts were returned to the participants to check for accuracy and to confirm how well their accounts were captured. The main emphasis was on whether the participants considered that the information in the transcripts matched what they intended. Member checking was also utilised in the later stages of data analysis when the themes were formed from the interview data. This is discussed later in this chapter.

The individual interviews with each participant were audio-recorded with their permission and assigned appropriate participant codes for later retrieval and analysis. The data collected from the participants is reported either in an aggregate form or using participant identification codes. Each participant was assigned a unique participant identification code.

At the end of each interview, I listened to the recordings and made my own notes without any judgmental evaluation (Lofland & Lofland, 1999). These notes helped to tease out themes, patterns and categories for later analysis. According to Groenewald (2004), such notes are already a step towards data analysis because they involve some interpretation.

As the researcher, my knowledge, experience, perspective and subjectivity during data collection were all important characteristics in this research. However, it was important for me as a researcher to prevent the data being prematurely categorised according to my own biases.

The process of note taking also helped to highlight issues and themes that required further clarification from the participants.

4.2.6 Post Data Collection Reflection

As I concluded each interview, I once again made brief notes on the interview process. I compared my notes with the pre-interview notes and reflected on the experience and the new insights I had gained. As an example, I returned to my pre-interview notes for participant ISP3 and upon reflection I realised how warm and accommodating the participant was during the interview.

I found it intriguing that some of my preconceptions and impressions about the participant were echoed during the interview. In particular, the idea of senior managers and executives being out of touch with the day-to-day operational challenges faced by InfoSec professionals surfaced during our discussion. The participant also expressed his frustration at not being able to secure senior roles in the field despite his extensive practical experience. He found himself hitting the 'glass ceiling' due to a lack of academic qualifications and seemed to regret not availing opportunities earlier in his career. Some other important themes that transpired during our discussion included his frustrations about user apathy towards InfoSec issues, lack of support from senior management and the stressful nature of the job itself.

I was very satisfied with the interview as it exceeded my original expectations. I was able to obtain deep and insightful accounts of the participant's experiences. He was very candid about his feelings and experiences and generally did not require much prompting. I was happy for the participant to take the lead as I focussed on attentively listening to the account of his lived experiences.

I found the pre- and post-interview note taking and subsequent reflections on the interview process very valuable. I was able to draw on these insights during the transcription and later analysis of the interview data through interconnection and integration of ideas and themes to generate theory.

I thoroughly enjoyed the process of conducting the interviews. It was a very stimulating and fulfilling experience that brought back a lot of familiar memories for me. I felt like I was able to connect with the participants on an emotional as well as a professional level. In a sense, I felt inspired and privileged to have an opportunity to hold an open and honest dialogue with other InfoSec professionals on an issue that is of enormous concern for our community of practice and the larger industry.

I felt a deep sense of awe and respect for the participants and the hugely important roles they play. I was grateful that they gave me the opportunity to peek into their world. As I listened to the audios and transcribed the interviews, I was amazed at how perceptive I had become towards how language is used to express different emotions and feelings. This was also a journey of discovery for me in which having studied the theoretical aspect of phenomenology, I was able to put the theory into practice. The process helped me to develop the crucial skills of conscientious listening, contemplation, and reflection.

During the process of transcription, I was able to highlight at least two instances in the interview with participant ISP3 where I attempted to empathise and almost unwittingly diverted the course of the discussion. Reflecting on this experience made me realise how important it is to remain steadfast upon the principles of phenomenological research and how seemingly minor and unintentional lapses could threaten the rigour and validity of the research.

Smith, Flowers and Larkin (2009) point out that the IPA approach to data collection brings with it a commitment to a degree of open-mindedness and interview (data collection) stage is the only time when the researcher must keep their preconceptions out of the process. I feel that this phenomenological attitude was pivotal in allowing me access to the lived experiences of the participants without imposing my personal research agenda. I found the phenomenological approach to data collection (interviews) very exhaustive and thoroughly intriguing and rewarding.

4.2.7 Data Management and Security

The management and security of data in qualitative research studies is an issue of great importance. As the main researcher, it is ultimately my responsibility to provide adequate safekeeping for the data collected from research participants. Rubin and Rubin (2012) point out that ‘a safe and sturdy storage system’ should be used for the management and safekeeping of IPA research data. They advise that a sturdy safety system should be used to protect the collected data from outsiders through a password protected filing and storage system.

Data management and security must be incorporated throughout the research study in order to promote effective archiving and protection of research participants’ information. The loss, theft or inappropriate use of confidential research data could seriously undermine the integrity of the researcher and the research study (Alase, 2017). As an added layer of security and safeguarding of participant data, Alase (2017) recommends deletion of all audio-taped information after it has been transcribed and validated by the participants.

I utilized several data management techniques to create, codify, organise, and securely store the data gathered throughout this research. Microsoft Word was used to create the initial participant invitation letter, pre-screening questionnaire, participant information sheet, informed consent form and the interview protocol documents. The recorded interviews were also transcribed using Microsoft Word and Adobe Acrobat. All the documents were saved as password protected electronic files. Microsoft Excel was used for the analysis and coding of data and the files were similarly password protected. My handwritten notes were scanned into PDF files. All the electronic files were organised using a multi-folder system, with separate folders for each participant, named using participant ID codes so the data inside the folder could not be traced back to a particular participant. Each individual folder was then encrypted on the hard drive. A backup copy of the data was kept on an encrypted USB storage device.

4.3 Data Analysis Stage

This stage of qualitative research is generally referred to as data analysis. According to Lester (1999) and Groenewald (2004), the term “explication” encapsulates the process of phenomenological analysis more succinctly. They refer to the interpretation offered by Hycner

(1999) who argued that the term “analysis” implies a breaking into parts to identify essential features and relationships, whereas explication involves investigation of the constituents of a phenomenon, whilst preserving the context of the whole. Phenomenological enquiry aims to unveil the inherent structures, essences and meanings that characterise the investigated phenomenon from the perspective of the participants. As such, keeping the whole intact is crucial to the goals of phenomenology. For the purpose of convenience both terms (analysis and explication) will be used interchangeably in this project.

As previously discussed, Interpretative Phenomenological Analysis (IPA) was the research methodology employed for this project. Creswell (2013) points out that phenomenology is not merely a descriptive process but also an interpretive process that allows a researcher to interpret the meaning of the lived experiences of the participants. He goes on to assert that phenomenologists focus on describing what all participants have in common as they experience a phenomenon (Creswell, 2013). As a qualitative research approach, IPA allows researchers to interpret and make sense of the lived experiences of participants that have experienced a common phenomenon. It allows different participants that have experienced similar events to tell their stories without distortions.

According to Smith, Flowers and Larkin (2009: 79) literature on data analysis using IPA does not prescribe a particular method, allowing the researcher considerable flexibility to choose from the repertoire of available strategies. Indeed, Smith, Flowers and Larkin (2009) encourage IPA researchers to be creative when devising an approach to data analysis. Following this advice, I opted for an eclectic approach to data analysis, combining between aspects of Hycner’s (1999) explication process and Moustakas’s (1994) framework. This combined approach provides a guide for expressing the analytical journey, via a series of stages, through to final theory development. In doing so, the interview data was considered within the context of its gathering and the participants, against known understandings.

Using the data (interview transcripts) collected from the participants, my intention was to untangle descriptions and statements, search for meanings and transform these into general themes that would inform a more effective approach to InfoSec awareness training programmes. Unlike quantitative research, a phenomenological investigation does not necessarily lead to definitive conclusions. The involvement of participants’ and researcher’s own subjective views and biases means that the research process is likely to be very fluid.

The diagram below illustrates the data analysis process. The data analysis process is summarised in the following stages:

1. Bracketing and phenomenological reduction through epoché
2. Delineating units of meaning
3. Clustering of units of meaning to form themes
4. Extracting general and unique themes from all interviews

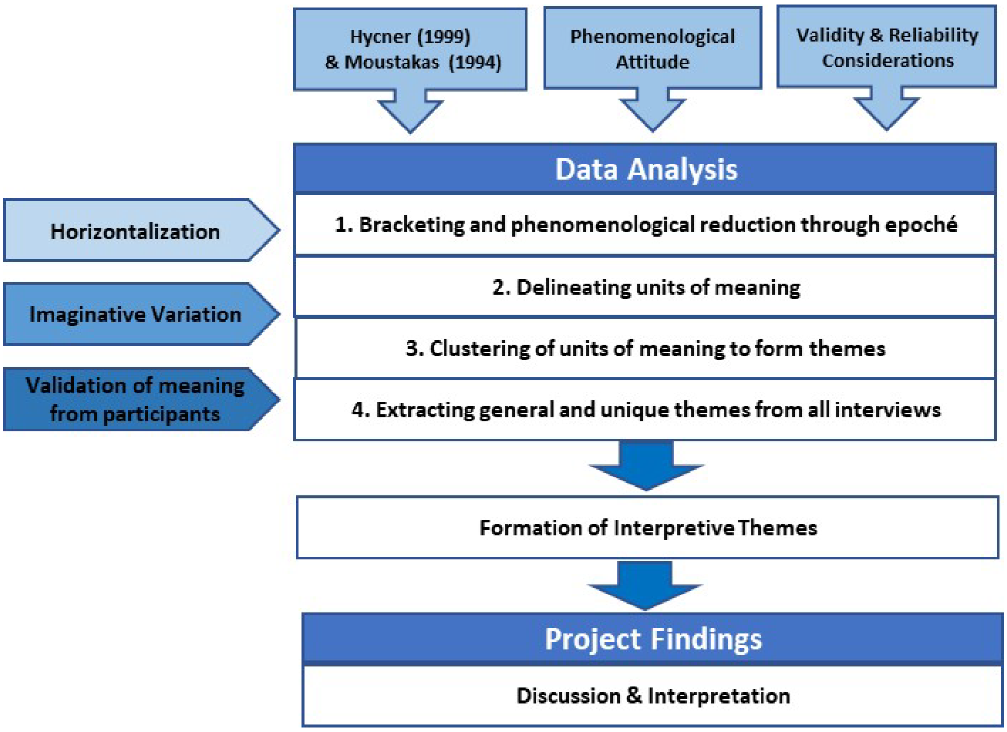

Hycner (1999)
& Moustakas (1994)
Phenomenological Attitude
Validity & Reliability Considerations
Data Analysis
Horizontalization
Imaginative Variation
Validation of meaning from participants
1. Bracketing and phenomenological reduction through epoché
2. Delineating units of meaning
3. Clustering of units of meaning to form themes
4. Extracting general and unique themes from all interviews
Formation of Interpretive Themes
Project Findings
Discussion & Interpretation

Figure 11: The data analysis process

1. Bracketing and phenomenological reduction through epoché

As discussed during the pre-data collection reflection stage, the process started with epoché (Moustakas, 1994) whereby I as the researcher put aside or 'bracketed out' any assumptions and beliefs about the phenomenon being investigated. This involved my reflections, recognising that my personal views and preconceptions can enter and influence the unique world of the participants and ultimately the research findings (Creswell, 1998).

Due to my status as an insider with prior experience in the same field of practice, I returned to this stage repeatedly during the data analysis to ensure that my experiences and preconceptions were not influencing the results. As Moustakas (1994) points out, epoché is not just a one-time process but rather a state of mind to ensure that the researcher remains open to new ideas and meanings. This was particularly pertinent for me as insider researcher, someone who is firmly established and experienced in the field of InfoSec and therefore has a vested interest. This approach to data analysis allowed me to remove myself from the data and instead focus on what was being conveyed through the data. In the later stages of analysis, as themes began to emerge, I found it essential to return to epoché to ensure that any new biases had not prevented me from recognising new insights into the phenomenon.

I commenced reading the interview transcripts, having assumed a phenomenological attitude, as described in the previous section. I set about reading the thick experiential descriptions of the participants from the transcripts to gain an intuitive and holistic understanding of the phenomenon. My aim was to get a feel for what was being said by the participants (Lester, 1999).

As part of the phenomenological reduction process, another concept that is related to epoché is horizontalization of the data, requiring the researcher to give equal value to all the participants` statements (Moustakas, 1994). This technique helped me to read through the transcripts with an open mind, without attaching significance to particular dimensions of the participants' experiences so as not to rush to any premature interpretations. I also consulted my pre and post interview reflective notes to help me piece together the meanings from each transcript and make sense of the overall phenomenon.

2. Delineating units of meaning

In this phase, I initiated the process of coding and grouping of core meanings revealed from the participants' experiences by extracting the statements that were seen to illuminate the investigated phenomenon (InfoSec awareness programmes). Coding helps concepts and categories to be identified by segmenting data (interview transcripts) into smaller units, allowing their conceptual properties to be described through labels. Coding helps to link a concept to the data and generate categories of different concepts. It is therefore an essential technique for a researcher to systematically organise and understand the data (Creswell, 1998; Hycner, 1999).

I re-read each interview transcript for clarity. The intention was to extract the meaning in the form of a situated description that captured the participant's experience. Vagle (2014) recommends multiple, line-by-line readings of all transcripts, each with a different set of goals. Using a hard copy of the transcripts, after the first reading, I made detailed notes and comments in the margins along with highlights for meanings that appeared to be clear.

Following Vagle's (2014) advice, I conducted three detailed line-by-line readings of the transcripts, to facilitate careful examination and triangulation of themes. With each subsequent reading taking a more critical view, I asked questions and made notes. The multiple readings helped me to understand what the participants were trying to convey and get a sense of the participants' state of mind with regards to how the phenomenon had affected their lived experiences.

I read through the transcripts to identify common themes by way of frequently repeated words or phrases. I sought out words, phrases, concepts, sentences, and emotions that directly related to the phenomenon under study. This was in essence the 'meaning unit'; words or statements pertaining to the 'core essence' of the participants' lived experiences conveyed in their responses (Alase, 2017). Based on Alase's (2017) recommendations, I completed the data coding process through three generic cycles.

During the first cycle, the lengthy and sometimes complicated participants' responses were gradually coded into chunky meaningful sentences. This helped me to dissect the responses into a manageable format (blocks of sentences). This also helped me to be mentally aware of frequently repeated key words and phrases as quite often such words and phrases can capture the core essence of the participants' lived experiences as it relates to the phenomenon. Using the concept of horizontalization, I gave all participant statements an equal weight, reserving my judgements, and not categorising or counting anything as duplicate.

During the second cycle, the chunky meaningful sentences from the first cycle were further condensed into fewer words as I sought to capture the core essence of what the participants were expressing and what the research topic meant to their lived experiences. Alase (2017) points out that although the first and second coding cycles condense the participants' responses to smaller manageable formats, the essence of the participants' thoughts and lived experiences is still accurately represented in the condensed coding.

The third cycle is the stage where I narrowed down the participants' responses to extremely few words. Alase (2017) refers to this as the category stage. At this stage I tried to encapsulate in a few words, the core essence (meaning unit) of the participants' lived experiences. My intention was to use words and phrases that illuminated the multifaceted phenomenon whilst privileging the participants' narratives.

In the beginning of the process, I tried to identify as many category codes as possible. I used the following criteria for coding (adapted from Lin, 2013):

- Wherever possible, I used a key term/word/phrase from within the transcript as a descriptive code
- Used an existing descriptive code only if it was a good fit
- If an existing descriptive code failed to capture the perceived meaning, created a new descriptive code using a key term/word/phrase from within the transcript
- If in doubt about the suitability of a code, created a new descriptive code

During the final coding cycle, any statements not related to research topic were eliminated. I also consolidated and eliminated redundant codes by readjusting the coding criteria as follows:

- A consolidated descriptive code was used if it was a good fit
- If an existing consolidated code failed to capture the perceived meaning, a new code was created
- If in doubt, the consolidated descriptive code was preferred

Using the generic coding described above, I was able to deconstruct the interview transcripts systematically and meticulously without 'diminishing or misrepresenting' the core meaning of participants' lived experiences (Alase, 2017).

Imaginative variation played an important role during the coding process by helping to reveal hidden frames of reference. Imaginative variation is a technique that takes the different participants' perspectives and unifies them into structural themes that represent the essence of the experience (Moustakas (1994). A given extract from a participant's response to a question could be interpreted from different angles. Imaginative variation helped me to interpret the units of meaning from different angles by varying the frames of reference. This ensured that different perspectives and interpretations were considered.

This stage required substantial judgement calls while consciously bracketing out my own presuppositions. The list of units of relevant meaning extracted from each interview was carefully scrutinised and redundant units were eliminated (Moustakas, 1994). At the end of this stage, 82 units of meaning were formed, comprising of 49 meaning units identifying shortcomings and another 54 meaning units identifying possible solutions relating to the research question of this project. There was an overlap between the meaning units as some of the meaning units were found to be relevant as both shortcomings and possible solutions and recommendations. An aggregate list of all units of meaning can be found in Appendix G, along with the corresponding project objective(s).

3. Clustering of units of meaning to form themes

Once a list of non-redundant units of meaning was available, I rigorously examined the list to try to elicit the essence of meaning of units within the holistic context (Hycner, 1999). Once again, this required judgement and skill on my part as I needed to bracket off my own presuppositions in order to remain true to the phenomenon. At this point, the focus was gradual filtering of the meaning units into themes. By grouping units of meaning together, clusters of themes were formed (Creswell, 1998; Moustakas, 1994) and I started to identify significant topics.

At this stage a summary incorporating all the themes elicited from the data was prepared to provide a holistic context. Hycner (1999) emphasises the importance of going back to the interviews (transcripts) and the list of non-redundant units of meaning to derive clusters of appropriate themes. This also required validity checks (Smith, Flowers and Larkin, 2009; Spinelli, 2005 & Groenewald, 2004) so I returned to the participants to determine if the essence of the interviews had been correctly captured (Hycner, 1999), to see if anything had been overlooked or missed and make necessary modifications accordingly.

4. Extracting general and unique themes from all interviews

Once the stages above had been carried out for each interview, the themes common to most or all of the interviews as well any individual variations (Hycner, 1999) were searched for. It was important to carry this out carefully so as not to suppress any minority voices which could act as important counterpoints. The aim here was to evolve with statements (themes) that reflect the authentic underlying meaning of the participants' thoughts and descriptions of their lived experiences of the phenomenon.

Colaizzi (1978: 59) describes this stage as a 'precarious leap' in which the researcher moves beyond the interview transcripts to arrive at meanings that 'should never sever connections' with the original interview transcripts. The researcher's formulations must illuminate the 'meanings hidden in the various contexts and horizons' within the various transcripts.

This stage culminated in the participant's everyday expressions being transformed into appropriate scientific discourse that supported the research (Sadala & Adorno, 2001). The final process of analysis produced seven interpretive themes of InfoSec professionals' lived experiences of InfoSec awareness training programmes.

As discussed previously, member checking is an important strategy to bolster the credibility and validity of qualitative research. Shenton (2004) recommends that member checking should also involve verification of the researcher's emerging themes, theories, and inferences by asking the participants to offer reasons for any particular patterns observed by the researcher. Member checking was used at this later stage of the project by referring the seven interpretive themes back to the participants for validation of the phenomenon.

A summary of the seven interpretive themes is provided below. A table of all the interpretive themes along with the associated meaning units is provided in Appendix H.

Theme 1	Understanding common user actions contributing to human errors
Theme 2	Identifying the most common attack vectors
Theme 3	Personal and social factors contributing to human errors
Theme 4	Factors that lead to InfoSec awareness programme failure
Theme 5	InfoSec strategies to prevent human errors
Theme 6	Understanding the psychological perspective of human behaviour in InfoSec
Theme 7	Essential components of an effective InfoSec awareness training programme

Table 6: List of interpretive themes

As previously discussed, IPA is an interpretive process that allows a researcher to interpret the meaning of the lived experiences of the participants (Creswell, 2013). At this stage of the project, it was important for me to consider how to gather together all the various elements that emerged from the research findings to form a multifaceted, collective experience of the phenomenon that can be demonstrated through linkages, patterns, and relationships. This entails construction of meaning through explanations, extrapolations and inferences from other sources in an effort to draw conclusions that go beyond a mere descriptive analysis of the interpretative themes.

The next chapter presents the findings according to the main interpretive themes above whereby I seek to draw out key issues discussed by the participants and interpretations and linkages are made by relating the findings to previous research, other views on the subject and to my personal experiences to develop tentative theories. The ideas discussed in the previous sections are further developed and a set of practical guidelines will emerge that organisations can potentially incorporate into their InfoSec awareness training programmes to reduce the risk of security breaches resulting from human errors. There is also likely to be some informed speculation with a clear reference to the findings and clarification of any assumptions being made. Qualitative research generally does not claim to offer definitive answers, and therefore the arguments and theories developed are likely to be of a suppositional structure.

Since phenomenological studies can only make detailed comments about individual situations, it would normally not be possible to claim that the theories developed in this project could be generalised to wider contexts (Shenton, 2004). However, by making the process of theory generation as transparent as possible, I believe that I can claim application of the theory to situations beyond the particular cases in this research study. Ultimately, the reader will be able to work through from the findings to the theories to see how the interpretations were derived and decide on the validity of the findings.

4.3.1 Post Data Analysis Reflection

IPA is primarily concerned with the examination of participants' lived experience in a way that facilitates the experience to be expressed in its own terms rather than according to some predefined criteria. It requires empathy on the part of the researcher and a 'willingness to enter into and respond to the participants' world' (Smith, Flowers and Larkin, 2009: 55).

As a practitioner-researcher with a predominantly technical (positivist) background, this was my first exposure to this kind of research paradigm. It took some time for me to comprehend and internalise the theoretical and philosophical tenets of the phenomenological approach. I found the data collection process to be remarkably intriguing, insightful and rewarding.

However, having gathered the data through interviews, I felt quite overwhelmed with the amount of data produced as I searched for a sense of order. I often found myself bogged down, confused and frustrated in the process of analysing the interview transcripts.

Smith, Flowers and Larkin (2009: 55) point out that qualitative research requires a researcher to engage with complexity. Contrary to my previous understanding of 'complexity' as a scientific term requiring a methodical and systematic approach to problem solving, I discovered that in qualitative research the term denotes unpredictability, chaos and mess. I occasionally felt out of my depth and not in control of the process.

The data coding process was laborious, time-consuming and 'imaginatively and emotionally demanding' (Alase, 2017). It was important to present the participants' lived experiences in a holistic way, preserving the interrelation and congruence between the various facets of the phenomenon. As a result of this requirement, during coding, I found it extremely difficult to restrict the descriptions and units of meaning to one theme.

I persevered and endeavoured to remain patient, flexible and open-minded throughout the process. I was fortunate to have the guidance and support of my academic advisors, professional colleagues and critical friends throughout the process.

Smith, Flowers and Larkin (2009: 79) highlight that the literature on data analysis using IPA does not prescribe a particular method. As such, there is no 'right or wrong way' of data analysis and the researcher has considerable flexibility in choosing from the repertoire of available strategies. Indeed, Smith, Flowers and Larkin (2009) encourage IPA researchers to be creative when devising an approach to data analysis.

As this was my first encounter with phenomenological research, I felt that it was necessary for me to have some generic guidelines that I could follow during data analysis. In this regard, I found Hycner's (1999) explication process and Moustakas's (1994) framework particularly useful. I found the concepts of horizontalizing and imaginative variations particularly intuitive and easy to follow. As I applied this framework and the various units of meaning and significant themes began to emerge, I was really pleased and developed a renewed sense of curiosity and determination to persist and go the distance.

During the interviews I endeavoured to ensure that my position as an experienced practitioner had minimal impact on the process. However, during the data analysis stage, I was able to draw on my experiences as an insider-researcher. I am familiar with the participants' professional practice field, having personally engaged with it for many years. This provided me with important contextual insights for judging and evaluating the participants' responses and teasing out the meanings from their individual experiences.

Even though I understood and appreciated the importance of InfoSec awareness programmes and human errors and clarified my agenda during the self-reflection stage, the phenomenological process still unveiled the unexpected. I was quite astonished and thoroughly satisfied with the way that the seven rich and deep interpretive themes unravelled and transpired from the data.

Summary

In this chapter, the theoretical and philosophical principles of phenomenology were applied to describe the process of data collection (interviews) and data analysis. The various stages of the process including the selection of research participants, the formation of interview questions, their evaluation by an expert panel, pilot test interviews and the actual interviews were described. A reflective account of the data collection and data analysis process was also provided.

The exhaustive and rigorous process of data analysis resulted in the formulation of seven interpretative themes encapsulating the lived experiences of InfoSec professionals in relation to the effectiveness of InfoSec awareness programmes.

The following chapter presents the findings of this research along with a discussion and interpretation of the findings.

Chapter 5: Project Findings

Overview

This chapter attempts to make sense of the data gathered in the previous chapter and presents the findings through a discussion and interpretation of the results. The results presented here focus on the phenomenon surrounding the effectiveness of InfoSec awareness programmes and how such programmes can be improved to reduce human errors in InfoSec. This chapter discusses the responses of the research participants (InfoSec academics and practitioners) in terms of the shortcomings in existing InfoSec awareness programmes and recommendations and possible solutions to make InfoSec awareness programmes more effective vis-à-vis human errors.

I will attempt to corroborate and reconcile the findings in light of the literature review in chapter 2 and additional relevant literature as well as my own professional knowledge, experience, and particular ontological and epistemological stance, as outlined in chapter 3. The process of interpretation of the results will lead to the emergence of new knowledge that will be presented in a meaningful way. More specifically, the discussion and interpretation of the findings will lead to the formation of a set of guidelines that will help to improve the processes and practices used to develop and implement future InfoSec awareness programmes. The latter, as the principal outcome of this project, will contribute to my community of practice as well as benefiting my own professional practice.

As detailed in the previous chapter, during data analysis, the open coding process resulted in a large number (82) of codes or units of meaning (Appendix G), comprising of 49 meaning units identifying shortcomings and another 54 meaning units identifying possible solutions and recommendations relating to the effectiveness of InfoSec awareness programmes. There was an overlap between the meaning units as some of the meaning units were found to be relevant as both shortcomings and possible solutions and recommendations. These units of meaning essentially encapsulate and reflect the original and underlying meanings of the participants' account of the phenomenon and related issues.

Through a process of interrogation and reflection (as detailed in previous chapter), the interpreted meanings of the participants' experiences yielded numerous rich and insightful themes. As a result, the units of meaning were consolidated into seven distinct interpretive themes (Appendix H). These interpretative themes also point to the shortcomings and possible solutions that address the main research question and the objectives of this project.

In this chapter, I bring together the many different strands that emerged from the research findings into a multifaceted and consolidated experience of the phenomena. I attempt to demonstrate this integrated perspective through patterns and relationships that go beyond mere descriptions of the interpretative themes.

Literature in phenomenological research emphasises the importance of looking further into descriptions, concepts and emergent themes and adopting a discursive approach during the write-up (Smith, Flowers and Larkin, 2009). Bazeley (2007) urges qualitative researchers to go beyond describing the themes and to seek out the multifaceted dimensions to understand the ‘bigger phenomenon’. Coffey and Atkinson (1996) point out that the analytical process in qualitative research should create and open pathways through the data.

As I critically explore and work through the emergent themes by piecing together the meanings of participants’ experiences, a bigger picture of the phenomenon will begin to emerge. As I present a narrative account of the participants’ experiences and discuss and interpret the findings, I will draw on the literature review in chapter 2, additional relevant literature as well as my own professional knowledge and experience.

In this chapter, all verbatim quotes from the participants are presented in italics. As much as possible, I have tried to present the participants’ descriptions verbatim, without deconstructing them. I feel that it is important to give the participants an opportunity to express themselves and to obtain an authentic representation of their experiences of the phenomenon. Each time, a new theme or aspect of the data is introduced, I will present ‘evidence’ for it from the participants’ transcripts. The presentation of verbatim accounts is also important to make my evidentiary base clear. This gives the reader the opportunity to substantiate the claims and a choice to agree or disagree with the claims.

Smith, Flowers and Larkin (2009: 110) point out that IPA is composed of both the ‘I’ and the ‘P’; a joint product of the researcher and the researched. It is an attempt to capture something of the lived experiences of the participants (the P) and this inevitably requires interpretation (the I) on my part. From an IPA perspective, the verbatim extracts from the participants represent the ‘P’ whilst my analytical comments form the ‘I’. Smith, Flowers and Larkin (2009: 110) portray this as a ‘dialogue between the participant and the researcher’ that is manifested in the ‘interweaving’ of analytic commentary and the participants’ interview extracts.

According to Smith, Flowers and Larkin (2009: 113), IPA studies usually separate the results section from the discussion and interpretation section. In this format, the results section simply presents an account of the participants’ experiences without reference to the extant literature.

In this project, I have chosen not to have a demarcation between the two sections. The results and the discussion and interpretation have been consolidated into this one chapter. A detailed discussion of this choice of format has already preceded in chapter 2. I will be presenting the findings of this project (in the form of the seven themes) together with a discussion and interpretation in order to place the work in a wider context. This will involve engaging in a dialogue between the findings and existing literature (chapter 2). As previously discussed in chapter 2, I will selectively introduce new literature in order to ‘illuminate’ and ‘problematize’ what other research studies say. In this way, the results can either be corroborated or refuted through existing literature. It is also likely that the discussion and interpretation of the results leads into unanticipated territory, not anticipated by the interview schedule. The latter will also require relevant literature that can help to frame such unexpected perspectives in a wider context.

The extensive list of units of meaning derived from the interviews with InfoSec academics and professionals was consolidated into seven interpretative themes. The units of meaning revealed a diverse range of InfoSec topics that I was able to amalgamate into relevant themes based on my own experience and judgement. I also sought validation of these themes from the participants as a form of member checking. The seven interpretive themes are as follows:

- **Theme 1: Understanding common user actions contributing to human errors**
- **Theme 2: Identifying the most common attack vectors**
- **Theme 3: Personal and social factors contributing to human errors**
- **Theme 4: Factors that lead to InfoSec awareness programme failure**
- **Theme 5: InfoSec strategies to prevent human errors**
- **Theme 6: Understanding the psychological perspective of human behaviour in InfoSec**
- **Theme 7: Essential components of an effective InfoSec awareness training programme**

I have organised the themes according to a format that I feel will help me to discuss and interpret the findings in a logical and structured manner. The development of the interpretive themes is closely linked to the project objectives. The main objectives of this project are as follows:

5. *Establish the main shortcomings in existing InfoSec awareness training programmes (vis-à-vis human errors) on the basis of a literature survey and engagement with InfoSec academics and practitioners*
6. *Determine possible solutions to help make InfoSec awareness training programmes more effective (vis-à-vis human errors) based on engagement with InfoSec academics and practitioners*
7. *Assess the validity and reliability of the proposed solutions (that emerge from objective #2) by corroboration with existing literature and own experience*
8. *Derive practical guidelines that can be incorporated into future InfoSec awareness training programmes to reduce human error*

I will discuss each theme in terms of the corresponding project objective(s) that the theme addresses. There isn't necessarily a strict one-to-one relationship between a theme and a project objective. For example, it is possible for a theme to illuminate shortcomings in InfoSec awareness programmes and at the same time point to possible solutions to address the shortcomings; thereby addressing two different objectives. The same holds true for the relationship between the interview questions (Appendix F) and the project objectives; a particular interview question could have elicited participant responses that correspond to multiple project objectives. Objective #3 is addressed during the course of the discussion and interpretation of the results in this chapter which will involve triangulating the findings with the literature review in chapter 2, my own experience as an InfoSec professional as well as additional literature introduced in this chapter.

Theme 1: Understanding common user actions contributing to human errors

The first theme derived from the participant interviews corresponds to objectives 1, 2 and 4. In order to address these objectives, it was important to gain an understanding of the kind of user actions that the participants felt most contributed to human errors. An understanding of these user behaviours is important for InfoSec professionals as it informs effective user training within a comprehensive InfoSec awareness programme.

The use of weak passwords by users was unanimously cited by almost all of the participants as a major contributing factor to human errors. A weak password is one of the easiest ways that cybercriminals can gain access to sensitive data, and this remains one of the most common causes of security breaches.

'….password security is one of those issues that seems to pop up again and again…..we've tried numerous mechanisms to enforce strict passwords but you still find one or two that slip through the net….it's an ongoing struggle to get everyone on board.' [ISP2]

According to the UK National Cyber Security Centre (NCSC) cyber survey (NCSC, 2019), some 23.2 million victim accounts worldwide used 123456 as password whilst less than half do not always use a strong password for their main email account.

'…weak passwords are probably one of the easiest ways for hackers to gain access to sensitive data. You are literally giving it to them on a plate….it is easy to crack simple passwords using brute force attacks or by simply guessing…..nowadays so much personal information can be gathered from internet profiles and social media accounts. This is another problem in itself, most people don't really understand what or how much personal information they can share online…….at the end of the day it comes down to user awareness.' [ISP3]

Research by NCSC confirms the concerns expressed by the InfoSec professionals. NCSC's research (NCSC, 2019) analysed 100,000 of the most commonly re-occurring passwords that have been cracked in global cyber breaches. They highlighted that many users were still choosing to protect sensitive data with easily guessable passwords, like first name, local football team or a popular band. According to Verizon's 2021 security breaches report (Verizon, 2021), 61% of security breaches occurred as a result of stolen or compromised user credentials.

In my experience, there are also concerns surrounding how users store passwords. Sometimes users manage to create really complex passwords but because they have difficulty remembering such passwords, they end up leaving them displayed on sticky notes on their desks, which really defeats the purpose of the exercise. The other issue is the use of the same password across multiple platforms which means that once the password is compromised, their access to all the platforms is compromised.

The recommendation from ISP3 is to '*have a robust and reliable password policy'* to tackle some of these challenges. I agree but would caution that although it is seemingly easy to put in place password policies, maintaining such policies is challenging and even very large enterprises are susceptible to making mistakes.

Another major contributing factor to human errors was identified as the careless handling of data by users. Some of the examples cited by participants include '*removing and misplacing files* (data) *without understanding their importance'* and *'making changes to important documents carelessly'* and even *'deleting sensitive and critical data'*. [ISP1, ISP3]

Some of the user actions that I have personally experienced and that would probably qualify for this category include users failing to backup critical data and sending sensitive data to wrong recipients through unsecured email systems (e.g., using personal accounts).

According to ISA2, to some extent, these user actions are expected when '*employees work with large and complex data involving repetitive tasks*'. The likelihood of such actions increases due to '*work pressures'* and the need to meet deadlines. I would add that there are also many distractions that users have to contend with, social media being a major culprit in modern times.

Some of the participants identified the use of unauthorized or outdated software by users as a factor that could contribute to human errors. Software companies often release regular updates and security patches to address the latest vulnerabilities in their products which could otherwise be exploited by hackers. Employees could unwittingly help cybercriminals to gain access to sensitive data. ISP1 expressed his frustrations about the issue:

'This was an issue we faced in the past because IT hadn't figured out a way to apply policies uniformly across all departments. We had a situation where some users, senior staff, dare I say,....they had greater access privileges than the normal guys……they often turned off the security features and updates on their machines....they found them irritating!....in the end IT had to put their foot down and make things clear….especially to the senior guys.'

I have also come across situations in my career where users turn off antivirus software functions just so they can download movies on their work machines. Turning off software updates can also have serious consequences for the entire company network as shown in the case of the WannaCry ransomware outbreak (Fruhlinger, 2018) that targeted unpatched computers running older versions of Microsoft Windows.

ISA1 referred to the practice of unauthorized software downloads by users as a major concern for organisations:

'Unvetted software is a serious threat....this kind of software can in itself be malicious. Cybercriminals often create such software and once the user installs it, they can exploit the vulnerabilities…. the back doors…. to access systems.'

Users present a variety of justifications for this kind of behaviour. As highlighted by participant ISP1, they find the security features and the update alerts inconvenient, '*irritating*' and '*time consuming*', often popping up when users are engaged in important tasks. Such updates often require a system reboot, so users typically keep putting them off. In my experience, users tend to give preference to older/outdated versions of software because they are used to the features and cannot be bothered to spend time learning the features in newer licensed version of the software. This also raises questions about providing users with appropriate training when newer versions of a software are introduced.

In all of the preceding discussions about the factors contributing to human errors, two aspects of human behaviour featured prominently, namely user carelessness and lack of awareness. It is quite evident that all the user actions discussed so far have their roots in user carelessness and lack of security awareness. User carelessness can be a major factor in and of itself and can also be the consequence of a lack of awareness.

The responses from the participants underscore the fact that users could potentially pose serious security threats to an organisation due to their negligence, carelessness, forgetfulness and laziness. However, when all these traits are combined in users who are also uneducated and untrained about the importance of security procedures and the associated implications, this is a recipe for disaster. Such employees could easily fall prey to phishing attacks or malicious applications that cybercriminal could exploit to gain access to sensitive data.

As a result of their lack of awareness, users could unwittingly assist cybercriminals in a variety of ways (Ekran System, 2019):

Suspicious email links and attachments – Clicking on such links could redirect users to fake and malicious website and downloads.

Unauthorized system changes – Users often make modifications to their devices to make things easier and speed up their tasks. Such unauthorized changes could cause serious disruption to normal business processes and even bring down entire networks.

Using public Wi-Fi – Nowadays Wi-Fi access is freely available in a variety of public locations such as airports, hotels and restaurants. However, most people do not understand that public Wi-Fi is inherently insecure and can easily be used by hackers to intercept communications and launch malicious attacks. A VPN can be used to make the connection secure using encryption.

Insecure devices – Employees often plug their personal devices such as USB drives, phones and tablets into work computers. These devices could contain malicious software that could infect the entire company's network.

Theme 2: Identifying the most common attack vectors

The second theme derived from the participant interviews corresponds to objectives 1 and 4 and encompasses what the participants thought were the most important attack vectors in current day InfoSec environments. An understanding of these attack vectors is important and forms an essential part of effective user training within a comprehensive InfoSec awareness programme.

The participants highlighted that social engineering attacks were popular with cybercriminals, and they had witnessed a rise in this type of attacks.

'I would say that is now the weapon of choice for the more sophisticated cybercriminals….in hindsight, early internet-based scams were pretty crude………We've come a long way since

the early days of internet scams……these guys have learnt to evolve and become ever more sophisticated.' [ISA4]

Although internet-based attacks (email, social media, etc) are the norm these days, social engineering attacks can also be employed face-to-face and over the telephone. It is essential that users understand these different forms of attacks and how to deal with then. Participants also reported a surge in phishing attacks:

'There's been a massive rise in phishing attacks……some of these people are damn good….I mean as a security professional, I can see right through them……for an average unsuspecting user though, it's not so easy.' [ISP2]

Phishing is essentially a type of social engineering attack. In my experience, it is probably one of the most prevalent threats faced by organisations today. It is a technique that is popular amongst cybercriminals as it can easily be customised to exploit current events such as the Covid-19 pandemic to play on users' fears and anxieties.

…..fortunately our spam filters pick up a lot of this stuff. That's not to say that everything gets picked up….there's always a few here and there that slip through……it all seems to be highly targeted these days…..a lot of thought has gone into it.' [ISP4]

As highlighted by the participant above, these types of attacks are becoming increasingly sophisticated and can even circumvent state of the art filters in some cases. The participant's reference to attacks being '*highly targeted*' calls attention to 'spear-phishing' attacks that target specific users and businesses, often through emails purporting to be from legitimate users. As part of the awareness training, users need to be trained to verify the content of emails, before clicking links or volunteering any important information.

One of the participants also referred to malware as a potential attack vector:

…..now the situation has improved somewhat……before IT access policies were streamlined we had some users downloading all kinds of stuff………thankfully much of it was innocuous but we had some surprises in a couple of cases.' [ISP1]

Malware describes various forms of malicious software used by cybercriminals to steal sensitive data such as user login credentials and financial information (Imam, 2020). Users can unintentionally download malware from the internet, phishing emails with attachments and removable media.

Byrd (2021) recommends that users should be made aware of the common delivery methods and the potential threats posed by malware. I would also advise users to always be suspicious of emails with attachments such as images, audio or video files or with links to other sites. I find that there is a misconception among many users that anything malicious (such as email attachments) will get picked up by the company's firewalls and filters, so it's perfectly safe to click on links and open attachments in emails. In reality, that is not the case for a vast majority of organisations.

The increasing use of mobile/smart devices and social media was described by some of the participants as an emerging attack vector.

'…using smart phones and tablets to access the corporate network….this trend is here to stay…..in fact it'll become the norm in the future…..there are many benefits but also potentially huge risks….' [ISA2]

Mobile devices such as laptops, smart phones and tablets certainly pose serious security threats in case of loss or theft. Any sensitive data stored on such devices could fall into the wrong hands, exposing the organization to further threats of unauthorized access and data breaches (USecure, 2021). The rise of social media use is a real concern for organisations:

'we're seeing a lot more of this now…..I mean every other person I know has a social media account of some type……..this culture of sharing everything…there's so much personal data available…..it's easy to see how someone could piece this information together to launch like a spear-phishing attack. Users have to understand the different ways that emails and phishing attacks are used….. cybercriminals can impersonate trusted brands or even other employees from the same organisation………' [ISA4]

I believe that social media offers huge opportunities for organisations, e.g., as powerful marketing and advertising tool to promote their products and services to a global audience. However, unfortunately, cybercriminals also see the opportunities that social media offers to exploit these platforms to launch attacks against organisations, putting their critical systems and reputation at risk. As pointed out by ISP4, user awareness training plays a key role in this.

The participants also made brief references to ransomware, password security and users working remotely as possible attack vector that can be exploited by cybercriminals.

Ransomware is essentially a type of malware through which cybercriminals can encrypt files on a user's computer and demand money in exchange for the decryption key. This type of attack is often carried out in combination with phishing emails. Byrd (2021) points out that although ransomware has been around for more than 30 years, it has gained popularity in the recent past due to the creation of crypto currencies such as bitcoin, providing cybercriminals opportunities to collect ransom money in an anonymous way. USecure (2021) recommends training users about best practices such as not opening suspicious links or files and secure passwords with multi-factor authentication.

The issue of weak passwords and how they can be exploited by cybercriminals to gain access to sensitive data has already been discussed under the first theme. In my experience, users will always be tempted to try to find ways arounds having to remember long and complex passwords. So, this issue is likely to persist and be a challenge for most organisations. Gardner and Thomas (2014) recommend that the focus should be on offering users practical advice such as using alpha-numeric passwords, multi-factor authentication and avoiding careless behaviour such as leaving passwords written on notes.

In the wake of COVID-19, working from home has become the new norm for many users. Whilst this mode of work offers many benefits for businesses, it is not without serious risks.

According to Byrd (2021), users must be trained to ensure that the organisation's network and data is not compromised through remote access. This includes training on updating software, secure WiFi access and use of VPNs to access the corporate networks.

As highlighted by the participants and confirmed by the literature review in chapter 2, social engineering, phishing attacks, and malware are all attack vectors that have increased in frequency and intensity over the recent years. The human error element is quite evident in all of these attack vectors and awareness of these attack vectors inevitably forms an important part of any user awareness training.

Theme 3: Personal and social factors contributing to human errors

The third theme derived from the participant interviews corresponds to objectives 1, 2 and 4 and identifies a number of personal and social factors that the participants highlighted as possible contributors to human errors in InfoSec. I have grouped these factors into appropriate categories and have tried to contextualise them with reference to wider literature and my own personal experience. An understanding of these personal and social factors is important and forms an essential part of effective user training within a comprehensive InfoSec awareness programme.

Schneier (2008) posits that the notion that robust technological security solutions alone can address all of an organisation's InfoSec challenges is a mere myth and demonstrates a serious lack of understanding and appreciation of the issue on the part of many organisations and security practitioners. As discussed under the previous two themes, the participant interviews have already highlighted the role of human factors such as distractions, work pressures, task experience, and user awareness in relation to human errors.

Klahr *et al*. (2017) claim that the vast majority of security breaches experienced by organisations are related to the exploitation of human factors. The end users are often regarded as the Achilles heel for an organisation. Nevertheless, much of the research in this area shows that organisations routinely overlook the role of human factors in security breaches (Moore, 2020). In my experience, many organisations neglect the human element as part of their security compliance evaluations and choose to focus their resources almost exclusively on technological controls and solutions. An understanding of the relevant human factors is crucial to understanding why human errors occur and how they can be addressed to mitigate their adverse effects (Bada, Sasse and Nurse, 2019).

The recognition of humans as the weakest link in InfoSec was clearly expressed in responses from both InfoSec academics and practitioners. ISA4 stated this as a '*well established fact*' and '*stating the obvious*' when highlighting the human element in InfoSec. According to ISP2, there's been a '*paradigm shift*' in how the role of humans is understood within the InfoSec practitioner community.

There was also a general recognition among the participants that many a times human errors result from users not being aware of the security risks and the correct course of action they should take. Without a conscious recognition of the potential security risks, users can also commit errors through their inaction. As an example, a user that is unaware of the risks of phishing emails is more likely to fall prey to phishing attempts. However, as ISA2 pointed out that the '*blame*' for a lack of awareness cannot be attributed '*exclusively to the end user*'. It is the responsibility of the organisation to ensure that its users are given the required awareness and training.

ISA3 alluded to some important aspects of user behaviour when discussing the challenges of implementing InfoSec awareness programmes:

'for any kind of change within the organisation, you need support from the employees….I think this is a major determining factor. You have to see what people are used to and find ways to gradually change things…..it's gotta be thought through….on the other hand, an authoritarian approach can be counterproductive….you'll find many different kinds of employees…in terms of attitudes and perceptions…..most may be cooperative but some may resist change….'

Here, the participant is referring to the importance of considering user habits and different user personalities in organisational contexts. Verplanke (2018) asserts that humans perform many actions as a result of a learned stimulus-response association and get used to performing familiar tasks. Some researchers (Alotaibi, Furnell and Clarke, 2016; Kowalski, Cappelli, and Moore, 2008) have argued that technology use is also directly related to user habits and consequently user behaviour is highly influenced by users' technology usage habits. This theory has been used as the basis for explaining user non-compliance with InfoSec policies (Alotaibi, Furnell and Clarke, 2016).

Researchers have also argued that a definitive relationship exists between user personality and InfoSec compliance behaviour (Alotaibi, Furnell and Clarke, 2016). They point to the research carried out by Shropshire *et al.* (2006); a study based on a sample of 120 computer users using a theoretical model that tested five personality attributes, namely open, agreeable, extrovert, conscientious and neurotic. Their results revealed that the attributes of agreeableness and conscientiousness impact a user's InfoSec compliance in a significantly positive manner.

In another study carried out by McBride, Carter and Warkentin (2012) involving 481 participants, the researchers sought to understand the link between personality attributes and user compliance with security policies. The results showed that open, agreeable and conscientious participants were much more likely to comply with security policies whilst extrovert and neurotic participants were more likely to violate security policies.

Research in this area seems to corroborate the point raised by the participant about the importance of considering the role of user habits and personality in the implementation of awareness programmes.

During the discussion about challenges to building InfoSec awareness programmes and strategies to mitigate human errors, ISA3 emphasised the importance of minimising opportunities for inappropriate behaviour and promoting user satisfaction. The participant suggested that users will commit errors whenever there is an opportunity to do so.

‘if you give them a chance to make mistakes, they will make mistakes!.....this has always been the case....’ [ISA3]

In my experience, this factor is almost always present in all security breaches resulting from human error. The more opportunities that users have to make mistakes, the more likely it is that they will commit errors at some point. As an example, if the IT team allow users to carry out software updates on their own devices (instead of enforcing updates through a policy), there is an opportunity for users to deliberately ignore update alerts due to laziness or carelessness as previously discussed.

I feel that the participant’s reference to employee’s ‘*feeling of wellbeing*’ and being ‘*satisfied with their job*’ is very pertinent since it is a well-established fact that employees that report positive feelings about their employers tend to perform better (D'Arcy, Hovav and Galletta, 2009). It follows therefore that users that are satisfied with their employer are more likely to act responsibly and comply with the organization's InfoSec policies. An empirical study by Hovav and Galletta (2009), involving 223 participants, confirmed that job satisfaction contributes positively to user’s security compliance.

Both InfoSec academics and practitioners highlighted the potential challenges associated with the rapid advances in technology. ISP4 mentioned how the traditional ‘*network perimeter is disappearing*’ whilst ISA3 referred to the changing ‘*user expectations*.’ I have personally witnessed how the technological convergence in the past decade has brought previously unrelated technologies together into a single device, in the form of smartphones and tablets. There is no doubt that this has blurred the lines between the home and the workplace. The traditional office-based work model is fast disappearing and users expect to be able to access and use work related applications and tools from anywhere and anytime. According to Colwill (2009), this rise of “technological democracy” creates some serious security challenges to the status quo. From our human error vs security beaches perspective, users are more likely to engage in behaviour that is detrimental to the overall security of the organisation.

Another important social factor that could potentially contribute to human errors in InfoSec is the organisational security culture. This point was touched on by both InfoSec academics and practitioners. ISA1 referred to the notion of ‘*shared values*’ and ‘*clearly defined expectations*’ whilst ISP3 mentioned the idea of ‘*accountability*’ and the importance of senior staff ‘*leading by example*’.

I believe that end users often know the correct course of action in a given situation but fail to follow it because there is an easier and quicker way to perform the task. However, when such behaviour is condoned and security falls to the bottom of users’ priority lists, error become more commonplace. A positive security culture undoubtedly helps to develop a security conscious workforce and promotes the desired user security behaviour. The importance of a security culture is discussed in more detail under theme 5, as part of strategies to prevent human errors.

Theme 4: Factors that lead to InfoSec awareness programme failure

The fourth theme derived from the participant interviews corresponds to objectives 1, 2 and 4 and identifies a number of important strands highlighted by the participants. A discussion and interpretation of these strands reveals insights into some important factors that could be considered as potential causes for the failure of existing InfoSec awareness programmes to bring about the desired change in user behaviour. I have tried to contextualise the emerging theory with reference to wider literature and my own personal experience. The theory generated in the course of the discussion and interpretations forms an essential part of effective user training within a comprehensive InfoSec awareness programme.

The participants drew attention to the fact that a certain perceptions surrounding the role of InfoSec awareness training persisted among users and senior managers.

ISP2 related how he experienced challenges from management who considered that InfoSec was becoming a '*police function*' with all the '*dos*' and '*don'ts*' and insisted on '*toning down*' to make it more appealing to the users. There was also '*resistance*' from some older employees who thought the whole thing was '*trap to catch them out.*' The attitude displayed by some of the other employees was: '*not another training please!*'

In describing the lack of buy-in from senior management, ISP4 referred to InfoSec awareness being '*treated as a stepchild*', that management did not seem to want to '*own*'.

ISP1 framed the users' perceptions of InfoSec awareness as:

'....they don't see how they can be affected....they're often oblivious to the threats around them...[they] don't get how they can expose vulnerabilities through their actions.....so security is rather an inconvenience....something outside of normal pattern of behaviour...in essence we're asking them to make a change to this behaviour which frankly is physically and mentally uncomfortable for many users.'

ISP2 also drew attention to the disparity between priorities of senior management and InfoSec professionals:

'...there are different agendas.....when it's a choice between delivering projects vs delivering awareness training.....projects generate revenue, so it's a no brainer...it's difficult for them to see the direct returns (ROI) *from security.'*

The participants' accounts above are quite representative of my own experiences with senior management. Although, I find that there has been significant improvement in perceptions and attitudes towards InfoSec awareness, unfortunately the 'tick-box' perception of awareness training still persists in some quarters.

Winkler and Manke (2013) point out that InfoSec awareness training is often perceived by management to be a mere compliance requirement. Although many compliance standards include awareness training as a requirement, they tend to be very vague and on their own do not guarantee security. Compliance with standards is a part and parcel of a successful security awareness programme and not the goal in itself.

Compliance standards generally outline generic requirements for a security awareness programme without details of the required content and structure. The auditors tasked with evaluating compliance often tend to know little about what makes a good awareness programme (Sjouwerman, 2021**)** and would easily approve once a year training session comprised of a short awareness video with a quiz to prove that all users participated and passed the quiz. Such activities form a very small part of a comprehensive awareness programme and on their own do not prove that they achieve the desired user behaviour (Legárd, 2020).

ISA4 raised an issue that could be considered a logical consequence of some of the challenges identified above by InfoSec practitioners:

'A lot can be deduced about an awareness programme from the person an organisation puts in charge to run it….does this person have the background and qualifications for the role?...often the answer is no!' [ISA4]

The participant is drawing attention to the fact that one can gather how much importance an organisation places on their awareness programme from the kind of person they appoint to run it. In my experience, this is not always thoroughly considered and often organisations hand over this important responsibility to security professionals that may have the right technical qualifications but lack other important skills. This is really reflection of a failure to recognise InfoSec awareness as a unique discipline in its own right.

Gardner and Thomas (2014) point out that in addition to relevant technical knowledge, skills and abilities, the person appointed to run an awareness programme must also possess appropriate communication and marketing skills since persuasion is an integral part of awareness. According to Bada, Sasse and Nurse (2019), a competent InfoSec awareness practitioner will also have familiarity with theories of learning and knowledge of different awareness techniques and tools.

ISA3 suggested that the failure of InfoSec awareness programmes can be attributed to a lack of understanding of what InfoSec awareness actually is:

'senior management and unfortunately also some security professionals don't seem to understand what the whole fuss is about….the finer distinctions are not understood and appreciated….it's not just semantics…this leads to inconsistent policies and messaging as far as the users are concerned.'

The participant was referring to differences between security awareness and security training. I think it's a valid point since security training and security awareness are not synonymous. The job of security training is to equip users with necessary security knowledge and repeatable skills to perform their jobs whilst the goal of security awareness is to change user behaviour. Gardner and Thomas (2014) point out that the act of delivering knowledge and skills to the user does not guarantee a change in behaviour. It must also take into account how users think and behave and create a personal connection of how the acquired knowledge impacts user actions.

In my experience, the terms security awareness and security training are often used interchangeably in the InfoSec industry. However, the two are not synonymous; in awareness activities, the user is the recipient of information, whilst during training a user is an active participant (Wilson and Hash, 2003). InfoSec awareness training does not aim to equip users with detailed technical knowledge of security policies and the various cyber threats but rather to provide them with general understanding and awareness of security related issues.

Santarcangelo (2011) defines awareness as a cultural attribute that is ultimately achieved through a combination of training, education, and life experience. The goal of awareness is to focus user attention on security in order to change behaviour and reinforce good security practices (Wilson and Hash, 2003). Awareness intends to help users recognise security concerns and respond accordingly. The user response is guided and supported through training that is tailored to their job-specific needs (Tomhave, 2010).

Both InfoSec academics and practitioners raised the issue of training materials and frequency of awareness training as important determining factors for the success / failure of awareness programmes.

ISP2 discussed the importance of '*tailoring materials to the audience*' and to present materials in a '*language*' and '*format*' that is '*relevant*' and '*appealing*', so the users do not '*tune out.*' ISP1 mentioned that he was restricted in '*how far*' he could go with training materials because it was difficult to get senior managers '*to sign off the required budget.*' In ISP4's case '*visual aids*', '*posters*' and '*newsletters*' were the easiest and readily available '*low-cost options.*'

According to ISA4, the '*amount of budget*', mode of delivery and '*quality of materials*' is all indicative of '*how much the organisation values security awareness training for its employees*.'

ISP2's point about relevant and appealing materials is certainly valid. Gardner and Thomas (2014) point out that many awareness programmes fail to change user behaviour because they are simply not engaging or appropriate for the organisational culture.

Some of the participants hinted at using online and computer-based training (CBT) for their awareness training and this in my experience is the most common (and perhaps most effective) choice of delivery mode. As Sjouwerman (2021) points out, when organisations have a 'check box mentality' towards awareness training, lower cost is often the determining factor. Consequently, many organisations favour a particular training delivery method because it appears to be the cheapest and easiest option that ticks the boxes for the purpose of compliance.

ISP2 and ISP3 both stated that their awareness training was predominantly focused on social engineering attacks and phishing simulations as they considered these to be '*the most prevalent attack vectors*.' Whilst this view is certainly corroborated by research (in chapter 2), I think it is potentially problematic. According to Legárd (2020) phishing simulations are useful and provide extremely valuable metrics but they only address a specific security awareness problem. I would argue that it is not adequate to focus all awareness training efforts on one or two specific topics. It is important to have a programme that covers a broad range of user behaviour related security awareness topics, delivered through different modes over multiple training sessions.

ISA1 highlighted an unintended and undesirable consequence of '*over doing*" security awareness:

'if the messaging, the format, and frequency are not carefully thought through….you just keep bombarding them with information and alerts about threats and policies…..you get to a point when they just switch off….they'll stop responding..'

Here, ISA1 drew attention to an important issue that could potentially result in failure of an awareness programme to change user behaviour. This can happen, as discussed previously, if security is perceived to be an inconvenience or an obstacle in users' everyday jobs (Gardner and Thomas, 2014). Bada, Sasse and Nurse (2019) caution that users could find the demands to always maintain a high level of vigilance and awareness quite stressful, leading to security fatigue.

ISA2 emphasised the importance of using metrics to evaluate the effectiveness of InfoSec awareness programmes:

'…having a programme is all well and good……without a mechanism to check that it's doing what it's supposed to do…I mean without that it's just a waste….time, money, effort…in the long run it's all meaningless.'

Gardner and Thomas (2014) state that a key factor in the failure of awareness programmes to change user behaviour is the inability of many organisations to measure the effectiveness of their awareness programmes.

ISP2 and ISP3 both described the use of '*user responses to phishing emails over a period of time*' to gauge the success of their awareness training. They mentioned receiving daily reports of '*percentage of fake links clicked*' by users and number of instances that users '*give up passwords*' in response to phishing emails. ISP2 also described the use of a learning management system (LMS) to deliver additional '*training with quizzes embedded in the material*' to track users' progress over time. ISP1 related that he did not have the opportunity (perhaps also the budget) to be '*innovative*' and simply '*tracked the number of employees that completed basic online training*.'

I believe that the importance of metrics to evaluate an awareness programme cannot be overemphasised. Evaluation can be accomplished through metrics before, during and after the implementation of a programme to assess if it is achieving the desired results. Organisations can collect various metrics such as before and after quiz scores, surveys, phishing email click rates, attendance rate, user feedback, etc. to determine what works and what does not work for their particular contexts and fine-tune the programme accordingly. The use of evaluation metrics and the results produced can serve as tangible proof to convince senior management about the importance of the awareness programme.

One of the frustrations expressed by the participants was the unrealistic expectations that management and sometimes users had of InfoSec awareness programmes:

'it takes so much effort to convince management to put a programme in place….when we finally get something in place….the expectations are just completely off the chart….we've been challenged many times…even the smallest inkling of a security issue….like this is supposed to fix every kind of security problem there is!' [ISP2]

'…difficult as it is to get across…..security threats will always be there……no amount of countermeasures or awareness training can mitigate everything.' [ISA3]

In my professional career, I have experienced being questioned and the value of security training being challenged. Unfortunately, there is tendency in some organisations to regard security awareness training as a panacea for all of their security related problems (Brodie, 2008). As Bada, Sasse and Nurse (2019) point out, security awareness is a process and not a one-stop solution for every security problem. When the human element is introduced into the security equation, there is no such thing as 100% security. The focus of security awareness is risk mitigation and not complete prevention.

Theme 5: InfoSec strategies to prevent human errors

The fifth theme derived from the participant interviews corresponds to objectives 1, 2 and 4. In the previous discussions, the participants identified what they considered to be the most important factors contributing to human errors in InfoSec. It was established that many of these factors have their origins in user carelessness and lack of awareness about InfoSec practices. The preceding discussion also highlighted the role of opportunity and the organisational security culture as two important factors contributing to human errors. The participants also indicated the potentially positive role of these two factors in helping to prevent human errors. In discussing the role of these two important factors in light of participants' responses, I have tried to contextualise the emerging theory with reference to the wider literature and my own personal experience. The theory generated in the course of the discussion and interpretations forms an essential part of effective user training within a comprehensive InfoSec awareness programme.

As discussed earlier, one of the primary reasons that users commit errors is because there is an opportunity for them to do so. ISA3 alluded to this point:

'if you give them a chance to make mistakes, they will make mistakes!.....this has always been the case….'

Therefore, it is crucial for organisations to reduce the opportunities for users to commit errors as much as possible. According to ISA3, this '*requires changes*', both in terms of '*technology and organisational practices….of course much depends on the environment and nature of business……generally though, access to resources must be granted carefully…..depending on roles and what employees need for the task…'*

I agree with the above assessment. The participant is referring to the idea of role-based user access to organisational resources. In the field of InfoSec, the principle of least privilege (POLP) is used to ensure that a user has only the minimum amount of access rights and functionality required to perform their job. The user's privileges can be increased if and when required. This will minimise the organisational exposure to a variety of security risks such as inadvertent deletion or corruption of data.

Another example of an approach to reducing opportunities for users to commit errors concerns the management of password security. As discussed previously, password related human errors are some of the biggest causes of security breaches. One of the reasons that users fail to take proper action despite knowing better is what is referred to as pain avoidance (USecure, 2021). It is suggested that creating and remembering a unique and strong password requires effort (pain) on the part of the user. One way to address this problem is to free the user from the burden of creating and remembering passwords by introducing password manager software or by employing other methods such as biometric and two-factor authentication.

The security culture of an organisation defines the values that underpin how users are expected to think and behave as it relates to security. A strong security-focused culture is undoubtedly crucial in reducing human error. This was something highlighted previously by ISA1 who alluded to the notion of '*shared values*' and '*clearly defined expectations*' whilst ISP3 referred to the idea of '*accountability*' and the importance of senior staff '*leading by example*'.

Research exploring organisational security culture has postulated that it can have both negative and positive impact on user behaviour as it relates to compliance with security policies (D'Arcy, Hovav and Galletta, 2009; Alotaibi, Furnell and Clarke, 2016). A poor security culture promotes an environment of sloppy cyber practices, finger-pointing, and mistrust. On the other hand, in organisations that value security by putting in place protective security measures, awareness and training programmes and strict compliance procedures that hold users accountable, it follows that users will be more willing and likely to comply (Furnell and Clarke, 2016).

Gardner and Thomas (2014) argue that security has to be embedded into everyday staff culture. A strong security-focused culture is one that is proactive rather than being reactive, ensuring that security is a key consideration in every action and decision. I would also argue that a security-focused culture is one where security-related issues are discussed with end-users, keeping them informed, encouraging them to learn about cyber risks, to ask questions, and reward them for being proactive. Using this approach, users become an extension of the security team (Price, 2018). ISA1 suggested the use of '*reminders', 'daily security tips', 'screen savers'* and *'office posters'* as some of the techniques to ensure that users are actively thinking about security.

A security policy defines the rules, standards, and guidelines for allowed activities and outlines the expected user behaviour with regards to an organisation's systems, data and assets (Yeagley, 2015). Arkvik (2021) posits that a security policy is an important expression of an organisation's overall security posture and a crucial part of a security-focused culture.

In summary, it could be argued that managing these factors (reducing opportunities for errors and promoting a security culture) are perhaps two of the most important approaches to preventing human error in InfoSec.

Theme 6: Understanding the psychological perspective of human behaviour in InfoSec

The sixth theme derived from the participant interviews corresponds to objectives 1, 2 and 4. In the previous discussions, the participants identified a number of personal and social factors as potential contributors to human errors. This section discusses various strands revealed from the participants' responses that are grouped under the broad category of psychological perspectives of human behaviour. The participants' responses touch on concerns related to the field of Human Computer Interaction (HCI) and the various sources of influence on human behaviour. I have tried to discuss and interpret the emergent strands with reference to existing literature in the field and my own experience, where applicable. The emergent theory will facilitate an improved understanding of the phenomenon under study and will form an essential part of effective user training within a comprehensive InfoSec awareness programme.

As discussed in the literature review section, the primary goal of security awareness training is to change user behaviour.

ISA3 asserted that:

'…..a lot of persuasion is required to get the employees on board….get them to act differently….to change their ways…easier said than done!....trouble is that persuasion alone is not always enough…you need to understand what makes them tick…a way to understand why users behave the way they do or conversely why don't they behave the way we expect them to…this is a fertile field for research….a lot of it still not explored properly.'

One of the main goals of awareness training is to persuade users to change their behaviour. However, what ISA3 is suggesting is that persuasion alone does not always work; that an understanding of the users' motivations and thought processes is also required in trying to change their behaviour. A number of researchers **(**Bada and Sasse, 2014; Robinson, 2021**;** Dolan, *et al*., 2010; Coventry, *et al*., 2014; Spitzner, 2012) have attempted to address this issue from the perspective of psychological models of human behaviour in order to identify potential factors that could facilitate a change in user behaviour.

ISA2 claimed that:

'…..changing behaviour cannot be achieved by just giving information about threats and expectations…..there's more to it…..the employee must understand it's importance, be willing to act and then actually go ahead and apply that information…..so in essence it's about effecting change in perceptions, intentions and attitudes.'

ISA2 is alluding to change in user perceptions, intentions, and attitudes by influencing the user's thought process. Patterson, *et al*. (2007) note that the use of influence strategies to change user behaviour has been studied and discussed by psychologists and social scientists for some time. Spitzner (2012) points out that influence strategies are already being used by cybercriminals through social engineering techniques to lure their victims. He claims that these techniques can be applied equally effectively by the “good guys” to achieve their goals. Wilson and Hash (2003) refer to the use of interesting and topical material as a way to make security messages persuasive and in turn influence user behaviour. According to Berkowitz (2000), the essential attributes of persuasive messages are: able to attract user attention, easily understood, relevant to the issue at hand, reduce resistance, and motivate desired action. Bada and Sasse (2014) refer to the use of ‘language of persuasion’ from psychological research to influence and change user behaviour. They argue that the use of persuasive messaging techniques is prevalent in media, advertising, and public relations, where the proponents seek to establish credibility and trust to arouse interest for a product or policy in order to motivate people to act in a certain way, e.g., to buy something or vote for someone.

Bada and Sasse (2014) argue that to effect change in user behaviour it is important to identify the various sources of influence affecting human behaviour. These can be conscious or unconscious influences, as well as personal, social and environmental influences.

Dolan, *et al* (2010) describe conscious influences in terms of a cognitive model that seeks to influence what users consciously think about. It suggests that users will consciously analyse and evaluate the information presented to them and consider the incentives in order to act according to their own best interests. The unconscious influences can be described in terms of a context model in which information and facts are less important and the focus is on automatic processes of judgement, rather like a mental shorthand (Cialdini, 2009). This approach to influencing behaviour seeks to change user behaviour without persuading or changing minds. Not surprisingly, the context model has received rather less attention amongst InfoSec researchers (Bada and Sasse, 2014).

Coventry, *et al*. (2014) note that personal motivations are one of the most dominant influences on user behaviour and are derived from the users’ knowledge, ability, skills, understanding of security issues along with their experiences, attitudes, beliefs, feelings, and perceptions. Personal influences include feelings connected with user actions, e.g., taking pride in a job, being satisfied at accomplishing a difficult task or being resentful for being coerced to do something. Patterson, *et al*. (2007) recommend that when users’ actions are linked to their personal values, they are more likely to exhibit positive behaviour.

Robinson (2021) points out that humans by nature tend to conform to social norms. As such social influences are linked to social interactions with other people and peer group pressure, whether that means following an established authority or simply following the crowd.

Patterson, *et al*. (2007) describe environmental influences on user behaviour as those originating from the physical environment of the user or the organisational culture in the way that it deals with user activities, e.g., reward and punishment, etc. According to Coventry, *et al*. (2014), environmental influences include user environment, the physical workplace and the technology. A change in environmental influences is often one of the easiest ways to achieve the desired change in user behaviour.

I believe that the perspectives offered by the participants and expounded upon by research in the field provide very useful insights into human behavioural factors that could help InfoSec professionals to employ and exploit the various sources of influence on user behaviour in order to design and implement more effective InfoSec awareness training programmes.

The participants also drew attention to an interesting and important approach to dealing with the problem of human errors.

ISA4 framed this as:

'.....the role of humans in security breaches is a well established fact....that's like stating the obvious....there must also be some consideration of technology design....especially poor design....how that facilitates human error and ultimately security breaches.....there are many examples....sharing of sensitive files, emailing the wrong recipient, unauthorised system changes.....a lot of these can be avoided...we can't pin all the blame on our employees.'

The participant's statement is essentially a reference to the field of Human Computer Interaction (HCI) which deals with how humans interact with computers. According to Jones (2005), the focus of HCI is to produce usable and safe systems. The three main elements of HCI are: human (user of the system), computer (any form of technology), and interaction (how the two work together). Sasse *et al* (2007) point out that to develop functional systems, the design process must be informed by an understanding of technology as well as human behaviour.

According to Bada, Sasse and Nurse (2019), the InfoSec research community has recognised that human behaviour has a crucial role in many security failures and has called for the human element to be considered in the design and implementation of security systems.

HCI-Sec (HCI related to InfoSec) is a specialist (and relatively nascent) field concerned with improving the usability of security features in end user systems. ISA1's statement below could therefore be framed in terms of this HCI-Sec perspective:

'dealing with the human factors is one aspect of the security problem......there is a need for smarter application design....one with embedded security...I don't mean the traditional application security as part of software development....it's more about design that facilitates users to act in a security conscious way...'

With an increasing role of human factors in InfoSec failures, HCI-Sec has attracted much attention from InfoSec researchers. It is essentially a transdisciplinary field that necessitates additional insights from InfoSec researchers and practitioners.

In my opinion, the participants, both being academics with research backgrounds have highlighted an important issue. It is certainly true that many security breaches can be traced back to human errors. However, it is also very noteworthy that many human errors can be attributed to poor HCI-Sec design that can inadvertently facilitate security breaches. According to Shelton (1999), HCI acknowledges the user as a fundamental element in the design of the system. Consequently, poor design will increase the likelihood of human errors. A good HCI-Sec design encourages the user to perform the task correctly and protect the system from errors.

Theme 7: Essential components of an effective InfoSec awareness training programme

The seventh theme derived from the participant interviews corresponds to objectives 2 and 4. In the previous discussions, the participants identified various factors that they considered to be possible causes for the failure of InfoSec awareness programmes. This section discusses the various strategies and elements highlighted in the participants' responses that are considered to be essential for an effective InfoSec awareness programme. The participants' responses have been interpreted in the context of existing literature in the field as well as my own experience. The theory generated in this section directly addresses objectives 2 and 4 of this project and is therefore an important step towards answering the research question.

As discussed in the previous sections, the participants' responses highlighted numerous factors that can contribute to human errors, resulting in security breaches and ultimately the failure of an InfoSec awareness programme. It was also established from the participants' responses and current research that a significant proportion of these human factors have their origins in user carelessness and lack of security awareness.

As discussed in the literature review (chapter 2), InfoSec awareness training is considered to be one of the most effective non-technical measures available to effect a change in user behaviour in order to ensure security of an organisation. This point was also echoed in the participants'' responses.

ISA2 emphasised that:

'a lot of security problems can be traced back to ignorance……the users not understanding the risks and what to do when they face such risks…..so they need the basics of security….they must be educated and trained on best practices…..that is the way to equip them to make sensible decisions.'

According to ISA1:

'….it is important for them to have a basic but broad familiarity with security topics they are likely to encounter……email, social media, phishing, malware….'

ISP3 described awareness training as:

'….. considering the traditional concept of security in terms of different layers… awareness training can be thought of as an additional layer of protection against attacks and breaches.'

McIlwraith (2006) asserts that "raising awareness is the single most effective thing that an InfoSec practitioner can do to make a positive difference to their organisation." Herold (2005) claims that …."security awareness training has been the most valuable yet the most overlooked and underfunded mechanism for improving the implementation of InfoSec."

I agree with the above assessment that investing in user awareness is perhaps one of the most critical and cost-efficient initiatives that an organisation can undertake. I would also add that awareness training is not a one-off solution but rather a continuous process in which users need to be constantly reminded of the potential security risks in their day-to-day activities. Ultimately, the protection of an organisation's information is the responsibility of all staff.

Whilst discussing what they considered to be essential components for an effective awareness programme, the participants highlighted the importance of presenting '*relevant material*' that includes '*real life examples that the users can relate to*.' [ISP4]

I also believe that InfoSec professionals must assess user roles and deliver awareness training according to their needs, in order to reinforce the message. Training material that is replete with jargon and technical terms will cause users to soon lose interest (Reciprocity, 2021).

ISP2 mentioned the importance of '*breaking down*' the material. I agree that it is important to deliver awareness training as small digestible segments with clear and simple messages so that users do not suffer from information overload.

Another useful suggestion offered by ISP4 was the idea of '*practical tips and guidelines*' that users can '*take away*' with them and '*immediately put into practice in their daily lives.*' Taking this one step further, Bada, Sasse and Nurse (2019) have emphasised the importance of testing users as a post training activity. Some of the participants had already described the use of simulated phishing attacks as their evaluation metrics. These could be used to test post-training user behaviour, so that users that fail such tests can automatically be referred for additional or refresher training (USecure, 2021).

Here, I would like to reiterate an earlier point about the importance of not treating awareness training as a one-off event on the annual work calendar. User awareness training is a process and must be repeated at regular intervals to ensure that the messages are retained, and security remains a high priority for all users. Breaking down training material into smaller manageable parts and delivering small segments to users throughout the year can ensure that the learning process is continuous.

The participants described a variety of methods that they have employed in their work environments to educate and raise user awareness as part of their InfoSec awareness programmes.

ISP3 stated:

'I try to make it [awareness training] *fun and interesting……for example I use movie posters with some kind of security related theme…it's an interesting way to catch people's attention….it gets them talking….and that's part of the aim….once people take interest in something, it's easier to start that conversation and introduce the security messages in a subtle way.'*

ISP2 described a different approach:

'One of the things we experimented with was using merchandise to push out security messages………things like pens, mouse mats, notepads and key fobs….there are many options. It was very well received but unfortunately we couldn't continue due to budgeting issues…..posters are also a great way to educate users…but they must be spread out throughout the workplace and updated regularly…..there are some great fun ideas online….we've created our own customised versions….'

ISP4 related:

'The security awareness day events have been a great success….lots of interest from employees and even managers…we've invited external speakers to talk about various security topics…sometimes it's difficult to get the numbers but I find that an offer of free snacks and drinks always helps!'

ISA2 described the use of '*visual aids*' and '*posters*' as '*cost-effective options*' that can serve as '*helpful reminders of security awareness*' in the workplace.

ISA4 suggested that there are '*a variety of means'* available to accomplish user awareness including use of '*email reminders*', '*posters*', '*web campaigns with tips and tricks*' and '*security advice adapted to specific business needs and operations*.' Other awareness raising methods suggested by ISA4 include *'screensavers with security messages', 'regular organisation-wide e-mail security messages', 'newsletters'* and *'brown bag seminars.'*

On reflection, my own past experience of InfoSec awareness programmes has been one where awareness training was considered a one-time annual event in which users sit through lengthy lectures consisting of slideshow presentations. For the most part, this type of training was considered a formality to ensure certain forms of regulatory compliance. Unfortunately, this approach to awareness training is not effective in terms of achieving the desired user behaviour. It is simply too much information for end users to digest and retain, let alone put into practice. This kind of training format is also not very engaging for end users (Gardner and Thomas, 2014) as it fails to arouse interest in users in the way that video and interactive content can do. The long intervals between training sessions and the lack of learning through repetition element means that user awareness plummets rapidly and security is no longer a focal point for end users (Legárd, 2020).

What has become increasingly clear to me over the years is that InfoSec awareness training is not a one-size-fits-all solution that can be applied uniformly in all situations. It is important to consider how training is structured, presented, and delivered in a way that will maximize its effectiveness in changing user behaviour and improving security for an organisation.

The methods highlighted by the participants to raise user awareness are certainly helpful in complimenting a comprehensive InfoSec awareness training programme rather than being deployed as substitutes or stand-alone solutions.

In addition to the methods used to raise awareness, it is also important to consider the most effective modes of delivery for awareness training.

ISP4 mentioned that:

'I personally favour the idea of classroom-based training.....there are opportunities for interaction, discussions, Q&A sessions, group activities.....the employees are not distracted....you have their attention....We tried this out for a bit but couldn't really sustain it...it wasn't cost-effective.....logistically it was challenging and the management hated it because employees were being taken away from their main tasks.'

The participant described his experience with classroom-based training and despite the many benefits, admitted that it was not a feasible option. Gardner and Thomas (2014) also point out that due to staffing issues, workforce distribution and availability of facilities, this mode of delivery is not the most efficient or cost-effective option.

ISP1 described making use of '*pre-installed training packages*' that consisted of '*video and other interactive content*' with '*embedded quizzes and activities*.' I have been involved in the design and rollout of this type of training materials. In my experience, this delivery mode is a great way to engage and train users that may not be suited to other more traditional modes of delivery. Users can watch videos, answer comprehension questions, and take part in interactive activities that test their understanding by allowing them to apply their knowledge in various hypothetical situations.

Most of the InfoSec practitioners confirmed that their awareness training was delivered through some kind of online platform. ISP3 mentioned using a third party company to purchase a web-based platform that they '*customised*' to their '*business specific needs*'.

I believe that the participants' experiences reflect the current trends in the InfoSec awareness training market. The online mode of delivery is increasingly popular amongst organisations as it can accommodate potentially unlimited number of users. It also offers flexibility by allowing users to work through the training material at their own pace, at any time and from any place. Legárd (2020) points out that businesses tend to favour this mode of delivery as it ensures that employees remain productive.

ISA1 touched on the idea of '*gamification of awareness training',* a concept that applies game mechanics to increase user engagement and loyalty; it is becoming increasingly popular in cloud-based training solutions.

ISACA (2019) point out that in the recent past, security awareness training has shifted to online or cloud-based delivery methods, typically in the form of software as a service (SaaS) model as this offers many advantages over the traditional delivery methods.

In my experience, no single mode of delivery can achieve the desired change in user behaviour. In practice, a combination of delivery methods is likely to be more effective in helping to get the message across to the users (Legárd, 2020).

InfoSec awareness programmes have long been promoted as being fundamental to improving organisational security. An intuitive assumption is generally made that increased security awareness leads to a security-enhancing change in user behaviour (D'Arcy, Hovav and Galletta, 2009). However, as is quite often the case with users, having an awareness of security risks does not always translate to correct user behaviour (McIlwraith, 2006). In practice, it is difficult to measure the benefit derived from InfoSec awareness programmes.

The idea of evaluating InfoSec awareness programmes was previously discussed under theme 4 in the context of factors that lead to failure of awareness programmes. ISA2 expressed the importance of evaluating the effectiveness of InfoSec awareness programmes:

'…having a programme is all well and good……without a mechanism to check that it's doing what it's supposed to do…I mean without that it's just a waste….time, money, effort…in the long run it's all meaningless.'

According to ISA3:

'…quizzes, questionnaires and surveys are some of the ways to measure employee awareness and establish baselines……the results can be compared after training to gauge the improvement…..security professionals can monitor trends over time for number and frequency of incidents….this would serve as a good indicator…to see if the programme is making an impact.'

The participant has offered some useful suggestions for evaluating an awareness programme. Vlandan (2020) suggests that in case of simulated phishing campaigns, employee responses to drills can be tracked over time to look for improvements after training.

I would also suggest that if an organisation lacks the internal resources and expertise, it is possible to consult third party specialists to assist with delivery and impact analysis of security awareness training. There is also a plethora of ready-made online security awareness training solutions that organisations can choose from. Some of the most established platforms include KnowBe4, Infosec IQ, Proofpoint and MetaCompliance to name a few (G2, 2020).

Regardless of the mode of delivery, use of internal or external expertise, senior management buy-in is a crucial element of an effective security awareness programme. The importance of senior management buy-in was highlighted by the participants under theme 4, where it was pointed out that a lack of management buy-in is a factor contributing to failure of InfoSec awareness programmes. Gardner and Thomas (2014) emphasise that business leaders must understand the requirements for planning and creating a security awareness training programme, be involved in the implementation and offer feedback throughout the process.

I would also reiterate, as discussed under theme 4, that to be truly effective, security awareness training has to be an embedded part of organisational culture, delivered regularly all year round and constantly adapting to the evolving threat landscape.

Summary

This chapter presented the findings of the project through a discussion and interpretation of the participant interviews. The findings were corroborated and reconciled in light of the literature review in chapter 2, additional relevant literature as well as my own professional knowledge, experience, and ontological and epistemological stance.

The findings presented in this chapter focus on the phenomenon surrounding the effectiveness of InfoSec awareness programmes and how such programmes can be improved to reduce human errors in InfoSec. This chapter discussed and interpreted the responses of the research participants (InfoSec academics and practitioners) in terms of the shortcomings in existing InfoSec awareness programmes and recommendations and possible solutions to make awareness programmes more effective vis-à-vis human errors.

The new knowledge that has emerged in this chapter will be presented in the next chapter in a coherent and meaningful way in the form of guidelines intended to help improve the processes and practices used to develop and implement effective InfoSec awareness programmes. The guidelines, as the principal outcome of this project, will make a significant contribution to my community of practice as well as benefiting my own professional practice.

Chapter 6: Conclusions & Recommendations

Overview

This chapter starts by restating the research problem and the four main objectives derived from it. The findings from the previous chapter will be presented in accordance with each project objective in order to demonstrate how each objective has been met. I will also present the findings in a coherent and meaningful way, in the form of guidelines intended to help improve the processes and practices used to develop and implement effective InfoSec awareness programmes.

This chapter will also present a discussion of the value of this project and the applicability of the outcome to my field of practice and the stakeholders. This will be followed by a discussion of the limitations of this project and recommendations and avenues for further research. Finally, I will present my reflections on the overall project and future directions.

6.1 Restating the Research Problem

Human error is arguably the greatest cause of InfoSec breaches. Consequently, human error can have potentially catastrophic consequences for organisations in the form of financial losses (loss of revenue, regulatory fines, mandatory compensation), loss of consumer confidence and damage to reputation. Security awareness training seeks to bring about better security through a positive change in user behaviour. Awareness training programmes form a crucial part of an organisation's overall security posture. Existing research shows that security awareness training is probably one of the most cost-effective ways to mitigate the risk of security breaches resulting from human error. Research also indicates steady increases in overall security budgets, specifically, organisational security awareness training budgets as well as the average user training time has been increasing steadily over the recent years. All of these crucial indicators seem to point to a state of security awareness training that is robust and fit for purpose. However, most recent global security surveys reveal that human behaviour remains probably the single greatest threat to InfoSec and security breaches resulting from human error are still rampant. Despite the prevalence and increased take up of awareness programmes amongst organisations, security breaches caused by human error are on the rise. It seems that issues persist with managing human behaviour despite the efforts of organizations to put in place suitable awareness programmes.

This phenomenon necessitates the need for a better understanding of why security awareness programmes fail to effect the desired change in user behaviour. Research findings seem to suggest that awareness training does not automatically lead to the desired user behaviour. This raises questions about the effectiveness of awareness training programmes and how such programmes could be made more meaningful and contextualized with suitable evaluation and feedback mechanisms to ensure continuing currency and relevance. This also raises questions about the methods used to communicate security messages to persuade users and the way that users process and respond to such messages. The research also raises issues relating to current approaches to managing human behaviour in InfoSec and how these could be improved to effect change in user behaviour. There are also questions surrounding the role of organisational culture in changing user behaviour. Although these were some of the more obvious issues and concerns that emerged in light of the literature review, more pertinent issues were expected to transpire during the course of this research.

6.2 Project Outcomes on the Basis of Research Objectives

This project was an effort to gain a better understanding of the issues surrounding InfoSec awareness training programmes and why they fail to effect change in user behaviour as their intended purpose. It was also an attempt to explore the possible solutions to the aforementioned problems and to elucidate the findings in the form of guidelines that could be incorporated into future organisational security awareness training programmes to reduce InfoSec breaches resulting from human error.

I set out to answer the following research question:

- ➢ *What are the main shortcomings in existing information security awareness training programmes and how can these be addressed in order to reduce human errors?*

The research question was broken down into the following objectives:

- *Establish the main shortcomings in existing InfoSec awareness training programmes (vis-à-vis human errors) on the basis of a literature survey and engagement with InfoSec academics and practitioners*
- *Determine possible solutions to help make InfoSec awareness training programmes more effective (vis-à-vis human errors) based on engagement with InfoSec academics and practitioners*
- *Assess the validity and reliability of the proposed solutions (that emerge from objective #2) by corroboration with existing literature and own experience*
- *Derive and formulate practical guidelines that can be incorporated into future InfoSec awareness training programmes to reduce human error*

In order to achieve the project objectives and answer the research question, I employed a multi-faceted research approach, drawing upon a robust literature survey and in-depth phenomenological interviews with InfoSec academics and practitioners. In the following sections, I present the findings from the previous chapter in the form of guidelines, in accordance with project objectives 1 and 2. It is important to note that objective #3 has already been addressed in chapter 5 during the course of the discussion and interpretation of the findings. In chapter 5, I offered a critical analysis of the findings with reference to wider literature and my own personal knowledge and experience in the field. This helped me to assess the validity and reliability of the findings and served as a form of triangulation. Furthermore, objective #4 is addressed in the form of guidelines that are presented below. The guidelines offered here are not meant to be prescriptive as their applicability and suitability depends on the specific business needs and environments.

Objective #1: Establish the main shortcomings in existing InfoSec awareness training programmes (vis-à-vis human errors) on the basis of a literature survey and engagement with InfoSec academics and practitioners.

In chapter 2, a literature review was presented in order to offer a 'big picture' of the major issues related to InfoSec awareness training programmes and to make connections across the broad related areas to enable the reader to develop a sense of the phenomenon of interest and the significance of the research. I opted for a partial review of the literature in order to strike a balance between the customary research practice (of exhaustive literature review) and not constructing a priori explanation of what the phenomenon 'is' or 'should be' according to pre-existing theoretical explanations. It was explained that an exhaustive literature review of the phenomenon prior to data collection phase could jeopardise the open-minded approach called for in IPA studies. However, I returned to the literature review (chapter 2) and also introduced some new literature during the data analysis phase (chapter 5) in order to frame the new angles that emerged and to place the findings in a wider context within my field of practice. A detailed discussion of the approach taken was provided in chapter 2.

The insights offered by the participants in relation to objective #1 had resonance across multiple interpretive themes. This section discusses factors that the participants identified as possible causes for the failure of InfoSec awareness programmes. The guidelines are presented here in a condensed format and the reader is advised to refer to chapter 5 for details. Objective #1 could also be interpreted as:

- ➢ What are the factors that must be understood and considered as part of an effective awareness programme?
- ➢ What are the factors that render an awareness programme ineffective?

All discussions related to objective #1 will be organised under the above headings.

What are the factors that must be understood and considered as part of an effective awareness programme?

In order to gain an accurate understanding of the shortcomings in existing InfoSec programmes, the participants emphasised the need to recognise and understand some of the most common user actions that contribute to human errors.

The use of weak passwords by end users was identified as one of the easiest ways for cybercriminals to gain access to sensitive data. As such weak passwords were identified as a major contributing factor to human errors and in turn security breaches.

The careless handling of sensitive data by users was highlighted as a major concern. The participants also identified the use of unauthorized and outdated software by users as a vulnerability that is often exploited by cybercriminals to gain access to sensitive data.

It was established that the common user actions identified by the participants had their roots in carelessness and lack of security awareness whereby carelessness can be a major factor in and of itself and can also be the consequence of a lack of awareness.

The participants' responses drew attention to the role of human factors such as negligence, carelessness, forgetfulness, and laziness and how these contribute to human error. It is worth noting that these human factors combined with lack of security awareness could potentially pose serious security threats to an organisation. Such employees could easily fall prey to a variety of attacks that cybercriminal can exploit to gain access to sensitive data.

The participants' responses emphasised the need to identify and understand the most common attack vectors faced by organisations. Social engineering attacks were regarded as the 'main weapon of choice' for cybercriminals and the frequency of such attacks along with phishing attacks was reported to be on the rise. Recent research also suggests a surge in phishing attacks in the wake of the Covid-19 pandemic as cybercriminals exploit people's fears and anxieties.

The rise in increasingly sophisticated and highly targeted 'spear-phishing' attacks was considered a major concern, especially given the fact that in some cases such attacks were able to circumvent state of the art security filters.

The participants expressed concerns about users unintentionally downloading malware from the internet and through phishing emails with attached images, audio and video files or links to other nefarious sites. Ransomware was highlighted as a particularly malicious form of malware. The rise of cryptocurrencies and their anonymous nature has fuelled a surge in ransomware attacks with a potential to hold an entire organisation hostage.

The increasing use of smart devices and social media was described by some participants as an emerging attack vector. Mobile devices such as laptops, smart phones and tablets pose serious security threats, in case of loss or theft, as sensitive data stored on such devices could fall into the hands of cybercriminals, exposing the organisation to further threats. It was noted that the rise of social media provides novel opportunities for cybercriminals to exploit these platforms to launch attacks against organisations.

The participants alluded to the rise in remote working as a potential attack vector since remote users are often outside the immediate control and influence of IT administrators. I also suggested that remote working assumes an even greater significance in the wake of COVID-19 pandemic for the reasons discussed in the literature review.

The participants' revelations and concerns about the rise in frequency and intensity of social engineering, phishing attacks, and malware attacks are corroborated by research and my own personal experience in the field.

The participants' responses highlighted the need to identify and understand the various personal and social factors that could contribute to human errors. The role of humans as the weakest link in InfoSec was recognised and echoed in the participants' responses. The participants also recognised that human errors often resulted from users not being aware of the security risks and the correct course of action they should take. Without a conscious recognition of the potential security risks, users are more likely to fall prey to various types of attacks. However, the blame for a user's lack of security awareness falls predominantly on the organisation rather than the user.

Some of the participants highlighted the importance of considering user habits and different user personalities as part of awareness training. Research in this area seems to confirm that how users interact with technology is very much influenced by their technology usage habits and this factor could be used as a basis to better understand user non-compliance with InfoSec policies. Research has also highlighted links between user personality and InfoSec compliance behaviour. A number of studies have shown that users with certain (positive) personality attributes are more likely to comply with InfoSec policies whilst those with certain (negative) personality attributes are more likely to violate security policies. Research seems to corroborate the point raised by the participants about the importance of considering the role of user habits and personality in the implementation of awareness programmes.

The role of 'opportunity' was considered to be crucial in terms of its effect on user behaviour. The more opportunities users are given to commit errors, the more likely they are to avail the opportunities. So, it was deemed necessary to minimise opportunities for user error as much as possible.

The participants raised the issue of job satisfaction and 'feeling of wellbeing' as a user attribute that has an effect on user behaviour. This point is corroborated by research suggesting that users that feel satisfied with their job are more likely to comply with the organisation's InfoSec policies. Perhaps somewhat related to the point about job satisfaction is the concern about an organisational security culture. Both the InfoSec academics and practitioners touched on this issue as an important social factor that could potentially contribute to human error. It was argued that when poor security behaviour is condoned or even worse, encouraged, then human error and security breaches become more commonplace. Conversely, a positive security culture helps to promote positive user security behaviour and a security conscious workforce.

The potential challenges associated with the rapid advances in technology were touched on by both InfoSec academics and practitioners. They referred to the 'disappearing network perimeter' and how the traditional demarcation between the home and the workplace had now been obfuscated. The convergence of technologies and changing user expectations was giving rise to serious security challenges in which users are more likely to engage in behaviour that is detrimental to the overall security of the organisation.

The human error element is quite evident in all of the various factors discussed above. An understanding of these factors by all stakeholders is important in order to appreciate how and what shortcomings can result from InfoSec awareness programmes. User training about the role of these factors forms an important part of an effective InfoSec awareness programme.

What are the factors that render an awareness programme ineffective?

In this section, the factors considered by the participants to contribute to the failure of awareness programmes are discussed.

The participants identified the internal political obstacles from management and users coupled with the lack of support and 'buy-in' from senior management as major factors for the failure of awareness programmes. Some participants also linked this to the disparity between priorities of senior management and InfoSec professionals. There was a perception that senior management were ultimately focused on revenue generation and InfoSec was treated with a 'tick-box' mentality that was just about meeting compliance requirements. The participants pointed out that one of the consequences of this approach to InfoSec is that organisations often delegated this important responsibility to managers who were not qualified to manage awareness programmes. This is also a reflection of the failure to recognise InfoSec awareness as a unique discipline.

The participants attributed the failure of awareness programmes to a lack of clear understanding of what InfoSec awareness actually is. The differences between security awareness and security training were not properly understood by management and the two are often used interchangeably, often resulting in incoherent policies.

The lack of appealing and engaging training materials was also identified as a factor in the failure of awareness programmes. The participants pointed out that cost was a major determining factor in the choice of training materials and management often favoured the cheapest option.

Some of the participants related that their awareness training was predominantly focused on social engineering and phishing attack simulations. It was pointed out that this approach to awareness training is flawed as it means that users remain ignorant of other important attack vectors and therefore potentially exposed to other threat types.

One of the participants highlighted that the security messages, the format, and frequency had to be carefully considered as 'over doing awareness' could lead to the undesirable consequence of users becoming disinterested and disengaged.

The lack of metrics to evaluate the effectiveness of InfoSec awareness programmes was identified as a key factor in the failure of awareness programmes to change user behaviour. The importance of metrics was also corroborated by research, and it was suggested that the results produced could serve as tangible proof to convince senior management about the importance of supporting the awareness programme.

An important factor identified by the participants as a potential contributor to the failure of a programme was the unrealistic expectations placed on the InfoSec awareness programme and regarding it as a panacea for all the security related problems. It was emphasised that the focus of security awareness is risk mitigation and not complete prevention.

Objective #2: Determine possible solutions to help make InfoSec awareness training programmes more effective (vis-à-vis human errors) based on engagement with InfoSec academics and practitioners.

The insights offered by the participants in relation to objective #2 span across multiple interpretive themes. As discussed under objective #1, the participants highlighted various factors that contribute to human errors, in turn leading to security breaches and ultimately the failure of an InfoSec awareness programme. This section discusses factors identified by the participants as being crucial to the success of an InfoSec awareness programme. As before, the guidelines are presented here in a condensed format and the reader is advised to refer to chapter 5 for details.

- **Awareness Training:** In general, all the participants reaffirmed the crucial role of awareness training in effecting a change in user behaviour in order to ensure security of an organisation. Conversely, a lack of security awareness and user carelessness were considered to be the main causes of human error and ultimately the failure of awareness programmes.
- **Relevant & Practical Material:** As essential components of an effective awareness programme, the participants stressed the importance of relevant materials tailored to the needs of the users and reinforced by real life examples that users can relate to. The training materials must be broken down into smaller digestible segments with clear and simple security messages. The use of excessive technical terms and jargon should be avoided to prevent user information overload. As part of the awareness training, participants raised the idea of providing practical tips and guidelines that could be taken away and immediately put into practice by users.
- **Regular Training:** An important recommendation that emerged was to avoid treating awareness training as a one-off event but rather to regard it as a process that must be repeated at regular intervals to ensure that security messages are retained, and security remains a high priority for all users.
- **Security Messages:** In terms of the methods used to convey security messages, the participants suggested the use of branded merchandise, screensavers, customised posters, visual aids, email reminders, web campaigns with tips and security advice adapted to specific business needs, as cost-effective options. The use of regular organisation-wide e-mail security messages, monthly newsletters, brown bag seminars, security awareness days and inviting external speakers were also recommended as helpful reminders of security awareness in the workplace.
- **User & Business Needs:** As a result of the discussions with the participants, it transpired that InfoSec awareness cannot be regarded as a ‘one-size-fits-all’ one-time annual solution for all situations. The way the training is structured, presented, and delivered must be carefully considered according to specific user and business needs in a way that will maximise its effectiveness in changing user behaviour and improving security for an organisation.
- **Delivery Mode:** The use of classroom-based (in person) training and online training were discussed as the two most effective modes of delivery for awareness training. Despite the many benefits offered by classroom-based training, it was suggested that it may not be suitable for all business environments due to staffing, cost, and logistical issues. The use of online training was considered to be the most practical mode of delivery due to its flexibility and the numerous benefits such as customisation and outsourcing options, ability to accommodate potentially unlimited number of users that can complete the training at their own pace and from anywhere. Online training

platforms can potentially minimise the time users spend away from their main jobs and are therefore more likely to be favoured by management. The preferences expressed by participants for online training is also consistent with trends in the InfoSec awareness training market. However, in practice, organisations are more likely to ‘mix and match’ between different modes of delivery according to their unique business environments and needs.

- **Metrics & Benchmarks:** The use of metrics and benchmarks to evaluate the effectiveness of programmes was emphasised as an important factor in the success of awareness programmes. The different types of metrics suggested include quizzes, questionnaires, and surveys to establish baselines and compare before and after training results to gauge improvement over time. InfoSec professionals can also monitor trends over time for the number and frequency of incidents to assess if the programme is meeting its objectives. The use of simulated phishing campaigns was identified as a popular and relevant metric due to the reported surge in phishing attacks across many business sectors. The tracking of user responses to phishing simulation drills was identified as an effective metric to measure improvements in user behaviour over time. For organisations lacking the internal resources and expertise, it was recommended that third party specialists could assist with the delivery and impact analysis of security awareness training.
- **Role-based User Access:** During the discussions (under objective #1) focussing on factors that contribute to the failure of awareness programmes, it was highlighted that generally, users commit errors because of the opportunities available to them. Consequently, it was deemed critical for organisations to reduce opportunities for users to commit errors. The use of role-based user access based on the principle of least privilege (POLP) was identified as being crucial to minimising opportunities for errors and organisational exposure to security risks.
- **User Perceptions & Attitudes:** One of the primary goals of InfoSec awareness training is to persuade users to change their behaviour. What emerged from the participants’ responses and subsequent discussions was that the act of persuasion goes beyond simply ‘informing’ and ‘training’ users. It is vitally important that users internalise the information and willingly act according to it. This requires an understanding of the users’ motivations and the thought processes behind their actions in order to bring about changes in user attitudes and behaviour. The discussion sought insights from related research in this area exploring psychological models of human behaviour. It was suggested that the concept of ‘language of persuasion’ as applied in media and commercial advertising could be used to influence user perceptions and attitudes towards awareness training.
- **Sources of Influence on Human Behaviour:** Psychological research also points to the crucial role played by the various sources of influence on human behaviour. The main sources of influence were identified as either conscious or unconscious. A cognitive model of human behaviour was suggested in which users consciously analyse and evaluate the information presented to them and consider the consequences of compliance and non-compliance in accordance with their own best interests. The role

of personal, social, and environmental factors was also considered to be crucial in influencing user behaviour. The participants' responses and subsequent discussions revealed very useful insights into human behavioural factors that InfoSec professionals can exploit in the design and delivery of InfoSec awareness programmes to bring about the desired change in user behaviour.

- **HCI-Sec Design:** The role of humans in security breaches is widely acknowledged in the InfoSec profession and research community. The participants also drew attention to the crucial role that poor technology design plays in facilitating and propagating human error. Research has shown that human errors can also be attributed to poor technology design that can inadvertently lead to security breaches. Poor technology design provides further opportunities for users to commit errors, as discussed earlier. It was suggested that the HCI elements of security must be considered carefully to bring about improvements in the security usability features in end user systems. Good HCI-Sec design is informed by an understanding of technology as well as human behaviour and should encourage users to perform the task correctly whilst protecting the system from errors.
- **Security Culture:** The consequences of a poor security culture and how it can be a major factor in the failure of an awareness programme was emphatically highlighted under objective #1. A strong security culture emphasises an organisation's core business values and sets the tone for how it expects all employees to think and behave as it relates to security matters. When an organisation values the importance of a strong security culture through awareness training, protective security measures and appropriately enforced policies, its employees are more likely to comply. A truly effective InfoSec awareness programme is not an afterthought or an 'add-on' but something that is an embedded part of organisational culture, conducted all year round and constantly adapting to the everchanging security threat landscape. It is not possible to develop a strong security focused culture without the support of senior management.
- **Management Buy-in:** The lack of management buy-in was identified as a major factor in the failure of awareness programmes. Senior management plays an important role in setting the foundations of a strong security culture through their statements and actions. Senior management buy-in at the highest organisational level is a major determining factor for the success of a programme. The participants emphasised the importance of senior figures acting as 'champions' for the awareness programme and leading their staff by example which inevitably influences the employees' behaviour in a positive way. Research shows a strong correlation between senior management's perception of InfoSec and how well InfoSec awareness initiatives are received by employees. Without the support of senior management and other stakeholders, there is likely to be passive resistance from employees. InfoSec professionals need to be able to achieve a consensus amongst major decision-makers about the importance of supporting and funding an awareness programme.

6.3 Evaluation of Project Outcomes and Relevance to Professional Practice

This project investigated the shortcomings in existing information security awareness training programmes and sought recommendations and solutions to address the shortcomings in order to reduce human errors. This project has proposed an alternative approach to InfoSec awareness training on the basis of a) literature survey of internationally peer-reviewed books, professional practice literature, journal papers, articles, policy documents and global security surveys b) engagement with InfoSec academics and practitioners.

In the previous section, I described the process by which each project objective was achieved. In particular the outcomes relating to objectives 1 and 2 were described in detail in the form of guidelines that encapsulate the shortcomings and the possible solutions to making InfoSec awareness programmes more effective in order to reduce human error.

This project addresses a very important problem within my field of practice. Security breaches resulting from human error can have potentially catastrophic consequences for organisations in the form of financial losses (loss of revenue, regulatory fines, mandatory compensation), loss of consumer confidence and damage to reputation. The role of awareness training in seeking to bring about better security through a positive change in user behaviour is well established. However, the effectiveness of awareness programmes in achieving this crucial goal is often called into question due to the factors discussed in chapter 2.

My unique approach to understanding this phenomenon and seeking an appropriate solution to the research problem employed interpretative phenomenological analysis (IPA) based on an interpretivist-constructivist research paradigm. InfoSec is considered an applied science that generally favours a positivist empiricist approach to research. My choice of research paradigm is uniquely crafted and can be considered an ‘alternative’ to the traditional ways of approaching the issue of awareness training and human error in my field of practice. I would argue that this alternative approach in itself is an important contribution to my field of practice.

I employed a phenomenological approach to conduct semi-structured interviews with two distinct groups of participants from within my professional community, namely InfoSec academics and practitioners. Although many previous InfoSec studies have employed qualitative research methodologies, the use of a ‘blended’ sample is not common. The fact that the two groups of participants approached the subject from their own unique perspectives, gave me the opportunity to gain a broader and deeper understanding of the issues.

In his seminal work, The Two Cultures and the Scientific Revolution (Snow, 2013), C.P. Snow discussed the strong dichotomy between the scientific culture and the culture of the humanities. Snow (2013) argued that the two cultures were drawing apart and their inhabitants were unable (or unwilling) to communicate their ideas beyond their own culture. Scientists didn’t read Jane Austen and humanists were unable to describe the second law of thermodynamics (McGinnis, 2018). Since the inhabitants of one culture lacked the knowledge and understanding of the other, a ‘mutual incomprehension’ hindered meaningful progress and the ability to find solutions to real world problems.

Snow (2013) also explored the idea of two distinct subcultures within the scientific community: namely pure vs applied sciences, whereby the former is concerned with theories and predictions whilst the latter is focused on the application of knowledge to solve real world problems.

There is no doubt that as our society becomes increasingly dependent on modern technology, there is a dire need to foster a stronger connection between these two subcultures (pure & applied) within the scientific community, for the benefit of the general public and humanity at large. This necessitates close cooperation between academic researchers and real-world practitioners from both camps to tackle real world socio-technical issues such as InfoSec awareness and human errors.

I mentioned earlier in this project report how during my undergraduate studies, I became disillusioned with my undergraduate degree programme due to what I perceived to be a disconnect between the abstract theories I was being taught and the real world (practice). This project gave me an opportunity to seek insights from both camps within my field of practice, by engaging InfoSec academics (pure scientists) and practitioners (applied scientists), in an effort to bridge the gap between the two subcultures (academic research and real-world practice). Snow (2013) aptly postulated the idea of a ‘third culture’ to narrow the self-imposed cultural divide.

Snow’s vivid distinction between scientific and humanistic knowledge could also be considered an antecedent to the modern-day debate between positivism and constructivism. My unique approach to this project employing an interpretivist-constructivist research paradigm to an applied science problem (that traditionally favours a positivist empiricist approach) is also an important part of the effort to narrow the cultural divide alluded to by Snow (2013).

Snow’s (2013) ideas about the great cultural divide in human intellectual activity were undoubtedly disruptive and ground-breaking for their time. However, I strongly believe that this gap has narrowed quite significantly in the recent decades. The cultural divisions so eloquently highlighted by Snow over 60 years ago, have ameliorated over time, owing to the natural evolution in both disciplines and the emergence of interdisciplinary scholarship and collaborative mindsets on both sides of the divide.

The concept of interdisciplinarity has gained much acceptance and has become firmly established within most scientific disciplines. This project is intrinsically transdisciplinary and testament to the above claim, as it draws on insights from InfoSec researchers, practitioners, computer scientists, communications engineers, psychologists, sociologists, and philosophers, among others, to understand and address the human factors in InfoSec.

My aim during this research was to understand the phenomenon from the participants’ perspective, tapping into their opinions, ideas and experiences in a way that helped to generate new theory and knowledge that will ultimately feedback into my own professional practice as well as benefitting my community of practice. I considered the participants as my co-researchers in this project and therefore my own personal and professional experience, technical knowledge and professional judgement was an indispensable part of this project. As an InfoSec practitioner-researcher, I am part of the same professional community as the research participants and my own experiential knowledge and beliefs constituted a vital part of this project. I was able to clarify the subjectivities that arose as a result of my own positionality, values, perspectives, understandings (and misunderstandings) that I brought into this research process. I considered myself to be working in collaboration with the participants in the process of co-creation of new knowledge and good professional practice in order to introduce change to my professional practice as well as my community of practice.

The outcome of this project in the form of guidelines will help to improve the processes and practices used to develop and implement effective InfoSec awareness programmes and can be incorporated into future awareness programmes to help reduce security breaches resulting from human errors.

The outcome of this project also offers important methodological and practical contributions for the design and implementation of effective InfoSec awareness training programmes. The guidelines offered here allow InfoSec professionals to carefully examine both the subjective and objective aspects of the implementation of effective awareness programmes. The practical implications that I have derived from the findings of this project revolve around four main areas:

a) An understanding of common user actions contributing to human errors
b) An understanding of the personal and social factors contributing to human errors
c) An understanding of the psychological perspectives of human behaviour in InfoSec
d) Combining all the above (a, b and c) areas to form an integrated understanding of the causes of human errors to design effective InfoSec awareness training programmes

The outcome of this project, in the form of guidelines, will ultimately inform my professional practice. I will be able to draw on my experience of conducting this research and the guidelines that have emerged, to enhance my current role as a consultant trainer. I have previously worked as a technical author, designing bespoke InfoSec courseware (refer to Appendix J) based on predominantly proprietary standards and technologies. The guidelines derived from the findings of this project will help me to design, market and deliver InfoSec courses rooted in real world research. This will undoubtedly raise my professional profile and enhance my future career prospects.

Based on my experience of the research journey and the subsequent findings, I intend to publish a number of papers and short articles in InfoSec and professional practice journals (refer to Appendix I for previous publications), planned for later part of the year. This will give me the opportunity to get my research out to the wider InfoSec community.

I also feel strongly that there is a need for a ‘guidebook’ to be published, informed by the findings of this research, to assist InfoSec professionals with practical guidelines to enhance their awareness programmes.

I had the opportunity to present this research at the Research Students' Summer Conference (RSSC2021) where it was very well received. I plan to share my findings at more such events, including the upcoming RSSC2022. I also have plans to present my work to critical communities of InfoSec professionals where I hope to find opportunities for further research and collaborative projects within my specialist area of interest.

The input from InfoSec academics was crucial to the success of his project. I feel that InfoSec academics, especially those engaged in teaching and mentoring activities have an important role to play in promoting InfoSec awareness. I have identified at least three universities in the UK currently offering undergraduate programmes in cybersecurity. Not surprisingly, a quick evaluation of these programmes revealed a predominantly technology-focused approach to security with very scant coverage of the important role of awareness training and the human factors. I feel that the project findings have an important contribution to make in the area of InfoSec curriculum enhancement. I am currently seeking opportunities to disseminate this message through lectures, seminars and other open day events organised at my former universities.

The outcome of this project will benefit the various stakeholders of this project. InfoSec academics and practitioners are obvious beneficiaries of this research, and the guidelines will be shared with them in a summarised format. The guidelines will be disseminated to my wider community of practice in the form of a whitepaper in order to highlight and promote the main features of the findings. It is likely that certain aspects of the findings will reverberate with certain stakeholders more than others. For example, the importance of a strong organisational security culture and the importance of senior management support as major factors in the success of an awareness programme are themes that are certain to find resonance with organisational leaders, managers, chief information officers and chief information security officers. These findings will enable senior management to elevate their leadership and governance relationship in order to benefit the organisation as a whole.

The guidelines relating to the use of weak passwords, careless handling of sensitive data, social engineering, spear-phishing attacks, the use of smart devices and social media, user habits and personalities all offer valuable insights for systems administrators and end users in a way that will help them to improve the processes and practices related to InfoSec within the workplace. For end users, an improved awareness within the workplace will also contribute to improved InfoSec practices at home, protecting other family members and the wider community.

Practitioner research has the potential to help all the stakeholders make positive contributions to our common professional practice. Research provides opportunities to enhance InfoSec professional practice by keeping it engaging and up to date. The insights and experiences shared by colleagues engaged in research and management of other awareness programmes is undoubtedly a valuable contribution to professional practice. The process of consulting colleagues and professional peers as part of the research serves an important stakeholder management purpose by keeping them on board and gaining their support in delivering the programme or making enhancements to an existing one. The dissemination of research findings will also help InfoSec professionals and other stakeholders to draw upon the good practices identified in this project to enhance their own professional practice.

6.4 Limitations and Future Research

As with any research undertaking, there are several limitations to this project. One of the main limitations stems from the methodological approach employed for this research. Phenomenology as a methodology is focused on the lived experiences of participants in relation to a particular phenomenon. This by its very nature necessitates a selective sample. The use of purposive sampling to select a sample based on specific criteria introduces the potential for sampling bias. However, as explained in chapter 3, this approach was necessary to answer the particular research question of this project.

The sample size for this study was limited to 8 participants and I put in place a number of measures to ensure that all of their experiences were broadly similar. This sample size may not be representative of the experiences of a larger population of InfoSec professionals. The experiences of the research participants represent a very specific area of InfoSec (awareness programmes and human error) and cannot be generalised to other areas of InfoSec or other industries for that matter. Additionally, all of the participants in this research were male and therefore their experiences are unlikely to be representative of female InfoSec professionals in this field.

This research is also limited due to the lack of generalisability of the findings. It was explained in chapter 3 that IPA studies do not normally claim to be generalisable. Given the unique sample and the specific research problem of this project, it would not be possible to make inferences about other similar contexts and phenomena.

InfoSec practitioners were interviewed to share their experiences about the implementation of InfoSec awareness programmes within their organisations. However, not all of these InfoSec practitioners had been in their current roles for the complete life cycle of the awareness programmes, especially from the early stages of design and implementation. Consequently, their experiences and insights about their organisation's awareness programme do not necessarily provide a complete perspective. The InfoSec professionals that preceded them in their current roles would be able to shed more light on this but it was not possible to get their input.

The main focus of this project was on SME organisations with fewer than 250 employees. Other factors such as the annual turnover and the management structure were not considered in this research, and it is possible that these factors could have an impact on the findings. In larger organisations, there is normally multiple levels of management and leadership above the InfoSec professionals that participated in this research. This could have a bearing on budgets and support for the programme. Future research could consider different sized organisations to determine if the size of an organisation has an impact on the effectiveness of InfoSec awareness programmes and the InfoSec professional who implement them.

All of the participants in this research lived and worked in the UK. This was necessary for the particular research design in order to obtain the depth and breadth of participants' experiences. However, their experiences are not necessarily representative of InfoSec professionals from other parts of world, as differences in social and business cultures could have an impact on how people perceive and interpret their experiences and the world around them. As a recommendation for future research, the scope of this project could be extended to other European countries and North America. There is also a case for considering different cultural contexts and characteristics as it relates to InfoSec awareness and future work could consider evaluation of several different InfoSec awareness programmes from around the world.

In this project, the role of InfoSec awareness programmes and human errors was investigated only from the perspective of InfoSec academics and practitioners. It is possible that InfoSec professionals in other roles within organisations have different experiences and can therefore offer their unique perspectives on the issues. In order to gain a better understanding of the issues and to find a more comprehensive solution to the research problem, future research could also consider the perspectives of end users and senior managers in the organisation.

One of the main limitations of conducting InfoSec research at an organisational level is the perceived intrusiveness of the research topic. Many of the professionals contacted about this research project simply declined to participate due to confidentiality concerns. Some of the professionals explained that they did not feel comfortable discussing potentially sensitive security related situations whilst some others explained that they were explicitly prohibited by their organisations to partake in any security related research initiatives. It is also possible that some of the professionals who did not respond to my initial invitations, did so for the same reasons. This is a well-known issue in the field of InfoSec research and many previous studies have highlighted similar challenges.

I believe that the benefits of collaboration and sharing information on important security related issues, such as awareness training, far outweigh some of the concerns expressed by security professionals. Ultimately, the insights gained, and the lessons learnt through cooperation as a community feed back into our shared professional practice and this project is a testament to that.

6.5 Final Reflections

The DProf programme provided me with the opportunity to consolidate and further enhance my understanding and expertise in the area of organisational InfoSec awareness training and human behaviour. The role of human factors in InfoSec has been a recurring theme in my professional practice over the years and it was area of research that I was particularly keen to explore and develop further.

I considered my own personal and professional experience, technical knowledge, and research background as a crucial part of my DProf research. I feel privileged to have had the opportunity to complete this project by drawing on my professional knowledge, experience, and insights to make a valuable contribution to an important area of InfoSec research and my professional practice.

From an ontological and epistemological perspective, my past professional practice had been rooted in a predominantly positivistic research paradigm, trying to understand various phenomena through mainly quantitative approaches. In carrying out this project, there has been a complete paradigm shift in my approach to research, resulting in a research methodology that was crafted on the principles of a constructivist-interpretivist research philosophy.

The overall journey has been a steep learning curve for me and a tremendous experience that I have thoroughly enjoyed. The opportunity to discuss and collaborate on issues of mutual concern with my professional peers to generate new insights and knowledge, that is beneficial for our community of practice, was a thoroughly rewarding experience for me.

The purpose of this project was not to test any existing concepts or theories in the field of InfoSec. Using a phenomenological approach as the basis of the research facilitated the participants' experiences to be expressed on their own terms rather than according to some predefined criteria. This required me to be empathetic and willing to enter into their unique worlds. As I conducted the interviews and analysed the participants' responses, I began to really appreciate their struggles and some of the political obstacles they faced from within. I felt quite inspired by their professionalism and the dedication shown towards their profession.

I sought to understand the meaning of the research participants' experiences and how they constructed their worldview in order to generate fresh theory and perspectives that would be valuable and applicable to my professional practice and my community of practice. The process of data analysis and interpretation arrived at theory that helps to answer the research question and consequently explains the phenomenon of interest.

The research process helped me to adopt a reflexive attitude to assess my personal values, motivations, beliefs, and expectations, specifically in the selection of an appropriate research methodology and in pursuit of a DProf more generally. As a practitioner-researcher, the issue of subjectivity was always at the forefront of my mind. As an InfoSec professional with experience in the same field as the research participants, I remained acutely conscious that my position could be a threat to the validity and objectivity of the data being collected. Costley and Armsby (2007) point out that the practitioner-researcher's subjectivity inevitably plays a prominent part in practice-based research. They argue that contextual knowledge is connected to subjectivity. After all, it is part of what made the research relevant and authentic.

Although it was impossible to eliminate the role of subjectivity completely, I continuously sought feedback from my academic advisor, consultant, and professional colleagues and critical friends to minimise its impact on the research. I diligently focused my attention on the input offered by the participants and consciously blocked out any preconceptions about my personal vision or desires for the project outcome. I also made sure to remind and emphasise to the participants that my role was that of a researcher and not as someone in the same professional capacity as them.

I learnt the importance of perseverance, being flexible and open-minded to new ideas and different approaches to problem solving. There were times when I felt completely overwhelmed, confused, and frustrated with the whole process. I found the process of data analysis to be particularly laborious and mentally and emotionally draining. I was very fortunate to have the support of my academic advisor, consultant, professional colleagues, and critical friends throughout the process.

This project challenged my cognitive abilities and my capacity to learn new skills. I found myself constantly reading, cross referencing information, considering alternative approaches, developing, and refining my ideas and theories. I further developed and enhanced my critical thinking skills and the ability to learn through deliberate reflection on my actions and past experiences.

This project has stretched the frontiers of my knowledge and experience and has tremendously helped in developing me intellectually and improving my analytical skills and divergent thinking. I have further enhanced my ability to analyse and synthesise complex and sometimes conflicting ideas to redefine knowledge and develop new theories. I have improved my ability to work independently and effectively, making use of additional support and resources to manage my own learning.

The process of conducting this research gave me an opportunity to improve my scholarly abilities and skills both academically and professionally by formulating solutions through dialogue and collaboration with supervisors, advisors, mentors, professional peers, research participants, and stakeholders. I have developed a much better awareness and understanding of ethical dilemmas and conflicting values that arise in professional practice and when dealing with research participants in the context of practitioner research.

I have been able to demonstrate effective and critical selection and development of an appropriate practice-based research methodology to achieve the objectives of this project. I was particularly intrigued by the mixing and matching of research theories, approaches and methods with my own personal values, motivations, goals, and professional experience to establish my own unique philosophical stance that I was able to reflect in the crafted research design of this project.

I am pleased with the way this research has evolved and how I have been able to put together a project that has resulted in practical and tangible outcomes for my own professional practice and for my community of practice. As this project comes to an end, I begin another exciting journey of seeking new challenges and forging new paths within my field of practice. I believe that the rigorous and challenging process of undertaking this DProf has given me a competitive edge and has greatly enhanced my professional profile and future career prospects. It has given me the opportunity to further develop myself and play a strategic thought leadership role in my chosen area of InfoSec research and practice.

Summary

This chapter presented the findings from the previous chapter according to each project objective in order to demonstrate how each objective had been achieved. The findings were presented in the form of guidelines intended to help improve the processes and practices used to develop and implement effective InfoSec awareness programmes.

This chapter also discussed the value of this project and the applicability of its outcome to my field of practice and the stakeholders. The limitations of this project and recommendations for further research were discussed. I concluded this chapter by reflecting on the overall project journey.

References

Alase, A. (2017). The Interpretative Phenomenological Analysis (IPA): A Guide to a Good Qualitative Research Approach. *International Journal of Education and Literacy Studies*.

Allison, P. and Pomeroy, E. (2000). How shall we 'know'? Epistemological concerns in research in experiential education. *Journal of Experiential Education*. 23 (2), 91–98.

Alomari, A., Elgayar, O. and Deokar, A., (2012) 'Security policy compliance: user acceptance perspective', *IEEE 45th Hawaii International Conference on System Sciences*, pp. 3317-3326.

Alotaibi, M., Furnell, S. and Clarke, N. (2016). Information security policies: A review of challenges and influencing factors. *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*, 352-358.

Amundsen, D., Msoroka, M., and Findsen, B. (2017). "It's a case of access." The problematics of accessing research participants. *Waikato Journal of Education*. 22 (4), 5-17.

Archibald, M. M., Ambagtsheer, R. C., Casey, M. G. and Lawless, M. (2019). Using zoom videoconferencing for qualitative data collection: Perceptions and experiences of researchers and participants. *International Journal of Qualitative Methods*. 18, 1-8.

Arksey, H., and Knight, P. (1999) *Interviewing for social scientists*, London: Sage

Arkvik, I. (2021). *What is an IT Security Policy?*. Available: https://www.visma.com/blog/what-is-an-it-security-policy-2 Last accessed 19th July 2021.

Bada, M., Sasse, A. and Nurse, J., 2019. *Cyber Security Awareness Campaigns: Why do they fail to change behaviour?*. [online] Available: https://arxiv.org/abs/1901.02672 Last accessed 18 January 2021.

Bada, M and Sasse, A. (2014). *Cyber Security Awareness Campaigns - Why do they fail to change behaviour?*. Available: https://discovery.ucl.ac.uk/id/eprint/1468954/1/Awareness%20CampaignsDraftWorkingPaper.pdf Last accessed 19th June 2020.

Bailey, C.A. (1996) *A guide to field research*, Thousand Oaks, CA: Pine Forge.

Bannister, A. (2020). *Remote working during coronavirus pandemic leads to rise in cyber-attacks.* Available: https://portswigger.net/daily-swig/remote-working-during-coronavirus-pandemic-leads-to-rise-in-cyber-attacks-say-security-professionals Last accessed 5th September 2020.

Bazeley, P (2007). *Qualitative Data Analysis with NVivo*. London: Sage Publications

BBC Business. (2018). *Australian worker overpaid by A$500,000.* Available: https://www.bbc.com/news/business-45327148 Last accessed 9th July 2021.

BEQOM. (2021). *In Compensation Management, Simple Human Error Can Cost Your Business Millions.* Available: https://www.beqom.com/blog/simple-human-error-can-cost-your-business-millions Last accessed 20th October 2021

Berger, J. G. (2004), “Dancing on the threshold of meaning : recognising and understanding the growing edge”, Journal of Transformative Education (2), p.336.

Berkowitz, B. (2000). *Using Principles of Persuasion.* Available: https://ctb.ku.edu/en/table-of-contents/participation/promoting-interest/principles-of-persuasion/main Last accessed 15th May 2021.

Bird, K. (2013). *New Version Of ISO/IEC 27001 To Better Tackle It Security Risks.* Available: https://www.iso.org/news/2013/08/Ref1767.html Last accessed 3rd September 2019.

Bogdan, R. C. and Biklen, S. K (2006). *Qualitative research in education: An introduction to theory and methods.* Allyn & Bacon

Boyd, C.O. (2001) ‘Phenomenology, the method’ in P.L. Munhall (eds), pp.93 - 122 *Nursing research: A qualitative perspective,* Sudbury, MA: Jones and Bartlett. Third Edition.

Brodie, C., 2008. *The Importance of Security Awareness Training*. [online] SANS Institute. Available: https://sansorg.egnyte.com/dl/w0S3vzcqqD Last accessed 13 August 2020.

Byrd, P. (2021). *13 Important Security Awareness Training Topics for 2021.* Available: https://hooksecurity.co/blog/13-important-security-awareness-training-topics-for-2021 Last accessed 15th November 2021.

Cano, J., 2019. *The Human Factor in Information Security*. [online] ISACA. Available: https://www.isaca.org/resources/isaca-journal/issues/2019/volume-5/the-human-factor-in-information-security Last accessed 8 May 2021.

Cialdini, R (2009). *Influence: Science and Practice*. 5th ed. London: Harper Business. 2-3.

CISA. (2020). *Defining Insider Threats.* Available: https://www.cisa.gov/defining-insider-threats Last accessed 2nd October 2021.

CISA. (2019). *Security Tip (ST04-001).* Available: https://us-cert.cisa.gov/ncas/tips/ST04-001 Last accessed 16th July 2021.

Cisco, 2021. *Cisco Secure Outcomes Study Report 2021*. [online] Cisco. Available: https://www.cisco.com/c/en/us/products/security/security-outcomes-study.html Last accessed 12 July 2021.

Coffey, A and Atkinson, P. (1996). *Making Sense of Qualitative Data*. Thousand Oaks, CA: Sage

Cohen, L., Manion, L. and Morrison, K. (2007). *Research methods in education* . 6th ed. New York, NY: Routledge.

Coker, J. (2021). *Reported HMRC-branded phishing scams grew by 87% during COVID-19.* Available: https://www.infosecurity-magazine.com/news/hmrc-phishing-scams-grew-covid/ Last accessed 3rd October 2021.

Colaizzi, P.F. (1978). Psychological Research as the Phenomenologist Views It. In: Valle, R.S. and Mark, K *Existential Phenomenological Alternatives for Psychology*. New York: Oxford University Press. 48-71.

Colwill, C. (2009). Human factors in information security: The insider threat-Who can you trust these days?. *Information Security Technical Report* . 14 (4), 186-196.

Cooper, R. (2009). Online interviewing: It's not as simple as point and click. *The Qualitative Report*. 14 (4), 250-253.

Cosgrove, A. (2021). *Why Employee Cyber-Awareness is Critical Every Day, Not Just During a Crisis.* Available: https://www.infosecurity-magazine.com/blogs/employee-cyber-awareness-crisis Last accessed 5th September 2021.

Costley, C. and Armsby, P. (2007) 'Research influences on a professional doctorate', *Research in Post-compulsory Education*, 12, 3, pp.343–55.

Coventry, L., Briggs, P., Blythe, J. and Tran, M. (2014). *Using behavioural insights to improve the public's use of cyber security best practices.* Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/309652/14-835-cyber-security-behavioural-insights.pdf Last accessed 16th July 2021.

Creswell, J. W. (2013). *Qualitative Inquiry and research design choosing among five approaches* . 3rd ed. Thousand Oaks, CA: Sage

Creswell, J.W. (1998). *Qualitative inquiry and research design: choosing among five traditions*. Thousand Oaks, CA: Sage

Crotty, M (1998). *The Foundations of Social Research: Meaning and Perspective in the Research Process*. Crows Nest, Australia: Allen & Unwin.

CrowdStrike, 2021. *2021 CrowdStrike Global Threat Report*. [online] CrowdStrike. Available: https://go.crowdstrike.com/crowdstrike-global-threat-report-2021 Last accessed 18 June 2021.

Curtis, S. (2014). *Government scheme shows who can be trusted on cybersecurity.* Available: https://www.telegraph.co.uk/technology/internet-security/10877217/Government-scheme-shows-who-can-be-trusted-on-cyber-security.html Last accessed 17th June 2020.

CybeReady. (2020). *The State of Security Awareness Training.* Available: https://cybeready.com/wp-content/uploads/The-State-Of-Security-Awareness-Training-v2.pdf Last accessed 3rd May 2021.

CybSafe. 2021. *7 reasons why security awareness training is important | CybSafe*. [online] Available: https://www.cybsafe.com/community/blog/7-reasons-why-security-awareness-training-is-important Last accessed 5 February 2021.

D'Arcy, J., Hovav, A. and Galletta, D. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research.* 20 (1), 70-98.

Dahlberg, K., Dahlberg, H. and Nystrom, M (2008). *Reflective Lifeworld Research*. 2nd ed. Lund, Sweden: Studentlitteratur. 1.

DCMS. (2021). *Cyber Security Breaches Survey 2021.* Available: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021 Last accessed 10th September 2021.

Deakin, H. and Wakefield, K. (2014). Skype interviewing: Reflections of two PhD researchers. *Qualitative Research*. 14 (5), 603–616.

Deloitte, 2020. *2020 Deloitte Cyber Survey*. [online] www2.deloitte.com. Available: https://www2.deloitte.com/content/dam/Deloitte/dk/Documents/Cyber/cyberreport/Cyber_survey_.pdf Last accessed 16 October 2020.

Dolan, P., Hallsworth, M., Halpern, D., King, K. and Vlaev, I. (2010). *Mindspace: Influencing behaviour through public policy.* Available: https://www.instituteforgovernment.org.uk/sites/default/files/publications/mindspace.pdf Last accessed 17th June 2020.

Dube, L. And Pare, E. (2003) 'Rigor in information systems positivist case research: Current practices, trends and recommendations', *MIS Quarterly*, 27, No. 4, pp. 597–635.

Easterby-Smith, M. Thorpe, R. And Lowe, A. (2002) *Management research: An introduction* London: Sage. Second Edition.

Easton, K. L. McComish, J. F. and Greenberg, R. (2000) 'Avoid common pitfalls in qualitative data collection and transcription', *Qualitative Health Research*, 10, pp.703-708.

Edkins, G. (2021). *Human Factors, Human Error & The Role of Bad Luck in Incident Investigations.* Available: https://www.safetywise.com/single-post/2016/08/30/human-factors-human-error-the-role-of-bad-luck-in-incident-investigations Last accessed 8th September 2021.

Ekran System. (2019). *How to Prevent Human Error: Top 4 Employee Cybersecurity Mistakes.* Available: https://www.ekransystem.com/en/blog/how-prevent-human-error-top-5-employee-cyber-security-mistakes Last accessed 13th June 2020.

Ellis, P (2016). *Understanding Research for Nursing Students*. 3rd ed. London: Sage

ENISA. (2010) 'How to raise information security awareness', *European Network and Information Security Agency.*

Enrici, I., Ancilli, M. and Lioy, A. (2010) 'A psychological approach to information technology security', *IEEE Conference Rzeszow, Poland, May 13-15 2010*, pp. 459-466.

Erlandson, D. A. Harris, E. L. Skipper, B. L. and Allen, S. D. (1993) *Doing naturalistic inquiry: a guide to methods*, London: Sage.

Ernest & Young. (2020). *EY Global Information Security Survey 2020.* Available: https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/advisory/ey-global-information-security-survey-2020-report.pdf Last accessed 18th October 2020

Fasulo, B. (2020). *The Difference Between Cybersecurity and Information Security.* Available: https://securityscorecard.com/blog/information-security-versus-cybersecurity Last accessed 3rd September 2020

FAU. (2016). *One in two users click on links from unknown senders.* Available: https://www.fau.eu/2016/08/25/news/research/one-in-two-users-click-on-links-from-unknown-senders Last accessed 3rd August 2020.

Faulkner, L.L., Kritzstein, P. B. and Zimmerman, J. J. (2011) 'Security infrastructure for commercial and military ports', *MTS Battelle Memorial Institute, Columbus, Ohio, USA*.

Ferbrache, D. (2020). *The rise of ransomware during COVID-19.* Available: https://home.kpmg/xx/en/home/insights/2020/05/rise-of-ransomware-during-covid-19.html Last accessed 5th August 2021.

Fogg, J. (2002). Persuasive technology: using computers to change what we think and do. *Ubiquity*. 2002 (5)

Fruhlinger, J. (2018). *What is WannaCry ransomware, how does it infect, and who was responsible?.* Available: https://www.csoonline.com/article/3227906/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html Last accessed 18th July 2021.

Furnell, S and Thomson, K. (2009). From culture to disobedience: Recognizing the varying user acceptance of IT security. *Computer Fraud & Security*. 2009 (2), 5-10.

G2. (2020). *Best Security Awareness Training Software.* Available: https://www.g2.com/categories/security-awareness-training Last accessed 15th August 2021.

Gardner, B. and Thomas, V., 2014. *Building an information security awareness program: defending against social engineering and technical threats*. 1st ed. Syngress.

GDPR. (2018). *What is GDPR, the EU's new data protection law?.* Available: https://gdpr.eu/what-is-gdpr/ Last accessed 20th September 2021.

General Data Protection Regulation (GDPR). 2018. *Art. 39 GDPR – Tasks of the data protection officer - General Data Protection Regulation (GDPR)*. [online] Available: https://gdpr-info.eu/art-39-gdpr Last accessed 7 September 2021.

Georgescu, E.. (2021). *Human Error in Cybersecurity.* Available: https://cybersecuritymagazine.com/human-error-in-cybersecurity/ Last accessed 15th September 2021.

Giorgi, A. (1985) *Phenomenology and psychological research*, Pittsburgh, PA: Duquesne University Press.

Gordon, L.A. Loeb, M.P. and Zhou, L. (2020). Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model. *Journal of Cybersecurity*. 6 (1).

GOV.UK. (2020). *Business population estimates for the UK and regions: 2019.* Available: https://www.gov.uk/government/statistics/business-population-estimates-2019/business-population-estimates-for-the-uk-and-regions-2019-statistical-release-html Last accessed 20th November 2021

Gray, D.E. (2009). *Doing Research in the Real World*. 2nd ed. Thousand Oaks, California: Sage Publications.

Groenewald, T. (2004) 'Phenomenological research design illustrated', *International Journal of Qualitative Methods,* 3, No. 1, pp. 1–26.

Guba, E. and Lincoln, Y. (2005) 'Paradigmatic controversies, contradictions, and emerging confluences' in N. Denzin and Y. Lincoln (eds), *The Sage handbook of qualitative research*, London: SAGE.

Guba, E. (1981) 'Criteria for assessing the trustworthiness of naturalistic inquiries', *Educational Communication and Technology Journal*, 29 (1981), pp.75–91.

Hanna, M. (2020). 'Exploring Cybersecurity Awareness and Training Strategies To Protect Information Systems and Data'. Doctoral thesis, Walden University, Minneapolis. Available: https://scholarworks.waldenu.edu/dissertations/8902/

Hansen, F. D. (2006). Human Error: A Concept Analysis. *Journal of Air Transportation*. 11 (3), 88

Haydon, G., Browne, G., and Van der Riet, P. (2018). Narrative inquiry as a research methodology exploring person centered care in nursing. *Collegian*. 25 (1), 125-129.

Herold, R. (2005) *Managing an information security and privacy awareness training programme*. Auerbach Publications.

Holliday, A. (2002) *Doing and writing qualitative research*, London: Sage

HSE. (2015). *Human factors: Managing human failures.* Available: https://www.hse.gov.uk/humanfactors/topics/humanfail.htm Last accessed 19th June 2020.

Hughes-Lartey, K., Li, M., Botchey, F. and Qin, Z., 2021. *Human factor, a critical weak point in the information security of an organization's Internet of things*. [online] ScienceDirect. Available: https://www.sciencedirect.com/science/article/pii/S2405844021006253 Last accessed 11 June 2021.

Hycner, R. H. (1999) 'Some guidelines for the phenomenological analysis of interview data' in A. Bryman & R. G. Burgess (eds) *Qualitative research* (Vol. 3, pp. 143-164). London: Sage.

IBM Security. (2021). *Cost of a Data Breach Report 2021.* Available: https://www.ibm.com/downloads/cas/OJDVQGRY Last accessed 10th October 2021.

IBM Security. (2019). *Cost of a Data Breach Report 2019.* Available: https://www.ibm.com/downloads/cas/RDEQK07R Last accessed 23rd June 2020.

Imam, F. (2020). *Top 10 security awareness training topics for your employees.* Available: https://resources.infosecinstitute.com/topic/top-10-security-awareness-training-topics-for-your-employees Last accessed 15th September 2021.

InfoSec. (2021). *IT Security Standards and Best Practices.* Available: https://www.infosec.gov.hk/en/useful-resources/it-security-standards-and-best-practices Last accessed 12th September 2021.

ISACA, 2019. *State of Cybersecurity 2019*, *Part 2: Current Trends in Attacks, Awareness and Governance* [online] www.isaca.com Available: https://www.isaca.org/go/state-of-cybersecurity-2020 Last accessed 21 September 2020.

ISO. (2021). *ISO/IEC 27032:2012 - Guidelines for cybersecurity.* Available: https://www.iso27001security.com/html/27032.html Last accessed 15th June 2020.

ISO/IEC JTC 1. (2013). *Information security, cybersecurity and privacy protection.* Available: https://www.iso.org/committee/45306/x/catalogue/ Last accessed 5th September 2020.

ISO/IEC. 2013. *ISO/IEC 27001:2013*. [online] Available: https://www.iso.org/standard/54534.html Last accessed 13 June 2021.

Janesick, V.J. (1994) 'The dance of qualitative research design' in N.K. Denson and Y.S. Lincoln (eds), *Handbook of qualitative research,* Thousand Oaks, CA: Sage.

Jonathan, A. S. (2004). Reflecting on the development of interpretative phenomenological analysis and its contribution to qualitative research in psychology. *Qualitative Research in Psychology*. 1 (1), 39-54.

Jones, M. (2005). *Introduction to HCI.* Available: https://www.cs.bham.ac.uk/~rxb/Teaching/HCI%20II/intro.html Last accessed 19th June 2020.

Kaspersky. (2018). *The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within.* Available: https://www.kaspersky.com/blog/the-human-factor-in-it-security/ Last accessed 3rd June 2020.

Kaspersky. (2021). *What is a security breach?.* Available: https://me-en.kaspersky.com/resource-center/threats/what-is-a-security-breach Last accessed 15th September 2021.

Kelion, L. (2020). *Excel: Why using Microsoft's tool caused Covid-19 results to be lost.* Available: https://www.bbc.com/news/technology-54423988 Last accessed 19th July 2021.

Kemmis, S. (2010) 'What is professional practice? Recognizing and respecting diversity in understandings of practice', [online] Available: https://www.researchgate.net/publication/226410200_What_Is_Professional_Practice_Recognising_and_Respecting_Diversity_in_Understandings_of_Practice Last accessed 5th June 2021.

Khidzir, Z. N., Mohamed, A. and Arshad, H. N. (2010) 'Information security factors: critical threats and vulnerabilities in ICT outsourcing', *IEEE Conference*, pp. 194-199.

King, C. (2010). *Insider Threat Deep Dive: IT Sabotage.* Available: https://insights.sei.cmu.edu/blog/insider-threat-deep-dive-it-sabotage/ Last accessed 17th June 2020.

Kissel, R. (2013). *Glossary of Key Information Security Terms* . Available: https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf Last accessed 3rd September 2020.

Klahr, R., Shah, J., Sheriffs, P., Rossington, T., Pestell, G., Button, M. and Wang, V. (2017). *Cyber security breaches survey 2017.* Available: https://researchportal.port.ac.uk/en/publications/cyber-security-breaches-survey-2017-main-report Last accessed 20th June 2020.

Kotulic, A. G. and Clark, J. G. (2004) 'Why there aren't more information security research studies', *Information & Management*, 41(5), pp. 597-607.

Kowalski, E., Cappelli, D. and Moore, A. (2008). *Insider Threat Study: Illicit Cyber Activity in the Information Technology and Telecommunications Sector.* Available: https://apps.dtic.mil/sti/citations/ADA638653 Last accessed 17th May 2020.

Ktoridou, D. and Dionysiou, I. (2011) ‘Case-based learning: an instructional model to incorporate information security topics in multidisciplinary courses at the University of Nicosia’, *IEEE Global Engineering Education Conference*, pp. 466-469.

Legárd, I., 2020. *Building an effective information security awareness program*. [online] Central and Eastern European EDem and EGov Days 338 (July):189-200. Available: https://doi.org/10.24989/ocg.338.15. Last accessed 8 February 2021.

Lester, S. (1999) ‘An introduction to phenomenological research’, Stan Lester Developments. Available from: https://www.researchgate.net/publication/255647619_An_introduction_to_phenomenological_research Last accessed 20th December 2020.

Liginlal, D., Sim, I., & Khansa, L. (2009). How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. *Computers & Security*, 28(3–4), 215–228.

Lin, C. S. (2013). Revealing the “Essence” of Things: Using Phenomenology in LIS Research. *Qualitative and Quantitative Methods in Libraries* . 4, 469 –478.

Lincoln, Y.S. and Guba, E. G. (1985) *Naturalistic inquiry*, Beverly Hills, CA: Sage.

Linda Findlay (2009) “Debating phenomenological research methods”, Phenomenology and Practice, Vol 3 (1) pp.6-25.

Lofland, J. and Lofland, L. H. (1999) ‘Data logging in observation: Fieldnotes’ in A. Bryman and R. G. Burgess (eds.) *Qualitative research*. Vol. 3. London: Sage.

Lowrey, T and Shrum, L. (2019). *Understanding the Language of Persuasion.* Available: https://www.hec.edu/en/knowledge/articles/understanding-language-persuasion Last accessed 9th March 2021.

Marshall, C. and Rossman, G. B. (1999) *Designing qualitative research*, Newbury Park: Sage. Third Edition

Martinuzzi, E. (2020). *Citi's $900 million loan error is still perplexing.* Available: https://www.bloomberg.com/opinion/articles/2020-08-25/citigroup-s-900-million-revlon-loan-error-is-still-perplexing Last accessed 16th October 2021.

McBride, M., Carter, L. and Warkentin, M. (2012). *The Role of Situational Factors and Personality on Cybersecurity Policy Violation.* Available: https://1library.net/document/z13wwe3q-role-situational-factors-personality-cybersecurity-policy-violation.html Last accessed 17th June 2020.

McCoyd, J. L. M. and Kerson, T. S. (2006). Conducting intensive interviews using email: A serendipitous comparative opportunity. *Qualitative Social Work*. 5 (3), 389–406.

McGinnis, J. (2018). *Bridging C. P. Snow's Two Cultures - Why science needs the humanities, and vice versa.* Available: https://www.city-journal.org/html/bridging-c-p-snows-two-cultures-15837.html Last accessed 1st May 2022.

McIlwraith, A. (2006) *Information security and employee behaviour: How to reduce risk through employee education, training and awareness*. Gower Publishing

Merleau-Ponty, M. (2012). *Phenomenology of Perception*. Translated by Donald Landes, France: Routledge, 2nd ed.

Merriam, S. B. (1998) *Qualitative research and case study applications in education*, San Francisco: Jossey-Bass.

Moore, J. (2020). *Why Cyber Essentials should be the first key step on your cyber security journey.* Available: https://www.ifsecglobal.com/critical-conversations/why-cyber-essentials-should-be-the-first-key-step-on-your-cyber-security-journey/ Last accessed 18th July 2021.

Moser, A. and Korstjens, I. (2017). Practical guidance to qualitative research. *European Journal of General Practice*. 23 (1), 271-273.

Moss, H. (2019). *Achieving Successful Outcomes With The NIST Cybersecurity Framework.* Available: https://www.govloop.com/resources/achieving-successful-outcomes-with-the-nist-cybersecurity-framework/ Last accessed 19th July 2020.

Moustakas, C. (1994) *Phenomenological research methods*, Thousand Oaks, CA: Sage.

Naden, C., 2021. *The cybersecurity skills gap*. [online] ISO. Available: https://www.iso.org/news/ref2655.html Last accessed 12 May 2021.

NCSC. (2019). *Most hacked passwords revealed as UK cyber survey exposes gaps in online security.* Available: https://www.ncsc.gov.uk/news/most-hacked-passwords-revealed-as-uk-cyber-survey-exposes-gaps-in-online-security Last accessed 17th June 2020.

Ngulube, P. (2017). Chapter 1. In: Ngulube, P *Handbook of Research on Theoretical Perspectives on Indigenous Knowledge Systems in Developing Countries*. USA: IGI Global. 21

NIST. (2018). *Cybersecurity Framework.* Available: https://www.nist.gov/cyberframework Last accessed 21st July 2021.

Norman, D. A. (1983). Design rules based on analyses of human error. *Communications of the ACM*, 26(4), 254–258. https://doi.org/10.1145/2163.358092

Novick, G. (2008). Is there a bias against telephone interviews in qualitative research?. *Research in Nursing and Health*. 31, 391-398.

O'Reilly, K. (2005) *Ethnographic methods*, London: Routledge.

Osterman Research. (2019). *The ROI of Security Awareness Training.* Available: https://www.mimecast.com/globalassets/documents/whitepapers/osterman-the-roi-of-security-awareness-training.pdf Last accessed 20th March 2020.

Ownsworth, T., Theodoros, D., Cahill, L., Vaezipour, A., Quinn, R., Kendall, M., Moyle, W. and Lucas, K. (2020). Perceived usability and acceptability of videoconferencing for delivering community-based rehabilitation to individuals with acquired brain injury: A qualitative investigation. *Journal of the International Neuropsychological Society*. 26 (1), 47-57.

Packet Labs. (2020). *The Role Of Human Error In Cybersecurity Breaches.* Available: https://www.packetlabs.net/human-error-in-cybersecurity/ Last accessed 17th June 2021.

Panetta, K. (2020). *7 Security Areas to Focus on During COVID-19.* Available: https://www.gartner.com/smarterwithgartner/7-security-areas-to-focus-on-during-covid-19 Last accessed 16th March 2021.

Parsons, K. McCormac, A. Butavicius, M. and Ferguson, L. (2010) 'Human factors and information security: Individual, culture and security environment', *Command, Control, Communications and Intelligence Division*, Defence Science and Technology Organization, DSTO-TR-2484, Department of Defence, Australian Government.

Patil, P., Zavarsky, P., Lindskog, D. and Ruhl, R. (2012) 'Fault tree analysis of accidental insider security events', *IEEE International Conference on Cyber Security*, pp. 113-118.

Patino, C. M. and Ferreira, J. C. (2018). Inclusion and exclusion criteria in research studies: definitions and why they matter. *Jornal Brasileiro De Pneumologia*. 44 (2), 84.

Patterson, K., Grenny, J., Maxfield, D., McMillan, R. and Switzler, I (2007). *Influencer: The Power to Change Anything*. London: McGraw-Hill

Patton, M. Q. (1990) *Qualitative evaluation and research methods*, Newbury Park, CA: Sage Publications. Second Edition.

PCI DSS. (2018). *PCI Data Security Standard Requirements and Security Assessment Procedures.* Available: https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss Last accessed 8th September 2020.

Perlroth, N. (2017). *All 3 Billion Yahoo Accounts Were Affected by 2013 Attack.* Available: https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html Last accessed 16th July 2020.

Peticca-Harris, A., deGama, N., and Elias, S. (2016). A dynamic process model for finding informants and gaining access in qualitative research. *Organizational Research Methods*. 19 (3), 376-401.

Polit, D. F. and Beck, C. T (2006). *Essentials of Nursing Research: Methods, Appraisal, and Utilization*. 6th ed. Philadelphia, PA: Lippincott Williams & Wilkins

Pope, E. M. (2020). From Participants to Co-Researchers: Methodological Alterations to a Qualitative Case Study. *The Qualitative Report*. 25 (10), 3749-3761

Posey, B. (2019). *What the Equifax Data Breach Says about Hacker Intent.* Available: https://www.itprotoday.com/security/what-equifax-data-breach-among-many-others-says-about-hacker-intent Last accessed 29th September 2021.

Price, A. (2018). *Can We Overcome Human Error in Cybersecurity?*. Available: https://fortifiedhealthsecurity.com/blog/can-overcome-human-error-cybersecurity Last accessed 17th June 2020.

ProofPoint. (2021). *2021 State of the Phish: An In-Depth Look at User Awareness, Vulnerability and Resilience.* Available: https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-state-of-the-phish-2021.pdf Last accessed 15th November 2021.

ProofPoint. (2020). *People-centric Cybersecurity: A Study of IT Leaders in the UK & Ireland.* Available: https://www.proofpoint.com/sites/default/files/white-papers/UK_CISO-REPORT_FINAL.pdf Last accessed 19th September 2021.

PwC, 2020. *Cyber Threats 2020: Report on the Global Threat Landscape*. [online] PwC. Available: https://www.pwc.co.uk/issues/cyber-security-services/insights/cyber-threats-2020-report-on-global-landscape.html Last accessed 19 July 2021.

PwC, 2018. The Global State of Information Security Survey 2018. [online] Available: https://www.pwc.com/sg/en/publications/assets/gsiss-2018.pdf Last accessed 3rd June 2019.

Rajbhandari, L. (2013) 'Consideration of opportunity and human factor: required paradigm shift for information security risk management', *IEEE European Intelligence and Security Informatics Conference*, pp. 147-150.

Reason, J. T. (1990). *Human Error* (First). Cambridge England ; New York: Cambridge University Press.

Reciprocity. (2021). *Security Awareness: 5 Ways to Educate Your Employees.* Available: https://reciprocity.com/security-awareness-5-ways-to-educate-employees Last accessed 10th July 2021.

Reciprocity. (2021). *The Ultimate Guide to Security Awareness Training.* Available: https://reciprocity.com/the-ultimate-guide-to-security-awareness-training Last accessed 15th September 2021.

Ridoutt, P. (2008). 'Improving the Development and Implementation of Modern Tourism Information and Communications Technologies In The Caribbean'. DProf thesis, Middlesex University, London. Available: https://eprints.mdx.ac.uk/id/eprint/2089

Rivard, J. R., Fisher, R. P., Robertson, B., and Mueller, D. H. (2014). Testing the cognitive interview with professional interviewers: Enhancing recall of specific details of recurring events. *Applied Cognitive Psychology*. 28 (6)

Robinson, A. (2021). *Using Influence Strategies to Improve Security Awareness Programs.* Available: https://sansorg.egnyte.com/dl/vYqisYL6LU Last accessed 10th November 2021.

Rock, C., 2018. *How To Stay In Control In The Ever-Changing World Of Technology*. [online] Forbes. Available: https://www.forbes.com/sites/forbestechcouncil/2018/12/18/how-to-stay-in-control-in-the-ever-changing-world-of-technology/?sh=294798b02789 Last accessed 3rd February 2021.

Rodriguez, S. (2018). *Facebook says hackers were able to access millions of phone numbers and email addresses.* Available: https://www.cnbc.com/2018/10/12/facebook-security-breach-details.html Last accessed 17th June 2021.

Rubin, H. J. and Rubin, I. S. (2012). *Qualitative interviewing the art of hearing data* . 3rd ed. Thousand Oaks, CA: Sage

Sadala, M. L. and Adorno, R. D. (2001) 'Phenomenology as a method to investigate the experiences lived: A perspective from Husserl and Merleau-Ponty's thought', *Journal of Advanced Nursing*, 37(3), pp.282-293.

Samy, N. G. and Ahmad, R. (2009) 'Threats to health information security', *IEEE Fifth International Conference on Information Assurance and Security*, pp. 540-543.

Santarcangelo, M. (2011). *Teach, don't just learn, to build your security career.* Available: https://www.csoonline.com/article/2128956/teach--don-t-just-learn--to-build-your-security-career.html Last accessed 9th July 2021.

Sasse, M.A. Ashenden, D. Lawrence, D. Coles-Kemp, L. Fléchais, I. and Kearney, P. (2007) 'Human vulnerabilities in security systems', *Human Factors Working Group White Paper, Cyber Security Knowledge Transfer Networks*.

Scarfone, K. Benigni, D. and Grance, T.. (2009). *Cyber Security Standards.* Available: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=152153 Last accessed 16th July 2021.

Schneier, B. (2008). *Schneier on Security*. New York: John Wiley & Sons.

Schwandt, T. A. (1997) *Qualitative inquiry: A dictionary of terms,* Thousand Oaks, CA: Sage.

Security Magazine. (2020). *Research Confirms Links Between Cyber Attacks, Consumer Purchasing and Brand Loyalty.* Available: https://www.securitymagazine.com/articles/92626-research-confirms-links-between-cyber-attacks-consumer-purchasing-and-brand-loyalty Last accessed 19th July 2020.

Seitz, S. (2016). Pixilated partnerships, overcoming obstacles in qualitative interviews via Skype: A research note. *Qualitative Research*. 16 (2), 229–235.

Shappell, S. and Wiegmann, D. (2001). Applying Reason: The human factors analysis and classification system. *Human Factors and Aerospace Safety*, 1, 59-86.

Shelton, C. (1999). *Human Interface/Human Error.* Available: https://users.ece.cmu.edu/~koopman/des_s99/human/ Last accessed 16th January 2021.

Shenton, A. K. (2004) 'Strategies for ensuring trustworthiness in qualitative research projects', *Education for Information*, 22(2), pp.63-75.

Shropshire, J., Warkentin, M., Johnston, A. and Schmidt, M. (2006). Personality and IT security: An application of the five-factor model. *AMCIS 2006 Proceedings*. 415

Sjouwerman, S. (2021). *7 reasons for security awareness failure.* Available: https://blog.knowbe4.com/bid/316206/7-reasons-for-security-awareness-failure Last accessed 10th October 2021.

Smith, J. A., Flowers, P., and Larkin, M. H. (2009). *Interpretative phenomenological analysis: theory, method and research*. Los Angeles: Sage

Smith, J.A. and Osborn, M. (2004). *Interpretative Phenomenological Analysis*. London: Sage

Smith, M. (2009) 'Changing staff behaviour', *Information Security Technical Report*, *ScienceDirect*, Volume 14, pp. 175.

Snow, C.P. (2013). *The Two Cultures and the Scientific Revolution*. 2nd ed. CT, USA: Martino Fine Books

Somasundram, D. (2007). 'A gender inclusive model in theological education for the Seventh-day Adventist church'. DProf thesis, Middlesex University, London. Available: https://eprints.mdx.ac.uk/id/eprint/2659

Spinelli (2005) The interpreted world : an introduction to phenomenological psychology, 2nd Edition, SAGE: London.

Spitzner, L. (2012). *Securing the human: building and deploying an effective security awareness program.* Available: https://www.sans.org/cyber-security-courses/managing-human-risk-mature-security-awareness-programs/ Last accessed 13th July 2021.

Stake, R.E. (1994) 'Case studies' in N.K. Denson and Y.S. Lincoln (eds), pp.236 - 247 *Handbook of qualitative research,* London: Sage.

Stallings, W. (2010) *Network security essentials: Applications and standards*, Fourth Edition. Prentice Hall.

Strauss, A. L. and Corbin, A. (1990) *Basics of qualitative research: Grounded theory procedures and techniques*, London: Sage.

Sun, F., Han, X. and Wang, J. (2010) ‘An immune danger theory inspired model for network security monitoring’, *IEEE International Conference on Challenges in Environmental Science and Computer Engineering*, pp. 33-35.

Symanovich, S. (2019). *What is a security breach?*. Available: https://us.norton.com/internetsecurity-privacy-security-breach.html Last accessed 19th June 2020.

Tomhave, B. (2010). *Education, Training, and Awareness - There's a Difference!*. Available: http://www.secureconsulting.net/2010/05/education_training_and_awarene.html Last accessed 19th September 2021.

Touchstone Security. (2020). *5 Benefits of Security Awareness Training.* Available: https://touchstonesecurity.com/security-training Last accessed 16th July 2021.

Turney, L. and Pocknee, C. (2005). Virtual focus groups: New frontiers in research. *International Journal of Qualitative Methods*. 4 (2), 32–43.

USecure. (2021). *The complete guide to security awareness training.* Available: https://www.usecure.io/en/guide/security-awareness-training Last accessed 15th September 2021.

Vagle, M. D (2014). *Crafting Phenomenological Research*. 2nd ed. New York, NY: Routledge.

Verizon. (2021). *Verizon 2021 Data Breach Investigations Report.* Available: https://www.verizon.com/business/resources/reports/dbir/ Last accessed 3rd September 2021.

Verplanke, B (2018). *The Psychology of Habit: Theory, Mechanisms, Change, and Contexts*. Bath, UK: Springer.

Vlandan, M. (2020). *What is Security Awareness Training?*. Available: https://reciprocity.com/resources/what-is-security-awareness-training Last accessed 3rd September 2020.

VMware. (2020). *Global Threat Report 2020.* Available: https://www.carbonblack.com/wp-content/uploads/VMWCB-Report-GTR-Extended-Enterprise-Under-Threat-Global.pdf Last accessed 20th July 2021.

Welman, J. C. and Kruger, S. J. (1999) *Research methodology for the business and administrative sciences,* Johannesburg, South Africa: International Thompson.

Wiederhold, B. K. (2020). Connecting through technology during the coronavirus disease 2019 pandemic: Avoiding “zoom fatigue.” *Cyberpsychology, Behavior, and Social Networking*. 23 (7), 437–438.

Wilson, M. and Hash, J., 2003. *Building an Information Technology Security Awareness and Training Program*. [ebook] National Institute of Standards and Technology. Available:

https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-50.pdf Last accessed 4 April 2021.

Winkler, I and Manke, S. (2013). *7 reasons for security awareness failure.* Available: https://www.csoonline.com/article/2133697/7-reasons-for-security-awareness-failure.html Last accessed 3rd September 2020.

Yeagley, G. (2015). *T Security Policies and Procedures: Why You Need Them.* Available: https://www.compassitc.com/blog/it-security-policies-and-procedures-why-you-need-them Last accessed 17th June 2019.

Yin, R. K (2009). *Case study research: design and methods*. 3rd ed. California: Sage Publication.

Appendix A: Email Letter of Invitation

Dear Sir / Madam:

My name is Lukman Sharif. I am currently pursuing a Doctorate in Professional Studies with Middlesex University, UK. My doctoral research project aims to explore the effectiveness of information security (InfoSec) awareness training. I am interested in understanding the experiences of InfoSec professionals in building and implementing InfoSec awareness programmes, their successes, failures, lessons learnt, and advice for other professionals looking to build their own InfoSec awareness programmes. In particular, I am attempting to gain an understanding of the main shortcomings in existing InfoSec awareness programmes and how these can be addressed in order to reduce human errors.

Your organisation was contacted as a potential partner for this research project based on satisfying some or all of the following criteria:

- It is a small to medium-sized enterprise (SME) with fewer than 250 employees
- It is engaged in professional, technical or scientific activities
- It maintains a chief information officer (CIO) and/or a chief information security officer (CISO) or someone with equivalent responsibility and authority
- It has implemented and manages an InfoSec awareness training programme
- It is engaged in research and development in the area of latest InfoSec threats and attack vectors with a particular focus on the role of human factors in InfoSec

Additionally, as a prospective research participant, you are involved in the design and implementation of your organisation's InfoSec awareness programme with strategic or tactical level oversight.

Your organisation has granted me permission to contact potential research participants for this project for the purpose of conducting interviews. The interview will be conducted online (via Zoom or Skype) and is expected to last approximately 60-90 minutes on a date and time that is convenient for you. Your participation in this research will be subject to the Middlesex University's Code of Practice for Research which is committed to maintaining high standards of ethics in research. Your participation in the study will provide valuable contributions towards an improved understanding of InfoSec awareness programmes and how their effectiveness can be enhanced to reduce human errors. Your participation in this research is voluntary and will not affect your standing at your organisation.

If you are interested in participating in this research, kindly complete the accompanying *Pre-Screening Questionnaire* and return it using the email below. If you have any further questions, please feel free to contact me at: LS855@live.mdx.ac.uk

I appreciate your time and consideration in this matter.

Lukman Sharif

Doctoral Candidate, Middlesex University, UK

Appendix B: Participant Pre-Screening Questionnaire

Project Title: *An Alternative Approach to Information Security Awareness Training to Reduce Human Errors*
Researcher: Lukman Sharif
Department: Institute for Work Based Learning, Middlesex University London
Email: LS855@live.mdx.ac.uk

This questionnaire has been designed to gather basic information from potential participants in order to determine their suitability for this research project. All information provided on this questionnaire will be treated with the utmost confidentiality and will not be shared with any third party. The completed questionnaire will be examined to determine eligibility; participation is not guaranteed. By completing this questionnaire, it is assumed that you are willing to share your InfoSec related professional experiences with the researcher.

Name:	***Age:***
Gender: *M / F*	***Education Level (Bachelor's/Master's/ Doctorate):***
Current job title and main responsibilities.	
Years of experience in InfoSec. Please list all job titles (up to past 10 years).	
InfoSec related (threats, human factors, awareness training) peer-reviewed research publications. Please list top three.	
InfoSec industry-recognized professional certifications. Please list top two.	
Does your organisation have an InfoSec awareness programme in place?	
Do you have responsibility for implementing / maintaining your organisation's InfoSec awareness programme? Please provide a brief description of your role.	

Appendix C: Participant Information Sheet (PIS)

Overview

It is important that you understand why this research is taking place and what it is likely to involve. Before you make a decision about whether or not you would like to participate in this study, please take some time to read and consider the following information carefully. Please do not hesitate to ask the main researcher if there is anything that is not clear or if you require further information.

Introduction

You are being invited to take part in a research project that I am undertaking as part of a Doctorate in Professional Studies (DProf) at Middlesex University, London, United Kingdom. This project provides an opportunity to investigate InfoSec awareness programmes implemented by organisations and the ways in which such programmes can be made more effective. This study aims to make a valuable contribution to our common professional practice (the field of InfoSec) by increasing our understanding of the importance of InfoSec awareness programmes and by offering guidelines to improve their effectiveness in mitigating security breaches resulting from human errors. Your contribution as an InfoSec professional is crucial to the success of this study. As an expert in this field and due to your first-hand experience with InfoSec research and awareness programmes, you are in a unique position to share your experiences and offer valuable insights into current practices in the field. The results of this study will eventually be published in scientific journals and may also be reported at professional practice and work-based learning seminars and conferences.

What is Involved

This research will be conducted through online interviews using Skype or Zoom. The interview is expected to last approximately 60-90 minutes on a date and time that is convenient for you. All interviews will be audio recorded. After the initial interview, a further 15-20 minutes of your time will be required (on a later day), for you to review and validate the transcripts and offer your thoughts on emergent themes generated during data analysis.

The researcher will commence the interview by asking you some basic background questions. The researcher seeks to explore your thoughts, perceptions, and reflections on your experience as it relates to the field of InfoSec. More specifically, depending on your specific InfoSec background, the areas to be explored could include:

- Design, implementation and maintenance of InfoSec awareness programmes
- The cybersecurity threat landscape - latest trends and attack vectors
- Appropriate and effective responses to InfoSec threats
- Human factors in InfoSec as potential contributors to the success/failure of awareness programmes

The discussion will follow interesting ideas and explore your answers in more detail.

The type of questions will include:

- Your reflections about the role of InfoSec awareness programmes in your organisation.
- How does InfoSec awareness training in your organisation affect the frequency of security breaches, especially those related to human errors?
- What you feel are the reasons for any perceived successes or failures? What practical lessons you can draw from your experiences? How you think InfoSec awareness programmes can be improved at your organisation (or in general)? What advice you can offer to other InfoSec professionals looking to build their own InfoSec awareness programmes?

During the interview, if you have any concerns or questions about what is being asked, please do not hesitate to bring it up. You may also decline to answer any question(s) if you choose. Your opinions and insights as an InfoSec professional are highly valued and your contribution is vital to the success of this project. The main researcher is also an InfoSec professional practicing in the same area with many years of experience and believes that the only way to advance our understanding of this research area is through close collaboration and sharing of expertise. At the conclusion of this research project, the findings will be shared with all of the participants in this research, other researchers, professional colleagues and stakeholders.

Privacy & Confidentiality Information

Your participation in this research will be subject to the Middlesex University's Code of Practice for Research which is committed to maintaining high standards of ethics in research. All information obtained in this project will remain fully confidential. You will not be asked for any sensitive organisational information such as security vulnerabilities, configurations, policy content or system architecture, etc. Your information will not be shared with any third party. The data collected in this research will be anonymised using codes to identify different research participants. The data will be presented in an aggregate form as part of my DProf project report and there will be no record that links the data collected from you with any personal data from which you could be identified. All notes, transcripts and identifying participant information will be locked away in personal possession of the researcher, stored in accordance with the UK Data Protection Act, 2018.

Your participation in this research is voluntary and you are free to withdraw at any time without prejudice. If you decide to participate in this research, you will be asked to sign a consent form. You are free to withdraw even after signing the consent form. If you withdraw from this research before data collection is completed, your data will be deleted/destroyed. However, it will not be possible to withdraw your data at a later stage due to the anonymised nature of the research. Ultimately, the data will be owned by Middlesex University. If you are satisfied with the information provided above and wish to participate in this research, kindly complete the attached *Participant Informed Consent Form* and email it back on the address provided.

Your time and consideration is greatly appreciated.

Lukman Sharif, Doctoral Candidate, Middlesex University, UK

Appendix D: Participant Informed Consent

Project Title: *An Alternative Approach to Information Security Awareness Training to Reduce Human Errors*
Researcher: Lukman Sharif
Department: Institute for Work Based Learning, Middlesex University London
Email: LS855@live.mdx.ac.uk

Middlesex University Research Ethics Committee has approved this research. This committee requires all participants to be notified that in case of any complaints regarding the way in which this research is conducted, their concerns can be sent directly to the main researcher at the above address. If you have any questions regarding your rights as a research participant, or if you have concerns you do not feel you can discuss with the main researcher, you can contact the Director of Studies at:

Middlesex University London, Institute for Work Based Learning, The Burroughs, Hendon Way, London, NW4 4BT, UK, Phone: +44 20 8411 3422, Email: ResearchDegrees@mdx.ac.uk

---

Consent:

I have read and understand the information provided on the accompanying Participant Information Sheet (PIS). I understand the nature and purpose of the research project and my involvement in it. I acknowledge Middlesex University Research Ethics Committee's approval of this research. I agree to take part in this research. I understand that my participation is voluntary and that I reserve the right to withdraw at any time, without prejudice. I understand that I will be given a copy of this consent.

I agree to the interview being audio recorded. I understand that all my data will be treated with the utmost confidentiality and that I will not be personally identified in the study or any future publications or reports.

I confirm that I have had the opportunity to ask questions and also understand that I may contact the main researcher if I require further information or if I wish to make a complaint regarding my involvement in the research.

Name (Print): ....

Contact Telephone Number: ....

Signature: ....

Date: ....

Appendix E: Interview Protocol

Project Title: *An Alternative Approach to Information Security Awareness Training to Reduce Human Errors*

Name of Interviewer: ____________________ Date: __________ Starting Time: _________

Participant ID Code: ________________

- Thank the participant for agreeing to participate in the research
- Introduce myself and explain the purpose of the research
- Describe the interview structure:
    - Participation is voluntary – may stop at any time if not comfortable
    - The interview will last for 60 – 90 minutes (until all questions / follow-up questions have been answered)
    - Interview will be audio recorded (recordings will be destroyed after transcription)
    - Further 15-20 minutes of participant's time required (on a later day) to validate the transcript and emergent themes
    - Researcher will take notes during the interview
    - Remind that all information will remain strictly confidential
- At the beginning of each audio recording, announce the Participant ID code, date and time
- Ensure that participant has signed the informed consent form
- Define any necessary terms likely to be used during the interview
- Ask the participant if they have any questions
- At the conclusion of the interview:
    - Thank the participant for their time
    - Assure confidentiality
    - Provide information on how / when they can receive results of the research

Interviewer's Notes:

____

____

____

____

Appendix F: Interview Questions

Interview Question	**Respondent** **(ISA / ISP)**	**Corresponding** **Objective (s)**
What do you perceive as the biggest challenges to building an InfoSec awareness program for organisations?	ISA, ISP	1, 2
Can you describe your feelings towards building your InfoSec awareness programme? What failures and pitfalls did you face?	ISP	1, 2
What were the major internal / political obstacles you experienced in implementing the InfoSec awareness programme and how did you deal with them?	ISP	1, 2, 4
What are your thoughts on the role of senior management in the success of an InfoSec awareness programme? Did you feel supported? How can you gain their support?	ISA, ISP	1, 2, 4
What would you describe as your main successes in implementing the InfoSec awareness programme?	ISP	2, 4
Why do you think phishing and other social engineering attacks are so widespread and successful?	ISA, ISP	1, 2, 4
From your experience, how do you think InfoSec awareness programmes can be improved to change human behaviour for the better?	ISA, ISP	2, 4
What InfoSec awareness strategies have you found to be most effective to prevent human error and to promote the protection of organisational information systems and data?	ISA, ISP	2, 4
How has the implementation of an InfoSec awareness programme affected the frequency and severity of security breaches in your organisation, especially those related to human errors?	ISP	1, 2, 4
How do you establish what InfoSec concepts are most important in your organisation’s InfoSec awareness programme?	ISA, ISP	2, 4
How do you determine that your users have been adequately trained through InfoSec awareness strategies to protect your organisational information systems and data?	ISA, ISP	2, 4
In your opinion, what is the best training frequency and what teaching and learning styles are most effective?	ISA, ISP	1, 2, 4

How do you measure the success of an InfoSec awareness programme?	ISA, ISP	2, 4
What evaluation mechanisms / metrics have you found to be useful for measuring the effectiveness of InfoSec programmes?	ISA, ISP	1, 2, 4
What constitutes an effective InfoSec awareness programme in your opinion?	ISA, ISP	1, 2, 4
What advice would you offer to other professionals wishing to build their own InfoSec awareness programme?	ISA, ISP	2, 4
ISA = InfoSec Academic ISA = InfoSec Practitioner		

Appendix G: Development of Units of Meaning

Open Code No	Unit of Meaning	Respondent (ISA / ISP)	Corresponding Objective (s)
1	Inappropriate training materials	ISA, ISP	1, 4
2	Breaking down materials	ISA, ISP	2, 4
3	Security culture	ISA, ISP	2, 4
4	Mobile device security	ISA	1, 4
5	Malware attacks	ISA	1
6	Incorrect understanding of InfoSec awareness training	ISA	1, 4
7	Lack of cybersecurity knowledge	ISA, ISP	1, 2, 4
8	Security fatigue	ISA	1
9	Punishment / consequences of noncompliance	ISA, ISP	2, 4
10	Build rapport with users	ISA, ISP	1, 2, 4
11	Proactive vs reactive security culture	ISA	1, 2, 4
12	Principle of least privilege	ISA, ISP	2, 4
13	Ready-made online InfoSec awareness training solutions	ISA	2, 4
14	Lack of empirical research in relation to human behaviour in awareness training	ISA	1, 4
15	User buy-in	ISA, ISP	1, 2, 4
16	Misunderstanding about InfoSec awareness budget requirements	ISA, ISP	1, 2, 4
17	Budget	ISA, ISP	1, 4
18	Uniform InfoSec awareness training for home and work	ISA	1, 2, 4

19	Different priorities for management and InfoSec professionals	ISP	1, 4
20	Tangible proofs to convince management	ISA, ISP	2, 4
21	Coordination with sales, marketing, and PR to communicate security messages	ISA, ISP	2, 4
22	Use of Learning Management System (LMS) to deliver and track training	ISA, ISP	1, 2, 4
23	Failure to recognize InfoSec awareness as a discipline	ISA	1, 4
24	Establishing baselines	ISA	4
25	One size fits all approach	ISA, ISP	2, 4
26	User reporting of suspicious behaviour	ISP	2, 4
27	Employee satisfaction	ISA	1, 2, 4
28	Ransomware	ISA	1
29	Online training	ISA, ISP	2, 4
30	Inform, not dictate	ISA	2, 4
31	Tracking users that complete training	ISA, ISP	2, 4
32	Start small and simple	ISA, ISP	2, 4
33	Use of vignettes with good / bad security characters	ISA, ISP	1, 2, 4
34	Reduce security load on users	ISA, ISP	1, 4
35	Humans as weakest link	ISA, ISP	1, 4
36	InfoSec awareness as a “police function”	ISP	1, 2, 4
37	Unified security message	ISA, ISP	2, 4
38	Security as an inconvenience	ISP	1, 4
39	Unrealistic expectations	ISA, ISP	1, 4
40	Continuous learning	ISA	2, 4
41	Technology democracy	ISA, ISP	1, 2, 4

42	Careless handling of sensitive data	ISA, ISP	1, 4
43	Social engineering	ISA, ISP	1
44	Single source training	ISA, ISP	1, 4
45	Lack of focus on InfoSec HCI	ISA	1, 4
46	Repetition of security messages	ISA, ISP	2, 4
47	Build / customize your own awareness programme	ISA, ISP	2, 4
48	Security treated as a “step-child”	ISP	1, 4
49	Dynamic InfoSec awareness programme – evolves to meet organisation’s needs	ISA, ISP	2, 4
50	Political obstacles to change	ISA, ISP	1, 4
51	Password and authentication	ISP	1
52	User habits	ISA	1, 2, 4
53	Use of outdated / unauthorized software	ISA, ISP	1, 4
54	Practical tips	ISA, ISP	2, 4
55	Lack of evaluation metrics	ISA, ISP	1, 4
56	Sources of influence on human behaviour	ISA	1, 2, 4
57	Seminars and external speakers	ISA, ISP	1, 2, 4
58	Classroom-based training	ISA, ISP	2, 4
59	Use of quizzes, surveys and questionnaires	ISA, ISP	2, 4
60	Phishing attacks	ISA, ISP	1
61	Personality traits	ISA	1, 2, 4
62	Rewards schemes for compliance	ISA, ISP	2, 4
63	Any InfoSec awareness programme better than none	ISA	1, 2, 4
64	Frequency of InfoSec awareness training	ISA, ISP	2, 4
65	People as the biggest investment	ISA, ISP	1, 2, 4

66	Organisation wide email security messages	ISA, ISP	2, 4
67	Interactive content	ISA	2, 4
68	Working remotely	ISP	1
69	Planned, targeted and consistent training	ISA, ISP	2, 4
70	Simulated phishing attacks	ISA, ISP	2, 4
71	Relevance to users’ daily lives	ISA, ISP	1, 2, 4
72	Security as a 24x7 function	ISP	1, 2, 4
73	Positive reinforcement – treat users with respect	ISA, ISP	2, 4
74	Enforcement of policies	ISA, ISP	1, 2, 4
75	Social networking	ISA	1, 4
76	Opportunity	ISA	2, 4
77	Senior management buy in	ISA, ISP	1, 2, 4
78	Fun and engaging training material	ISP	2, 4
79	Learning and teaching styles	ISA, ISP	1, 4
80	Gamification of InfoSec awareness training	ISA	2, 4
81	Relevant material	ISA, ISP	2, 4
82	Use of weak password	ISP	1, 4

Appendix H: Consolidation of Units of Meaning to Form Themes

Theme 1: Understanding common user actions contributing to human errors

Open Code No	Unit of Meaning	Respondent (ISA / ISP)	Corresponding Objective (s)
7	Lack of cybersecurity knowledge	ISA, ISP	1, 2, 4
42	Careless handling of sensitive data	ISA, ISP	1, 4
53	Use of outdated / unauthorized software	ISA, ISP	1, 4
82	Use of weak password	ISP	1, 4

Theme 2: Identifying the most common attack vectors

Open Code No	Unit of Meaning	Respondent (ISA / ISP)	Corresponding Objective (s)
4	Mobile device security	ISA	1, 4
5	Malware attacks	ISA, ISP	1
28	Ransomware	ISA	1
43	Social engineering	ISA, ISP	1
51	Password and authentication	ISP	1
60	Phishing attacks	ISA, ISP	1
68	Working remotely	ISP	1
75	Social networking	ISA	1, 4

Theme 3: Personal and social factors contributing to human errors

Open Code No	Unit of Meaning	Respondent (ISA / ISP)	Corresponding Objective (s)
3	Security culture	ISA, ISP	1, 2, 4
27	Employee satisfaction	ISA	1, 2, 4
35	Humans as weakest link	ISA, ISP	1, 4

41	Technology democracy	ISA, ISP	1, 2, 4
52	User habits	ISA	1, 2, 4
61	Personality traits	ISA	1, 2, 4
76	Opportunity	ISA	1, 2, 4

Theme 4: Factors that lead to InfoSec awareness programme failure

Open Code No	Unit of Meaning	Respondent (ISA / ISP)	Corresponding Objective (s)
1	Inappropriate training materials	ISA, ISP	1, 4
3	Security culture	ISA, ISP	1, 2, 4
6	Incorrect understanding of InfoSec awareness training	ISA	1, 4
8	Security fatigue	ISA	1
16	Misunderstanding about InfoSec awareness budget requirements	ISA, ISP	1, 2, 4
19	Different priorities for management and InfoSec professionals	ISP	1, 4
23	Failure to recognize InfoSec awareness as a discipline	ISA	1, 4
36	InfoSec awareness as a “police function”	ISP	1, 2, 4
38	Security as an inconvenience	ISP	1, 4
39	Unrealistic expectations	ISA, ISP	1, 4
44	Single source training	ISA, ISP	1, 4
48	Security treated as a “step-child”	ISP	1, 4
50	Political obstacles to change	ISA, ISP	1, 4
55	Lack of evaluation metrics	ISA, ISP	1, 4
74	Enforcement of policies	ISA, ISP	1, 2, 4
77	Senior management buy in	ISA, ISP	1, 2, 4

Theme 5: InfoSec strategies to prevent human errors

Open Code No	Unit of Meaning	Respondent (ISA / ISP)	Corresponding Objective (s)
3	Security culture	ISA, ISP	2, 4
76	Opportunity	ISA	2, 4

Theme 6: Understanding the psychological perspective of human behaviour in InfoSec

Open Code No	Unit of Meaning	Respondent (ISA / ISP)	Corresponding Objective (s)
14	Lack of empirical research in relation to human behaviour in awareness training	ISA	1, 4
45	Lack of focus on InfoSec HCI	ISA	1, 4
56	Sources of influence on human behaviour	ISA	1, 2, 4

Theme 7: Essential components of an effective InfoSec awareness training programme

Open Code No	Unit of Meaning	Respondent (ISA / ISP)	Corresponding Objective (s)
2	Breaking down materials	ISA, ISP	2, 4
3	Security culture	ISA, ISP	2, 4
9	Punishment / consequences of noncompliance	ISA, ISP	2, 4
10	Build rapport with users	ISA, ISP	2, 4
11	Proactive vs reactive security culture	ISA	2, 4
12	Principle of least privilege	ISA, ISP	2, 4
13	Ready-made online InfoSec awareness training solutions	ISA	2, 4
15	User buy-in	ISA, ISP	2, 4
17	Budget	ISA, ISP	4
18	Uniform InfoSec awareness training for home and work	ISA	2, 4

20	Tangible proofs to convince management	ISA, ISP	2, 4
21	Coordination with sales, marketing, and PR to communicate security messages	ISA, ISP	2, 4
22	Use of Learning Management System (LMS) to deliver and track training	ISA, ISP	2, 4
24	Establishing baselines	ISA	4
25	One size fits all approach	ISA, ISP	2, 4
26	User reporting of suspicious behaviour	ISP	2, 4
29	Online training	ISA, ISP	2, 4
30	Inform, not dictate	ISA	2, 4
31	Tracking users that complete training	ISA, ISP	2, 4
32	Start small and simple	ISA, ISP	2, 4
33	Use of vignettes with good / bad security characters	ISA, ISP	2
34	Reduce security load on users	ISA, ISP	4
37	Unified security message	ISA, ISP	2, 4
40	Continuous learning	ISA	2, 4
46	Repetition of security messages	ISA, ISP	2, 4
47	Build / customize your own awareness programme	ISA, ISP	2, 4
49	Dynamic InfoSec awareness programme – evolves to meet organisation’s needs	ISA, ISP	2, 4
54	Practical tips	ISA, ISP	2, 4
57	Seminars and external speakers	ISA, ISP	2, 4
58	Classroom-based training	ISA, ISP	2, 4
59	Use of quizzes, surveys and questionnaires	ISA, ISP	2, 4
62	Rewards schemes for compliance	ISA, ISP	2, 4

63	Any InfoSec awareness programme better than none	ISA	2, 4
64	Frequency of InfoSec awareness training	ISA, ISP	2, 4
65	People as the biggest investment	ISA, ISP	4
66	Organisation wide email security messages	ISA, ISP	2, 4
67	Interactive content	ISA	2, 4
69	Planned, targeted and consistent training	ISA, ISP	2, 4
70	Simulated phishing attacks	ISA, ISP	2, 4
71	Relevance to users' daily lives	ISA, ISP	4
72	Security as a 24x7 function	ISP	4
73	Positive reinforcement – treat users with respect	ISA, ISP	2, 4
74	Enforcement of policies	ISA, ISP	2, 4
77	Senior management buy in	ISA, ISP	2, 4
78	Fun and engaging training material	ISP	2, 4
79	Learning and teaching styles	ISA, ISP	4
80	Gamification of InfoSec awareness training	ISA	2, 4
81	Relevant material	ISA, ISP	2, 4

Appendix I: List of Publications

L. Sharif and M. Ahmed (2010). IPSec: A Practical Approach. Germany: LAP Lambert Academic Publishing Co.

M. Ahmed, L. Sharif, M. N. Kabir and M. Al-Maimani (2012), "Human Errors in Information Security", International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE), Vol. 1, No. 3, pp 82-87, July 2012

M. Ahmed, L. Sharif, Y. M. Alginahi and M. N. Kabir (2011), "A Survey of Routing Attacks in Wireless Sensor Networks", Umm Ul Qurra University, Makkah, KSA, Wireless Sensor Networks Meeting, May 18-19, 2011.

Issa-Salwe, L. Sharif and M. Ahmed (2011), "Strategic Information Systems Planning as the Centre of Information Systems Strategies", International Journal of Research and Reviews in Computer Science (IJRRCS), Vol. 2, No. 1, pp 156-162, March 2011.

L. Sharif and M. Ahmed (2011), 'An Evaluation of the Digital Britain Report', Trends in Information Management (TRIM), Vol. 7, Issue 1, pp 19-30, Jan-Jun 2011.

L. Sharif and M. Ahmed (2011), 'Direct Broadcast Satellite (DBS) Television Systems', International Journal of Research and Reviews in Wireless Communications (IJRRWC), Vol. 1, No. 1, pp 1-6, March 2011.

L. Sharif and M. Ahmed (2010), "The Wormhole Routing Attack in Wireless Sensor Networks (WSN)", Journal of Information Processing Systems (JIPS), Volume 6, No. 2, pp 177-184, June 2010.

M. Ahmed, L. Sharif, A. Issa-Salwe, and A. Alharby (2010), "Information Security: Securing a Network Device with Passwords to Protect Information", Trends in Information Management (TRIM), Vol. 6, Issue 1, pp 62-76, Jan-Jun 2010.

Y. M. Alginahi, M. Ahmed, O. Tayan, A. A. Siddiqi, L. Sharif, A. Alharby and R. Nour (2009), "ICT Students' Stress and its Coping Strategies - English Perspective - A Case Study of Midsize Middle Eastern University", Trends in Information Management, V 5 (2), pp. 111-127, July-Dec

Appendix J: Advanced Developments in Professional Practice - Level 8 RAL Claim

Section 1

1.1. Introduction

I have been working in the Computer Communications and Information Security industry for over 15 years. During this period, I have worked in a variety of highly technical and leadership roles including Chief Technical Officer, Head of Training & Consultancy, Senior Network Consultant, IT Security Solutions Architect, Technical Instructor, Senior Lecturer, Researcher and Author.

I will present my reflections on the development of prominent aspects of my career that I believe will be relevant and useful in the context of my DProf project. In particular there are specific patterns of learning in my current and past professional practice that I believe to be of significant scope and impact to make an RAL level 8 claim. I have presented three cases in order to identify and highlight these specific patterns of learning. These cases will incorporate specific themes, projects, strategic personal and professional development and achievements as well as aspects of generic learning that I will be able to draw on in my DProf project work. This claim also provides an opportunity for me to map out an area of my professional practice that I intend to investigate further in my DProf project.

The professional cases I have selected will demonstrate core research and publication skills and experience as well as specific technical, leadership and project management skills in the field of **Computer Communications Engineering and Information Security**. The latter has allowed me to develop my strategic thinking and professional practice to an advanced intellectual level and influence my community of practice. In my current roles as a Security Solutions Architect, Senior Lecturer in Information Security and a Researcher, I continue to engage in strategic projects and advanced research activities in order to maintain professional influence and impact in my field of practice.

The patterns of learning highlighted in the RAL cases will provide a strong foundation to build on for my DProf project and will prove to be invaluable in writing the literature review, choosing and planning appropriate research methodologies and critical analysis of data and results in order to further develop and enhance my professional and academic standing. The overall process involved in this submission also provides me the opportunity to critically review and reflect on my learning and achievements to date in a focused and coherent manner that I can carry forward in order to further enhance and advance my professional practice.

1.2. Overview of My Current Professional Area

I have been passionate about engineering and computer communications technologies from an early age. Much of the technological advancement in this field has traditionally been driven by hard science such as engineering and mathematics. However, there is a growing recognition of the role of human and social factors in technological innovation. In the field of information technology, this trend manifests itself as human-centred computing and is increasingly visible in modern communications technologies.

Over the years, my own professional practice in the field of computer communications engineering and information security has followed a similar trend with a shift in focus from a purely technical approach to one that is more socio-technical in nature. This approach recognises that information security is both a human and technological problem.

The field of information security is concerned with protecting the confidentially, integrity and availability of information and information systems (Stallings, 2010). Information security has traditionally been considered a technological issue with much attention often focused on technical solutions. Security technologies such as firewalls, antivirus software, and VPNs are undoubtedly invaluable weapons in an organisations' information security armoury. However, technology alone cannot deal with all information security risks. It is ultimately the users in any organisation that are the primary line of defence (Parsons et al, 2010).

A number of major studies [PWC, 2012; Deloitte, 2011: Ernst & Young, 2012 & Sasse et al, 2007] in the recent past have shown that an overwhelming percentage of information security breaches are caused by human factors. There is a general consensus amongst scholars and practitioners that information security is predominantly a human problem. Consequently, there is a need for a holistic approach to understanding human behaviour in this field. Such an approach is intrinsically transdisciplinary because it requires collaboration between information security researchers, practitioners, computer scientists, communications engineers, psychologists, sociologists and philosophers, among others, to understand and address the human factors in information security (Sasse et al, 2007).

The theme of human factors in information security features prominently in the RAL cases that I have presented here. This is also an area of research that I intend to explore further for my DProf project. In the following sections, I will provide a critically reflective account of the RAL cases and the advanced level learning that I have achieved in the specific area of my professional practice. I will conclude by briefly discussing the particular aspects of my professional practice that I intend to research and develop further as part of my DProf project.

1.3. Overview of RAL @ Level 8 Claim

I will present the following cases for my RAL @ Level 8 claim of 120 credits:

RAL Case 1:	
Period:	June 2004 - August 2010
Professional Role:	IT Security Solutions Architect, Technical Author
Credit claimed for:	Book publication
IPSec: A Practical Approach – Network Security (Refer to Appendices A & B for details)	

<table>
<tr><td colspan="2"><b>RAL Case 2:</b></td></tr>
<tr><td>Period:</td><td>March 2005 - Present</td></tr>
<tr><td>Professional Role:</td><td>Senior Lecturer in Computer Networks & Information Security, Researcher</td></tr>
<tr><td>Credit claimed for:</td><td>Research papers / articles in international journals (Refer to Appendix C for details)</td></tr>
<tr><td colspan="2"><i>M. Ahmed, L. Sharif, M. N. Kabir and M. Al-Maimani (2012), “Human Errors in Information Security”, International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE), Vol. 1, No. 3, pp 82-87, July 2012</i>
<i>M. Ahmed, L. Sharif, Y. M. Alginahi and M. N. Kabir (2011), “A Survey of Routing Attacks in Wireless Sensor Networks”, Umm Ul Qurra University, Makkah, KSA, Wireless Sensor Networks Meeting, May 18-19, 2011.</i>
<i>Issa-Salwe, L. Sharif and M. Ahmed (2011), “Strategic Information Systems Planning as the Centre of Information Systems Strategies”, International Journal of Research and Reviews in Computer Science (IJRRCS), Vol. 2, No. 1, pp 156-162, March 2011.</i>
<i>L. Sharif and M. Ahmed (2011), ‘An Evaluation of the Digital Britain Report’, Trends in Information Management (TRIM), Vol. 7, Issue 1, pp 19-30, Jan-Jun 2011.</i>
<i>L. Sharif and M. Ahmed (2011), ‘Direct Broadcast Satellite (DBS) Television Systems’, International Journal of Research and Reviews in Wireless Communications (IJRRWC), Vol. 1, No. 1, pp 1-6, March 2011.</i>
<i>L. Sharif and M. Ahmed (2010), “The Wormhole Routing Attack in Wireless Sensor Networks (WSN)”, Journal of Information Processing Systems (JIPS), Volume 6, No. 2, pp 177-184, June 2010.</i>
<i>M. Ahmed, L. Sharif, A. Issa-Salwe, and A. Alharby (2010), “Information Security: Securing a Network Device with Passwords to Protect Information”, Trends in Information Management (TRIM), Vol. 6, Issue 1, pp 62-76, Jan-Jun 2010.</i>
<i>Y. M. Alginahi, M. Ahmed, O. Tayan, A. A. Siddiqi, L. Sharif, A. Alharby and R. Nour (2009), “ICT Students’ Stress and its Coping Strategies - English Perspective - A Case Study of Midsize Middle Eastern University”, Trends in Information Management, V 5 (2), pp. 111-127, July-Dec</i></td></tr>
</table>

<table>
<tr><td colspan="2"><b>RAL Case 3:</b></td></tr>
<tr><td>Period:</td><td>June 2000 – September 2003 <i>(<b>Note</b>: I continue to use updated and customised versions of this course in my current teaching)</i></td></tr>
<tr><td>Professional Role:</td><td>Senior Network Solutions Architect, Senior IT Instructor, Technical Author</td></tr>
<tr><td>Credit claimed for:</td><td>Information Security Training Course</td></tr>
</table>

Managing Network Security (Refer to Appendices D, E for details)	

In the following section, I will go through each case in detail in order to identify and highlight the significant depth and breadth of professional learning that I have already achieved in my area of DProf research interest and to support my claim for advanced developments in professional practice.

Section 2

2.1. Advanced Learning and Experience Gained Through Publishing My Book (RAL Case 1)

Overview

I started my career in the computer communications and network security industry as a field engineer. Throughout much of my professional practice to date, I have sought to maintain as much direct hands-on involvement in projects as possible. I am a firm believer in the value of undertaking research in practical settings. The latter could be in the form of simulations, test-beds, pilots and action research, in order to maximise the usefulness and applicability of the research findings. To date, much of my learning, education and professional experience has reflected this approach.

In my role as an IT Security Solutions Architect and Technical Author, I was very fortunate to receive funding to conduct an industry-based research project in the field of computer communications and information security. Due to my involvement in the industry, I was able to conduct an industry-based research project with a practical and tangible impact for my employer at the time. I carried out an investigation of advanced IP Security (IPSec) algorithms and protocols for IP version 4 communications. This involved detailed critical evaluation of component IPSec protocols and algorithms with a practical implementation using Cisco IOS router platform.

I was able to utilise my practical industry experience and my academic research experience in a way that led to the successful publication of this book (Please refer to Appendices A & B for details). As the primary author, I wrote 6 out of the 9 chapters of the book as well as playing a lead role in the design and practical implementation of the lab simulations presented in the book (Appendix G: A1, A2, B1, B2, B3, B4, C1, C2, C3, C4).

One of the key issues highlighted in the book was the role played by end users and systems administrators as it relates to the successful implementation and enforcement of security policies. It was found that despite having deployed state of the art intrusion detection systems and firewalls, many organisations were still vulnerable to a variety of security threats due to misconfigurations and a lack of clarity and proper enforcement of security policies. The role of training, awareness and orientation courses and workshops was identified as a key factor in helping organisations tackle such issues (Appendix G: B1, B4).

Case Evaluation & Reflections

The book explores advanced IPSec algorithms and protocols for IP version 4 communications. The architecture of the IPSec protocol framework and component protocols such as Authentication Header (AH), Encapsulating Security Payload (ESP) and Internet Key Exchange (IKE) are critically evaluated from a practical point of view. (Please refer to Appendices A & B for details).

The publication of this book was an also effort on my part to help address what I perceived to be a lack of correlation between theory and practice in the information security literature (Appendix G: A2, C1, C4). I recall that during my undergraduate studies I took a network security module and despite my best efforts at the time I could not find a book on the subject with practical examples. The practical focus of the book was the main unique selling point. I was able to combine my academic research and industrial experience in an effective way to ensure that the book appealed to a wide audience. Consequently, the book was targeted at academics, students and security professionals looking for an in depth and practical guide to the field of IP security (Appendix G: A1, B2, B4, C3).

The publication of this book has been an interesting experience for me. From a professional perspective the overall experience has been thoroughly rewarding. However, in terms of the actual process of publishing and promoting the book, I have learnt some very useful lessons.

My co-author and I were originally of the opinion that the issue of quality is really a subjective issue and therefore did not feel there was a need to involve a professional editor. Instead, we relied on other colleagues in the same field to provide critical feedback which in hindsight was probably not a wise decision. The process of peer-review is a fundamental component of quality control. It helps to ensure that the work has been evaluated and critiqued by fellows and experts in the same field. In hindsight, I feel that we should not have selected close colleagues to act as referees for the book. This would have minimised any element of bias and conflict of interests and would help to ensure a thorough and objective critical review of the work (Appendix G: A3, B1, B2, B4, C1).

I have found it extremely difficult to be noticed as a new author in the book publishing world where so many different titles are being churned out every day with intense competition and thin margins. The fact that publishers are increasingly shifting the marketing responsibility to authors only exacerbates the situation for a newcomer. The advent of electronic publishing offers many exciting opportunities and some of the issues I have experienced with my book would probably be irrelevant in this context. I am very keen to explore this medium for my future publications to ensure that my work can be made easily accessible to the widest possible audience.

Looking back at my work, I believe that the concept of combining academic research and practical industrial experience still has significant appeal for professionals in my field. Having been involved in university level teaching, I also feel that the approach taken by the book still has a strong appeal for undergraduate and postgraduate level students. However, I feel that the subject of the book is somewhat lagging behind the current industry standards. The book is primarily focused on security for IP version 4 communications. However, this standard will soon be superseded by IP version 6. Although many of the concepts covered in the book would still be relevant, the technical specifics will inevitably change. In hindsight, I would probably not have hastened to publish my work without having carefully thought through these implications (Appendix G: B2, B4, C1).

Although the role of social aspects of information security is an important theme in the book, it is predominantly skewed towards technical solutions. However, since the publication of this book, the focus of my professional practice and academic research has steadily shifted towards socio-economic aspects of information security in recognition of the fact that this particular area of research now represents some of the most important challenges and opportunities for the field (Appendix G: A2, C1).

My experience of writing this book helped me to appreciate the importance of communications and security technologies and their practical application for businesses and growth of economy. During my university studies I had been frustrated at the lack of emphasis on practical applications of technical knowledge. Having gained substantial industrial experience and being able to pass on my knowledge and expertise through this book gave me a great sense of satisfaction. A detailed critical reflection of this aspect of my past learning has already been presented in Review of Learning (DPS4520).

The opportunity to publish a book in the field of Information Security has helped me to acquire a deeper understanding of the field (Appendix G: A1, A2). It has also helped me to appreciate the theoretical, philosophical, and ethical principles underpinning academic and industrial research. I have been able to extend my analytical and logical thinking to a high degree. It also helped me to widen my abstract thinking, creativity, and problem-solving skills.

The skills and experience that I have gained from this advanced authorship will be invaluable in helping me to plan and execute my DProf research. I believe that the knowledge that I have acquired in the process will provide me with a strong foundation for my particular area of DProf research (Please refer to section 3.1). The experience will help me tremendously in conducting my DProf literature review and exploring various research methodologies and data collection methods. I am confident that the overall experience will benefit me academically and professionally for the years to come (Appendix G: B2, B4, C1, C2, C4).

2.2. Advanced Learning and Experience Gained Through Publishing in International Journals (RAL Case 2)

Overview

In this role, I have been responsible for the teaching of Computer Communications and Information Security modules to undergraduate students and industry professionals (from March 2005 – Present). As with my previous roles, the emphasis is on delivering courses that are industrially relevant and provide the students with the necessary professional and technical skills to pursue a career in their chosen field. I also work with senior management to define and implement strategies to further develop and grow the training and consultancy division. In this role, I also have the opportunity to carry out research and lead a small research team focusing on Wireless Networks and Information Security. I have been able to build on the skills and experience gained from the publication of my book to further develop my research activities successfully resulting in a number of publications in international peer-reviewed journals (Please refer to Appendix C).

Case Evaluation & Reflections

I joined a public university in the UK in 2005 as a Technical Instructor and began teaching Computer Communications and Information Security courses at undergraduate and postgraduate level (Appendix G: A1). I brought with me a strong grasp of Communications and Information Security technologies and practices with extensive technical experience and strong strategic and business knowledge. I also completed an MSc in Electronic Engineering with a specialist focus on Wireless Networks and Information Security (Appendix G: A1, B3). The MSc has helped me acquire in depth knowledge and understanding of network architectures, applications and protocols and information security principles and technologies. It has also helped to develop my broader thinking and understanding of the various technologies in a more integrated manner providing me with a strong foundation for my DProf research.

Over the years I have completed numerous research methods training courses and workshops. However, my experience of publishing papers and articles in international journals (Please refer to Appendix C for details) has helped me to truly understand and implement the various research techniques and methodologies I had previously learned about (Appendix G: A1, A2, B1, B4, C1, C2, C3, C4).

My publication experience has helped to expand my thinking in terms of working with very different types of data and information to what I had been used to previously. I gained familiarity with social science research techniques which was a completely new area for me. The idea of conducting interviews and administering questionnaires to gather data was an interesting experience and a new way of gathering data for me. I was able to appreciate the theory and practice of different research methodologies. I also acquired important skills in qualitative and quantitative research methodologies and learnt to use various software packages for data analysis and presentation (Appendix G: A2, B1, B2, C1).

The journal publications have also helped to develop my divergent thinking skills in terms of understanding and working with different types of data and the ways in which the resulting data can be analysed and synthesised to make sense of emerging theory. I gained important insights into my own behaviour as a researcher and how some of my own biases could influence the data (Appendix G: B2, C1).

The research papers and articles have given me an opportunity to conduct research into various network and information security related areas in significant depth. The opportunity to carry out a detailed literature review for each paper not only enhanced my subject specific knowledge but also helped me to develop critical awareness of the subject and the ability to construct persuasive arguments supported by empirical evidence (Appendix G: A1, A2, B1, B3, C1, C2, C3).

Most of the papers that I have published have been through close collaboration with colleagues working in academia and industry. This has typically involved a great deal of group discussions on various information security related issues. This gave me an opportunity to exchange ideas with other group members and receive critical peer review of my work. It has been a really interesting and useful experience to participate in such lively group discussions. I was able to put forward my own perspective based on many years of industrial experience. The overall experience and personal reflection helped me to analyse my own behaviour, motivations, and personal values. It also gave me a sense of belonging and professionalism in my field and useful insights into the dynamics of my community of practice. The experience also helped me to appreciate how as a member of this community, my ideas can make an impact and help to bridge the gap in my own academic and professional knowledge and understanding (Appendix G: B2, B4, C3, C4).

To date, two of my publications have been cited in reputable journals, giving me an encouraging indication of the relevance and impact of my work. As in the case of my book publication, I believe that I have been able to develop and present my own unique perspective in my publications based on a rich mix of academic and industrial experience. In all of my publications to date, I have sought to relate my research findings to current industry practices in order to further enhance understanding of the relevant issues (Appendix G: B3, C2).

A significant portion of my research and publications have been based on a quantitative research paradigm, generally focusing on controlling and predicting phenomena through experimental studies and statistical analysis. Since this approach has its roots in positivism, the researcher is regarded as being entirely independent from the participants and the phenomena being studied (Creswell, 1998).

However, a number of my recent publications have been based on a qualitative research paradigm. In particular my paper entitled 'ICT Students' Stress and its Coping Strategies' employed a phenomenological research approach to explore the emotions, attitudes, and perceptions of the participants. This has also coincided with a shift in focus in my professional practice from a technical approach to one that is more socio-technical in nature. The use of qualitative research has been necessary in this context in order to probe deep into the subjective qualities governing human behaviour and to enhance my understanding of various issues in the field of information security.

My experience with qualitative research has helped me to understand that as a researcher my own emotions and experiences can sometimes have a positive role to play and provide valuable knowledge and insights into a topic. In the context of my DProf research project, I fit the profile of both a researcher and a participant. My DProf research is likely to involve close involvement with the research participants in a way that it may not be possible for me to cast aside my own views, biases, and perceptions. I feel that I will need to exercise extreme caution in making key decisions in order to manage the risks involved in this type of research (Appendix G: A2, A3, B2, C1).

My publication experience has also helped me develop my leadership and project management skills (Appendix G: C3, C4). My previous project management experience from industry had been predominantly in team environments. However, much of the research work has been largely self-driven and has required me to be self-sufficient and be able to organise and manage my time very effectively. This experience will no doubt provide me with a strong foundation to build and develop my DProf research project.

2.3. Advanced Learning and Experience Gained Through Writing and Delivering Information Security Course (RAL Case 3)

Overview

In this role, I worked for a consultancy firm specialising in information security and communications technologies. I was involved in the provision of consultancy and training services to a number of large corporate clients. This role proved to be a very steep learning curve as I had the opportunity to work with some of the leading-edge technologies in the field and gained invaluable professional experience working with high profile corporate customers on large scale international projects.

I was responsible for the delivery of a number of bespoke data communications and information security courses for major corporate clients. A major aspect of this role was the design and development of specialist information security courses. I also revised a number of existing courses to incorporate practical and industrially relevant lab exercises and simulations which was hugely appreciated by the delegates attending the courses.

I designed and developed an information security course (Please refer to Appendices D, E & F) that focused on the fundamental principles and practices of information security and was complimented by practical hands-on lab exercises to provide security professionals with a comprehensive introduction to this area. This course was part of a series of courses in information security and thus laid the foundation for the later more advanced courses. This course has undergone numerous revisions since it was first developed, and I continue to teach this course in various customised forms.

Case Evaluation & Reflections

This course was aimed at senior information security professionals and managers as well as communications engineering graduates looking to specialise in the field of information security. There were approximately 110 delegates who participated in this course from 2002 to present (Please refer to Appendix F). I further developed and customised this course as a standalone module that I delivered to postgraduate students at a university over the period of one semester in 2008/2009 (Appendix G: A1, B1, B3, C2, C3).

The primary focus of the course was the principles and practices of information security in the context of secure network communications. It focused on the evaluation of potential threats to an organisation's network. One of the key themes of the course was the psychological and societal aspects of information security, probing into the mind of the intruder and identifying their characteristics and motives.

Since the development of this course, I believe that the nature of the information security threat has changed substantially. The huge advances in intrusion detection and prevention technology have meant that the outsider threats to an organisation's network can be significantly contained. Today, a large proportion of security threats to organisations come from users and employees who are not trained on computers or are not aware of various computer security threats. There is an ever-increasing number of people that are connected to the Internet and engaging with modern technologies without any formal training or awareness of the associated security risks (Appendix G: B2, C1).

The development of this course was largely an individual effort and required me to organise myself and manage a lot of information and tasks in an effective way for successful completion. I learnt to manage my time and commitments effectively. Although, I found this challenging at times, the overall experience was very rewarding and extremely satisfying (Appendix G: C2, C4).

I worked closely with senior management and clients at all stages of the course development in order to ensure that client requirements were properly addressed. This role required substantial project management skills as well as helping me to further develop my team leadership skills. I learnt how to manage people and delegate tasks effectively. I learnt the importance of having a vision of where to go and being able to articulate it effectively to others. I developed excellent communication and problem-solving skills and the ability to work under pressure to meet deadlines (Appendix G: B3, C3).

There were also other broader learning opportunities to extend my knowledge and skills as part of this project. Due to the limited time available for this course it was crucial for the success of the project to be able to build a good rapport with stakeholders and gain their confidence. This gave me the opportunity to further develop my negotiation and influencing skills. However, I was also quite conscious of potential sources of bias that could be introduced into the project as a result of my actions. I found myself continuously assessing my behaviour and adjusting my approach accordingly during negotiations with clients and senior management. This way of working also helped me to develop a more reflective way of thinking about myself and the project work (Appendix G: A3, B2, C1).

I gained valuable insights into the skills required to provide strategic leadership. The ability to communicate, inspire and manage people effectively at this level was an important skill that I was able to further develop. This was also an extremely useful period in terms of my personal and professional development. I learnt a great deal about personal influence, charisma and importance of negotiation skills. I also had the opportunity to attend formal training and professional development courses during this period. The latter gave me more confidence in dealing with new and challenging situations as well as being able to manage pressure more effectively. I am confident that I will be able to draw on all of this useful experience to successfully complete my DProf project.

Section 3

3.1. Moving Towards My DProf Project

A number of major studies [PWC, 2012; Deloitte, 2011: Ernst & Young, 2012 & Sasse et al, 2007] in the recent past have shown that an overwhelming percentage of information security breaches are caused by human factors. Depending on the nature of the industry, security breaches could result in catastrophic losses. Consequently, the human element cannot be ignored in any organisational security risk analysis.

Information security is ultimately about people. Much of the research into how attackers manage to compromise IT systems clearly illustrates that the human element is always crucial to the majority of successful attacks (Colwill, 2009). The information security research community has recognised that human behaviour has a crucial role in many security failures and has frequently called for the human factors to be considered in the design and implementation of security in IT systems (Sasse et al, 2007).

There are many different reasons for the security breaches resulting from (insider) human factors, including carelessness, lack of effective and strict security policies and inadequate user training and awareness (Eminagaoglu et al, 2009). Although technical solutions are very important, unfortunately, they do not address the ignorance or omission on the part of the people using IT systems.

Much of the research [Wilson et al, 2009; ENISA, 2010; ISO/IEC27001:2005, 2005] into information security standards and best practices identifies information security training and awareness as a form of management control intended to achieve prevention and mitigation of security breaches and is regarded as a key contributor to achieving optimum security. My own personal experience of more than fifteen years in the Computer Communications and Information Security industry has taught me that the security of an organisation is very much dependent on the knowledge and awareness of the end users and those who manage them. As such information security training and awareness provide a very crucial layer of protection against security attacks and breaches.

Although information security training and awareness programmes have long been promoted as being fundamental to information security practice, the effectiveness of such programmes is a topic that is often debated, especially so because there is little empirical evidence to support the link between awareness and effectiveness. Instead, an intuitive assumption is generally made that increased awareness leads to a security-enhancing change in user behaviour (Bock-Brown, 2004).

My DProf research aims to gain a better understanding of the issues involved and propose a framework to improve the effectiveness of information security education and awareness programmes in order to achieve active participation and behavioural change at an individual and organisational level towards the acceptance and compliance of information security policies.

I have chosen to pursue this area for my DProf research project as I believe it will allow me to attain the knowledge and experience I need to make a personal contribution to the field of Computer Communications Engineering and Information Security.

3.2. Conclusions

In my professional practice to date, I have been very fortunate to have had the opportunity to work in both academia and industry. This has benefitted me hugely over the years and has stretched the frontiers of my knowledge and experience. This experience has also tremendously helped in developing me intellectually and improving my analytical skills and divergent thinking.

In reflecting on my previous learning, my experience of conducting independent research has been very rewarding and has helped me to acquire some invaluable skills for a research career. It has given me the confidence to publish my book and other work in international peer reviewed journals. The research experience so far has greatly boosted my confidence. I believe that my academic qualifications to date combined with my extensive commercial experience has helped me tremendously in developing essential strategies, skills and qualities needed to pursue DProf research in my chosen area of information security.

I strongly believe that my research and publication skills and experience will help me immensely in writing my DProf research project. I recognise that there are areas of weakness in my learning and development that require attention. In particular, I feel that I need to work on my critical analysis skills as well as learning through reflection on past experiences.

The above attributes, together with the knowledge, skills and expertise I have developed over the past 15 years in computer communications engineering and information security, will strengthen my approach to undertaking the DProf research project.

As far as my future interests and expectations are concerned, I believe that the DProf will provide me the next step in my learning. This is also an opportunity for me to improve my scholarly abilities and skills both academically and professionally.

I feel privileged and excited at the same time to be able to bring to the programme my own mix of skills and experience to work with in order to develop my research and have the opportunity to make a positive contribution to my community of practice.

I believe that the rigorous and challenging process of undertaking a DProf will give me a competitive edge and greatly improve my career prospects. It will also give me the opportunity to further develop myself and play a strategic thought leadership role in my chosen area of information security research.

Appendix A: Book Publication

L. Sharif & M. Ahmed (2010), "IPSec: A Practical Approach: Network Security", LAP Lambert Academic Publishing Co, Germany, August 2010. ISBN-13: 978-3838395968

This book explores advanced IPSec algorithms and protocols for IP version 4 communications from a practical point of view. The architecture of the IPSec protocol framework is discussed and a detailed critical evaluation of component protocols such as Authentication Header (AH), Encapsulating Security Payload (ESP) and Internet Key Exchange (IKE) is provided. The various encryption and integrity-checking mechanisms used by IPSec are evaluated. A detailed packet-by-packet analysis of IKE protocol transactions in IPSec is also provided. A practical implementation using Cisco IOS router platform evaluates how the various IPSec protocols and standards could be combined to create a robust and functional Virtual Private Network (VPN). Various command line tools within the Cisco IOS are used to test and decompose the configuration to provide an in-depth analysis of the role of individual component protocols. Various Internet drafts and Requests for Comments (RFCs) from the Internet Engineering Task Force (IETF) are evaluated to identify the major limitations in the IPSec standard.

Appendix B: Table of Contents for IPSec Book - A Practical Approach: Network Security

ABOUT THE AUTHORS

TABLE OF FIGURES

PREFACE

ACKNOWLEDGEMENTS

CHAPTER 1: INTRODUCTION

CHAPTER 2: VIRTUAL PRIVATE NETWORKS

2.1 VIRTUAL PRIVATE NETWORK EVOLUTION

2.2 COMPARISON OF VPN TECHNOLOGIES

- Point-to-Point Tunnelling Protocol (PPTP)
- Layer 2 Forwarding (L2F)
- Layer 2 Tunnelling Protocol (L2TP)
- IP Encapsulation Within IP (IP-In-IP)
- Generic Routing Encapsulation (GRE)
- Multi-Protocol Label Switching (MPLS)
- IP Security (IPSec)

CHAPTER 3: TCP/IP OVERVIEW

3.1 TCP/IP LAYERS

3.2 INTERNET PROTOCOL VERSION 4 (IP V4)

3.3 IP ADDRESSING

3.4 SECURITY – AT WHICH LAYER?

- Application Layer
- Transport Layer
- Network Layer
- Data Link Layer

CHAPTER 4: IPSEC OVERVIEW

4.1 THE NEED FOR SECURITY

4.2 VPN OVERVIEW

4.3 VPN CATEGORIES

- Remote Access VPNs
- Intranet VPNs
- Extranet VPNs

4.4 WHY IPSEC?

4.5 THE IPSEC PROTOCOLS

- Authentication Header (AH)
- Encapsulating Security Payload (ESP)
- Packet Encapsulation in IPSec
- Transport Mode
- Tunnel Mode
- IKE Overview

4.6 SECURITY ASSOCIATIONS (SA)

CHAPTER 6: IPSEC NEGOTIATIONS USING THE IKE PROTOCOL

6.1 MAIN MODE USING PRE-SHARED KEY AUTHENTICATION FOLLOWED BY QUICK-MODE NEGOTIATION

- IKE Phase 1 (Main Mode): Sending Message 1
- IKE Phase 1 (Main Mode): Sending Message 2
- IKE Phase 1 (Main Mode): Sending Message 3
- IKE Phase 1 (Main Mode): Sending Message 4
- IKE Phase 1 (Main Mode): Sending Message 5
- IKE Phase 1 (Main Mode): Sending Message 6
- IKE Phase 2 (Quick Mode): Sending Message 1
- IKE Phase 2 (Quick Mode): Sending Message 2
- IKE Phase 2 (Quick Mode): Sending Message 3

CHAPTER 7: IPSEC IMPLEMENTATION

7.1 COMBINING IPSEC PROTOCOLS TO CREATE A VPN

7.2 IPSEC VPN PRE-CONFIGURATION STEPS

7.3 HOW IPSEC VPNS ARE ESTABLISHED

7.4 CISCO IOS IPSEC CONFIGURATION OVERVIEW

- Determine Security Requirements
- Configure IKE And Create IKE/ISAKMP Policies
- Configure IKE/ISAKMP Policies
- Configure Transform Sets
- Configure Crypto Access Lists
- Configure Crypto Maps
- Global Lifetimes For IPSec SAs
- Apply Crypto Map Sets To Interfaces
- Testing And Verifying IPSec VPN Configurations
- Testing And Verifying IKE
- Testing and Verifying IPSec

CHAPTER 8: LIMITATIONS OF IPSEC

8.1 IPSEC PEER/KEY MANAGEMENT

8.2 IPSEC INTERACTION WITH MULTICAST TRAFFIC

8.3 IPSEC AND QUALITY OF SERVICE (QOS)

8.4 IPSEC RESOURCE CONSUMPTION

8.5 CONFIGURATION COMPLEXITY

8.6 IPSEC MULTI-VENDOR INTEROPERABILITY PROBLEMS

8.7 LACK OF END-TO-END PROTECTION

8.8 IPSEC INTERACTION WITH FIREWALLS

8.9 IPSEC INTERACTION WITH NAT

- Impact Of NAT On IPSec

CHAPTER 5: ENCRYPTION AND INTEGRITY-CHECKING MECHANISMS IN IPSEC

5.1 MESSAGE ENCRYPTION

- Data Encryption Standard (DES)
- Triple DES (3DES)

5.2 MESSAGE INTEGRITY CHECKING

- HMAC-Message Digest 5 (MD5)
- HMAC-Secure Hash Algorithm-1 (SHA-1)

5.3 PEER AUTHENTICATION MECHANISMS

- Pre-Shared Keys
- RSA Digital Signatures
- RSA Encrypted Nonces

5.4 KEY MANAGEMENT MECHANISMS

- Diffie-Hellman Protocol
- Certificate Authorities (CA)

CHAPTER 9: CONCLUSIONS

APPENDIX A: IMPLEMENTING ROUTER-TO-ROUTER IPSEC VPN USING PRE-SHARED KEYS AS THE AUTHENTICATION MECHANISM

APPENDIX B: TESTING & ANALYSIS OF IPSEC VPN CONFIGURATIONS

APPENDIX C: DIFFIE-HELLMAN ALGORITHM AND NONCE GENERATION

APPENDIX D: IKE / IPSEC COMMAND REFERENCE

APPENDIX E: TECHNICAL SPECIFICATIONS OF ROUTERS

APPENDIX F: IPSEC RELATED RFCS

GLOSSARY

BIBLIOGRAPHY

Appendix C: Papers and Articles in International Journals

M. Ahmed, L. Sharif, M. N. Kabir and M. Al-Maimani (2012), "Human Errors in Information Security", International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE), Vol. 1, No. 3, pp 82-87, July 2012

The target audience of this paper is professionals and stakeholders in charge of securing the assets of their organisations and institutions. This paper starts by providing a brief overview of information security, outlining the main goals and techniques of the discipline. The paper also discusses the role of human factors and how the information security research community has recognised the increasingly crucial role of human behaviour in many security failures. This is followed by a review of up to date literature on human errors in information security.

M. Ahmed, L. Sharif, Y. M. Alginahi and M. N. Kabir (2011), "A Survey of Routing Attacks in Wireless Sensor Networks", Umm Ul Qurra University, Makkah, KSA, Wireless Sensor Networks Meeting, May 18-19, 2011.

The flexibility and rapid deployment characteristics of Wireless Sensor Networks (WSN) offer tremendous potential to provide attractive, low cost solutions to a variety of real world problems. Routing plays a central role in sensor networks and consequently routing security in WSNs is a hugely important area of research. However, providing secure routing in WSNs is a challenging task due to the inherently constrained capabilities of sensor nodes.

One of the many ways that a sensor node might fail is due to a routing attack. A wide variety of routing protocols have been proposed for WSNs; however, most do not take security into account as a main goal. Routing attacks can have devastating effects on WSNs and present a major challenge when designing robust security mechanisms. In this paper, some of the most common routing attacks in WSNs are examined. A variety of countermeasures have been evaluated but most of these countermeasures suffer from flaws which make them unsuitable for use in large scale WSN deployments.

This survey paper makes it evident that it is extremely difficult to utilize existing protocols to provide protection against routing attacks. It is recommended that routing protocols should be designed from scratch where such common attacks can be rendered meaningless.

A. Issa-Salwe, L. Sharif and M. Ahmed (2011), "Strategic Information Systems Planning as the Centre of Information Systems Strategies", International Journal of Research and Reviews in Computer Science (IJRRCS), Vol. 2, No. 1, pp 156-162, March 2011.

Strategic Information Systems Planning (SISP) has been a theme of considerable importance to Information Systems (IS) professionals in both the business and academic communities for the last two decades. SISP process is intended to ensure that technology activities are properly aligned with the evolving needs and strategies of the organization. Success can be achieved when an organization can achieve balance between IS and its organizational planning. This paper examines the research on this ever-important topic and focuses on the importance of SISP to IS strategies.

L. Sharif and M. Ahmed (2011), 'An Evaluation of the Digital Britain Report', Trends in Information Management (TRIM), Vol. 7, Issue 1, pp 19-30, Jan-Jun 2011.

The UK government outlined its vision of the future in the "Digital Britain" report published in June 2009. The paper provides an evaluation of the report and offers professional comments with a particular focus on Universal Broadband Access and Next Generation Access (NGA) networks. The paper also provides an overview of the currently available fixed and wireless broadband access technologies in the UK and the main challenges associated with these technologies in terms of migration towards NGA networks. The UK government has often been criticized for its lack of leadership in the provision of adequate broadband access in rural areas. The paper further discusses the government stance with regard to this issue and proposes solutions that could be cost-effectively deployed to extend coverage of broadband access to rural areas. The paper also reviews some of the successful NGA deployments around the world and discusses some of the useful lessons that could be drawn from these examples. A brief summary of some of the social and economic benefits associated with universal broadband access is also provided.

L. Sharif and M. Ahmed (2011), 'Direct Broadcast Satellite (DBS) Television Systems', International Journal of Research and Reviews in Wireless Communications (IJRRWC), Vol. 1, No. 1, pp 1-6, March 2011.

Consumers around the world enjoy digital television from a variety of sources including terrestrial, cable, satellite and broadband Internet broadcast systems. However, it is satellite broadcast systems that have provided consumers real widespread opportunity to enjoy digital television. This paper presents an overview of direct broadcast satellite (DBS) systems used in the delivery of digital television. The key DBS system building blocks are identified including the broadcaster as well as the consumer side of the communication link. This paper also discusses the key technology evolutions that facilitated the introduction of DBS services, the most common services provided through DBS TV technology and the future directions that this technology is likely to take.

L. Sharif and M. Ahmed (2010), "The Wormhole Routing Attack in Wireless Sensor Networks (WSN)", Journal of Information Processing Systems (JIPS), Volume 6, No. 2, pp 177-184, June 2010.

Although there is an array of routing protocols that have been proposed for Wireless Sensor Networks (WSN), most do not consider security as a main goal. In WSNs routing attacks can have devastating effects and present a major challenge when designing robust security mechanisms. This paper examines some of the most common routing attacks in WSNs with a particular focus on the wormhole routing attack. A detailed investigation of the wormhole routing attack and evaluation of some of the proposed countermeasures makes it evident that it is extremely difficult to retrofit existing protocols with defenses against routing attacks. It is suggested that one of the ways to approach this rich field of research problems in WSNs could be to carefully design new routing protocols in which attacks such as wormholes can be rendered meaningless.

M. Ahmed, L. Sharif, A. Issa-Salwe, and A. Alharby (2010), "Information Security: Securing a Network Device with Passwords to Protect Information", Trends in Information Management (TRIM), Vol. 6, Issue 1, pp 62-76, Jan-Jun 2010.

Information security is a complex and critical subject, conventionally only tackled by well-trained and experienced professionals. The importance of an effective password policy at the device level is obvious and often entire networks can be brought down due to the lack of simple password security on a single device. This paper emphasises the need for an effective device-level password security as an essential component of a more comprehensive organisational security policy.

Y. M. Alginahi, M. Ahmed, O. Tayan, A. A. Siddiqi, L. Sharif, A. Alharby and R. Nour (2009), "ICT Students' Stress and its Coping Strategies - English Perspective - A Case Study of Midsize Middle Eastern University", Trends in Information Management, V 5 (2), pp. 111-127, July-Dec 2009.

This study evaluates the perceptions of stress among Information and Communications Technology (ICT) students and their coping strategies in dealing with English as the medium of instruction during their university studies. A semi-structured survey was conducted using a sample of 267 male students of a Computer Science college from a midsize Middle Eastern university. The study also used a phenomenological approach with semi-structured interviews carried out with ten students in order to clarify some of the findings. Since the research topic is based on student's stress perceptions, the phenomenological analysis of student's interviews was an appropriate tool for this study. Phenomenology enables participants to express their feelings about a particular situation or incident in their own point of view which may not be easy to express on a survey. All of students who took part in this study thought that they had been stressed at one time or another due to having English as the medium of instruction without a Preparatory Year English Program (PYEP) before entering ICT courses. 62% of the students maintained that they have had episodes of stress due to the English language during their studies at one time or another. The students use different mechanisms to cope with stress outside the university, including engaging themselves in sports, surfing the web, meditation, hanging out with friends, sleeping or going in to isolation. The students demand interactive English language courses, more leisure time activities on campus, proper guidance in English language courses to ease their ICT studies as well as advisory services and peer counselling on campus to reduce their stress.

Appendix D: Information Security Training Course

Managing Network Security
This course is concerned with the principles and practices of information security with a particular focus on secure network communications. It provides an evaluation of potential threats to an organisation’s network with reference to three main categories of security issues: technology weaknesses, configuration weaknesses and policy weaknesses. The course moves on to look at psychological and societal aspects of information security by getting into the mind of the intruder and identifying their characteristics and motives. The various information security threat types such as denial of service, unauthorized access and data manipulation are also described. There is a strong focus on the design and implementation of a robust network security policy with numerous case studies to illustrate what the policy should contain and how to test the policy using a security audit.

Appendix E: Table of Contents for Information Security Training Course

Managing Network Security

Course Introduction

Module 1: Identifying Network Security Threats

- Network Security Issues
- Know Your Enemies
- The Human Element in Security
- Types of Security Threats

Module 2: AAA Security

- Overview of Authentication Methods
- TACACS+ & RADIUS

Module 3: Introduction to Cisco PIX Firewall

- PIX Firewall For AAA Security
- Network Address Translation (NAT) with PIX
- PIX Firewall Advanced Features

Module 4: Perimeter Router Security

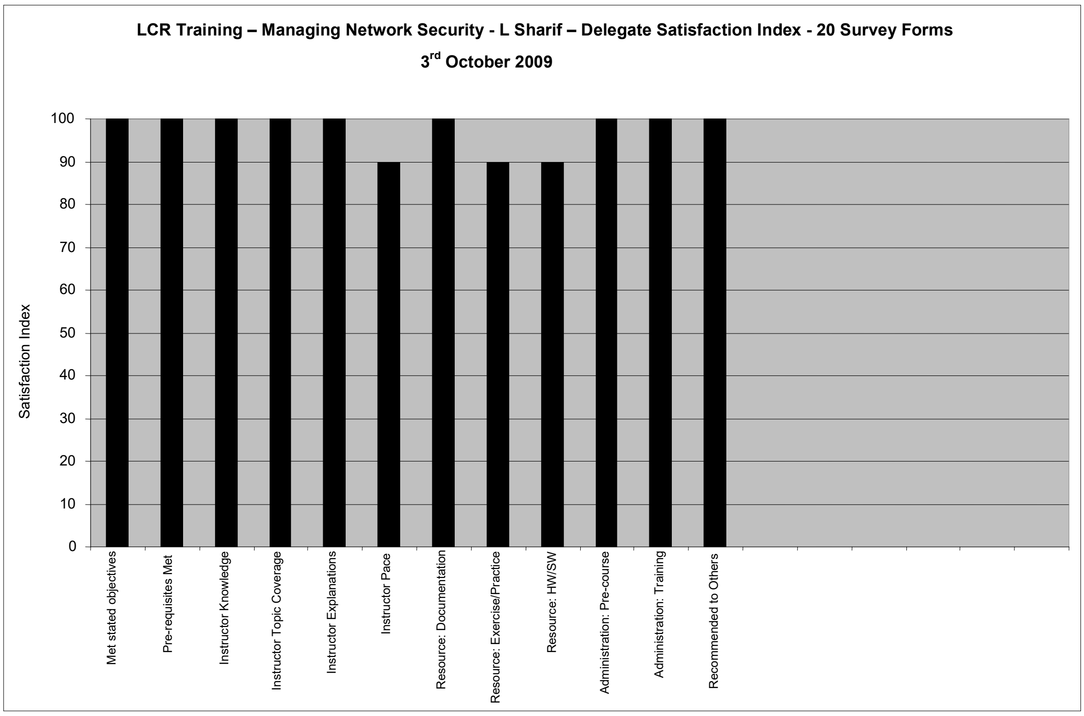
Module 5: Context-Based Access Control (CBAC)

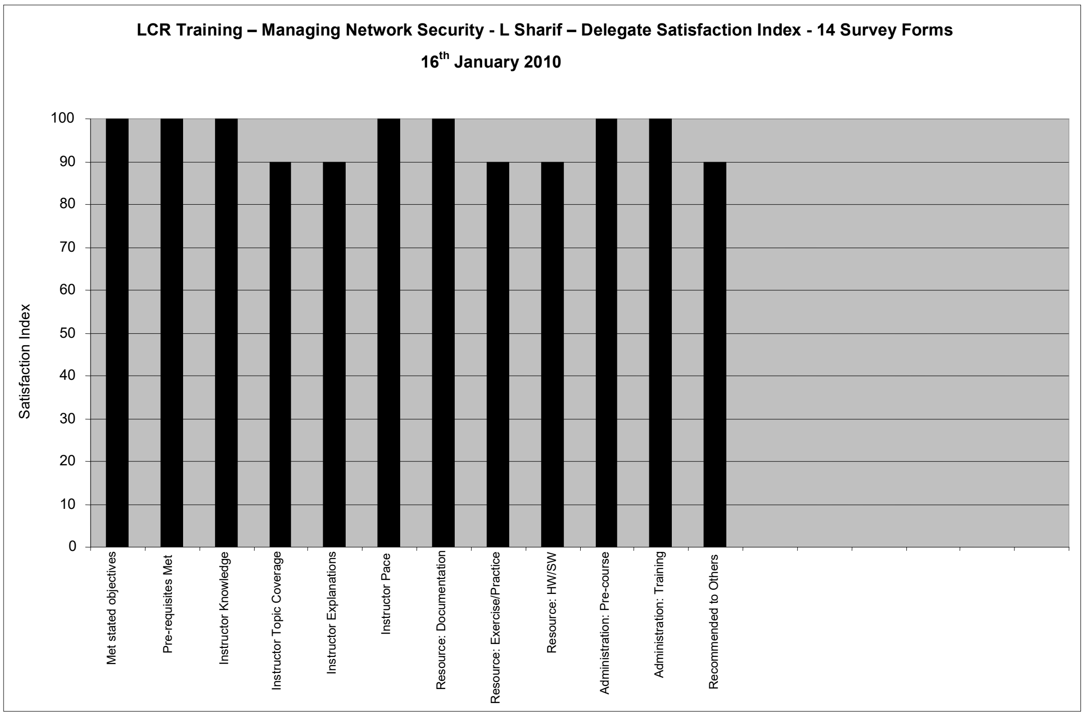
Module 6: Firewall Intrusion Detection System (IDS)

Module 7: Managing the Human Factor in Information Security

Lab Manual

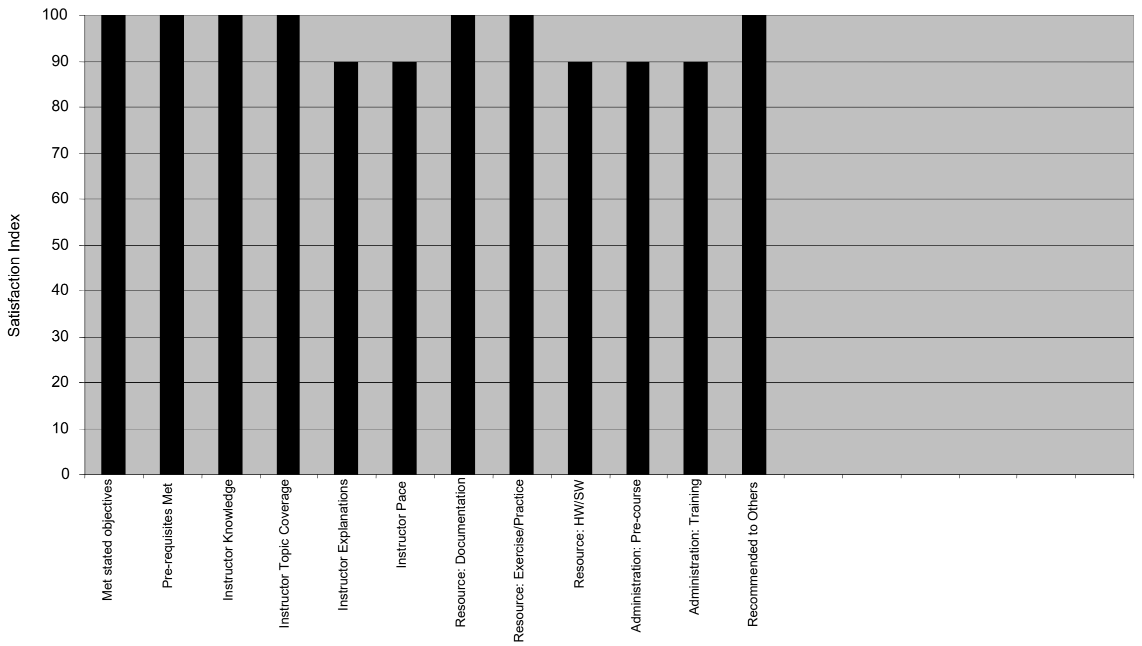
Appendix F: Quality Assurance Surveys for Information Security Training Course





LCR Training – Managing Network Security - L Sharif – Delegate Satisfaction Index - 16 Survey Forms

10th July 2010



Appendix G: Learning Outcomes and Assessment Criteria for DPS5120

A1	**Knowledge**	Evidence that the candidate has depth and range of knowledge in a complex area and is currently working at the leading edge of practice underpinned by theoretical understanding.
A2	**Research and development capability**	Demonstrates effective and critical selection, combination and use of research and development methods; can develop new approaches in new situations and contribute to the development of practice-based research methodology.
A3	**Ethical understanding**	Demonstrates awareness of ethical dilemmas and conflicting values which may arise in professional practice and work situations; able to formulate solutions in dialogue with superiors, peers, clients, mentors and others.
B1	**Analysis and synthesis**	Demonstrates ability to analyse and synthesise complex and possibly conflicting ideas and information in order to redefine knowledge and develop new approaches.
B2	**Self-appraisal/reflection on practice**	Provides evidence of work with 'critical communities' through whom a new or modified paradigm is being established. Habitually reflects on own and others practice so that self-appraisal and reflective inquiry are intertwined, thereby improving the candidate's own and others’ action.
B3	**Planning/management of learning**	Is autonomous in management of own learning; makes professional use of others in support of self-directed learning and is fully aware of political implications of the study.
B4	**Evaluation**	Can independently evaluate/argue a complex position concerning alternative approaches; can accurately assess/report on own and others work; can critique and justify evaluations as constituting bases for improvement in practice.
C1	**Awareness of operational context and application of learning**	Can take into account complex, unpredictable, specialised work contexts requiring innovative approaches, which involve exploring current limits of knowledge and, in particular, interdisciplinary approaches and understanding. Is able to translate and disseminate theoretical knowledge into workable frameworks and/or models for practice.
C2	**Use of resources**	Effective use of resources is wide ranging, complex and is likely to impact upon the work of others.
C3	**Communication/presentation skills**	Can engage in full professional and academic communication with others in their field and place of work; can give papers/presentations to 'critical communities' for developmental purposes.
C4	**Responsibility and leadership**	Autonomy within bounds of professional practice with high level of responsibility for self and others. Ability to provide leadership as appropriate.

References

Bock-Brown, J. (2004) *Human aspects of information assurance*, Information security group. Royal Holloway, University of London.

Colwill, C. (2009). 'Human factors in information security: The insider threat: Who can you trust these days?', *Information Security Technical Report*, Vol.14, No.4, pp.186 - 196

Creswell, J.W. (1998) *Qualitative inquiry and research design: choosing among five traditions*. Thousand Oaks, CA: Sage.

Deloitte (2011) *Raising the bar: 2011 TMT global security study - Key findings*

Eminagaoglu, M. Uçar, E. and Eren, S. (2009) 'The positive outcomes of information security awareness training in companies: A case study', *Information Security Technical Report*, Vol. 14, pp.223-229

ENISA. (2010) 'How to raise information security awareness', *European Network and Information Security Agency*

Ernst & Young (2012) *Global information security survey: Fighting to close the gap. Insights on IT risk*

ISO/IEC 27001:2005. (2005). *International Standards Organisation. Information Security Management System – Requirements*

McIlwraith, A. (2006) *Information security and employee behaviour: How to reduce risk through employee education, training and awareness*. Gower Publishing

Parsons, K. McCormac, A. Butavicius, M. and Ferguson, L. (2010) 'Human factors and information security: Individual, culture and security environment', *Command, Control, Communications and Intelligence Division*, Defence Science and Technology Organisation, DSTO-TR-2484, Department of Defence, Australian Government

PWC (2012) *Information security breaches survey - Technical report*. PriceWaterhouseCoopers.

Sasse, M.A. Ashenden, D. Lawrence, D. Coles-Kemp, L. Fléchais, I. and Kearney, P. (2007) 'Human vulnerabilities in security systems', *Human Factors Working Group White Paper, Cyber Security Knowledge Transfer Networks*.

Stallings, W. (2010) *Network security essentials: Applications and standards*, Fourth Edition. Prentice Hall.

Wilson, M. Stine, K. and Bowen, P. (2009) 'Information security training requirements: A role- and performance-based model', *Recommendations of the National Institute of Standards and Technology, NIST Special Publication,* 800-16