A Framework to Mitigate Phishing Threats

Edwin Donald Frauenstein

A Framework to Mitigate Phishing Threats

by

Edwin Donald Frauenstein

Dissertation

submitted in fulfilment of the requirements for the degree of Magister of Technologiae

in

Information Technology

in the

Faculty of Engineering, the Built Environment and Information Technology

of the

Nelson Mandela Metropolitan University

Supervisor: Prof. Rossouw von Solms

Co-supervisor: Prof. Kerry-Lynn Thomson

January 2013

ABSTRACT

We live today in the information age with users being able to access and share information freely by using both personal computers and their handheld devices. This, in turn, has been made possible by the Internet. However, this poses security risks as attempts are made to use this same environment in order to compromise the confidentiality, integrity and availability of information. Accordingly, there is an urgent need for users and organisations to protect their information resources from agents posing a security threat.

Organisations typically spend large amounts of money as well as dedicating resources to improve their technological defences against general security threats. However, the agents posing these threats are adopting social engineering techniques in order to bypass the technical measures which organisations are putting in place. These social engineering techniques are often effective because they target human behaviour, something which the majority of researchers believe is a far easier alternative than hacking information systems. As such, phishing effectively makes use of a combination of social engineering techniques which involve crafty technical emails and website designs which gain the trust of their victims.

Within an organisational context, there are a number of areas which phishers exploit. These areas include human factors, organisational aspects and technological controls. Ironically, these same areas serve simultaneously as security measures against phishing attacks. However, each of these three areas mentioned above are characterised by gaps which arise as a result of human involvement. As a result, the current approach to mitigating phishing threats comprises a single-layer defence model only. However, this study proposes a holistic model which integrates each of these three areas by strengthening the human element in each of these areas by means of a security awareness, training and education programme.

DECLARATION

I, **Edwin Donald Frauenstein**, hereby declare that:

- The work in this dissertation is my own work.
- All sources used or referred to have been documented and acknowledged.
- This dissertation has not previously been submitted in either full or partial fulfilment of the requirements for an equivalent or higher qualification at any other recognised educational institution.

_____

Edwin Donald Frauenstein

2013

ACKNOWLEDGEMENTS

Firstly, I would like to thank Professor Rossouw von Solms for his guidance, valuable insight and support during the course of this dissertation. I would also like to thank him for providing me with the exposure and experience which enabled me to present research papers at conferences, both locally and internationally. You have inspired me to continue with my research career.

I would like to thank the Nelson Mandela Metropolitan University (NMMU) for providing the necessary funding and support for research related activities.

Thank you also to my parents for encouraging me and supporting me throughout the years.

In addition, I would like to thank my colleagues at Walter Sisulu University (WSU) for supporting me emotionally and encouraging me over the years with this project.

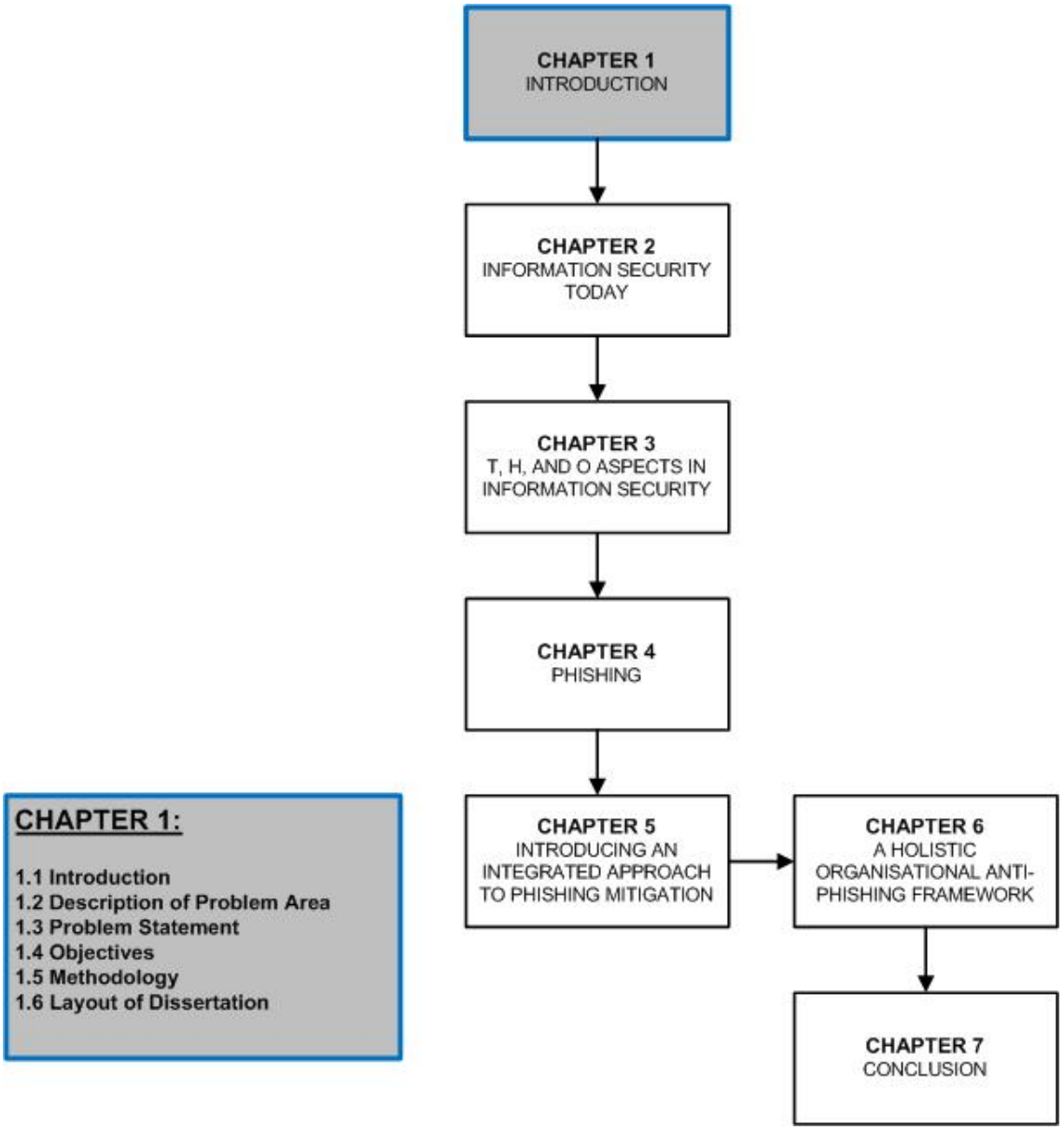
Finally, I would like to thank the following people for their contribution to this study:
Thomas Monk for correcting some of my earlier literature chapters
Alexa Barnby for her professional proofreading of this dissertation
Sean Allam, Morne Owen and Daryan Rowe who participated in the interviews.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1
INTRODUCTION



1.1 Introduction

This chapter aims to provide a synopsis of the study. The chapter presents the problem area of the study, the problem statement, the research objectives, the research methods and design and, finally, the outline of the dissertation.

1.2 Description of Problem Area

The world in which we live today has changed radically compared to a few decades ago. Using current computer devices, information is now literally at our fingertips. To a large extent this has been made possible by the Internet. Using Internet search engines it is now possible to find the information available on virtually any topic in an instant, instead of having to search physically through books in a library. There are also no longer any geographical barriers to communication with individuals, as commonly used technologies such as email, social networks, streaming video and instant messengers have made this possible. In addition, the members of the general population now rely on using their sophisticated smart phones to access and share information. In other words, the world as we once knew it has, metaphorically speaking, been reduced to the size of one's computer monitor or mobile phone screen. This transformation has resulted in what is now known as the Information or Digital Age. Instead of information being made available in paper-based format (e.g. books, newspapers) only, it is now in an electronic format that may be stored and transferred using computer technology. Provided that there is an Internet connection, it is now possible to access information easily and at any given time. Unfortunately, this access to information has had undesirable consequences with threat agents making use of the opportunity to steal information from individuals. Thus, this has, in turn, increased the need to secure information and computer systems against threat agents - information security.

Information security involves protecting information against a wide variety of threat agents in order to both minimise risk and ensure business continuity (ISO/IEC 27002, 2005, p. viii). Today, most organisations use computer systems to exchange sensitive information. This information is regarded as an organisational asset. As such, individuals, organisations and governments depend largely on information

being embedded in secure, private and trustworthy information technology (IT) infrastructures (DACS, 2008).

There are several types of agents who pose security threats to information. Threat agents may be classified into human threat agents and natural disasters (Microsoft, 1999). However, the human threat is the most dangerous of these threats as the motives behind these threats are usually malicious, for example, denying services involving IT, stealing information and damaging information. In order to do this threat agents use means such as viruses, social engineering techniques, malware attacks, hacking and phishing (Microsoft, 1999). On the other hand, in order to secure information against these attacks, organisations usually apply technological controls and have security policies in place (Microsoft, 1999). However, this study attests that it is not possible for these controls alone to avert information security threats, especially phishing.

Apart from the common procedure of hacking, **phishing** represents an alternative way of gaining unauthorised access to information. There is significant evidence in the literature to substantiate the claim that phishing is a burgeoning problem in industry (Sophos, 2005; Litan, 2006). In view of the fact that there are no boundaries to the Internet, phishing may affect all users who are connected to the Internet, as well as posing a constant threat that may affect every individual within an organisation (Ohaya, 2006; Orgill, Romney, Bailey, & Orgill, 2004; Pickworth, 2009; Safecode, 2008; Threat Insight Quarterly, 2005). Organisations and their customers have lost millions of dollars as a result of phishing. The power of phishing lies in its ability to circumvent technological defences because it exploits human behaviour and knowledge. Dhamija, Tygar and Hearst (2006) believe that users generally have great difficulty in distinguishing legitimate websites from spoofed websites. However, despite this, organisations continue to focus primarily on securing their computer systems using technological controls and, thus, neglecting the human element.

Typically, phishing involves a fraudster who uses social engineering techniques in the context of an email message in order to steal confidential information from a user by imitating as a legitimate entity (Kumaraguru, Rhee, Sheng, Hasan, Acquisti, Cranor, & Hong, 2007). These types of fraudsters are referred to as phishers. Most of the organisations cited in such emails are well-known financial institutions.

Phishing is at its most effective using the email because the email message may be made to appear authentic through the use of the corporate logos and terminology typical of the institution from which the email is purported to originate. Typically, phishers use a fabricated story to convince their victims either to resolve a particular problem or to claim a substantial prize. The user is usually also required to complete this process by clicking on a hyperlink contained within the email. This hyperlink then directs the user to a spoofed website which requires the victim to log in using personal information (e.g. username, password, account number). The user believes that the spoofed website is genuine because it looks almost identical to the actual website. However, unbeknownst to the user, the spoofed website records his/her personal information which will then be used by the phisher for the phisher's own ends. Chapter 4 discusses phishing in more detail.

Individuals are placing both themselves and organisations at risk mainly as a result of a lack of knowledge of information security practices, as well as a lack of knowledge about the possible consequences of their actions and behaviour. It would appear that the cultures in several organisations encourage users to rely primarily on technology in order to prevent phishing attacks when, in fact, technology is only a part of the solution to resolving the problem. There are numerous factors that may possibly contribute to a successful phishing attack, including weak organisational policies, negligent human behaviour and inadequate technology-related controls. This study broadly categorises these factors as human factors, organisational aspects and technological controls (HOT). Many literary sources have emphasised that it is the human factors that comprise the greatest security risk and that this is the result of a lack in user education (Jakobsson, 2007; Kumaraguru et al., 2007; Kumaraguru et al, 2009; Ohaya, 2006; Orgill et al, 2004; Robila & Ragucci, 2006; Sheng, Magnien, Kumaraguru, Acquisti, Cranor, Hong, & Nunge, 2007; Van der Merwe, Loock, & Dabrowski, 2005a).

In view of the fact people are considered to be the weakest link in security, they are usually the target of social engineering attacks (Orgill et al., 2004). Another concern is that the attack methods and the tools used by phishers are constantly changing as technology evolves, with each new threat contributing to the difficulty of securing an information system. Since phishers make effective use of technology in order to trick their victims, it may be argued that a user's lack of knowledge regarding the secure

use of technology further adds to the difficulty of protecting users. In addition, users and organisations may not even be aware of the dangers that phishing presents or how to identify these threats, despite the numerous literature studies that may educate users on how to do this (Alsaid, 2006; Bergholz, 2009; Drake, Oliver, & Koontz, 2004; Fette, Sadeh, & Tomasic, 2007; Garera, Provos, Chew, & Rubin, 2007; Krammer, 2006; Patel, 2007).

1.3 Problem Statement

It is evident, in view of the brief background presented in the previous section, that there are numerous dangers and consequences which may arise from phishing attacks. In addition, the previous section also discussed those areas which phishing exploits. Phishing poses an increasing security threat to the information of both individuals and organisations. Organisations are usually affected financially by these attacks.

A cyber security study conducted by Deloitte revealed that chief information security officers (CISOs) are of the opinion that phishing and pharming currently pose the highest cyber security threat to their organisations (Deloitte, 2012). However, the concern is that organisations are not necessarily implementing a holistic anti-phishing approach to mitigate the risk posed by phishers, as organisations typically follow a single-layer approach by focusing primarily on technology controls, educating humans or implementing a security policy. However, despite the fact that organisations may have such measures in place, all these require both human cooperation and knowledge, as humans are usually involved in each of them. However, employees may either ignore security policies or they may be unaware of them, while technological controls may not be managed and/or used correctly by the different users. In addition, the organisation (i.e. management) may not perceive the importance of information security or even understand security risks. This, in turn, creates an opportunity for phishing to exploit any of these vulnerabilities.

1.4 Objectives

The primary objective of this research study is to create a holistic anti-phishing framework to help protect organisations against phishing attacks. This study categorises security controls into human, organisational and technological

dimensions (HOT). It would be ideal to address each of these dimensions in a holistic manner and not in isolation. This may be addressed by means of an educational intervention as it is essential that all the users in an organisation are educated in each of these areas so as to launch a multi-layered defence approach. The anticipated framework should form a stronger layer of defence against phishing attacks as compared to the current single-layer model. In order to achieve the primary research objective, it is necessary to address a number of secondary research objectives. These objectives include the following:

- Identify, through literature, those areas that phishing threat agents exploit.
- Identify current protection measures that have been put in place by organisations to guard against phishing attacks.
- Identify the major elements that should play a role in protecting organisations against phishing attacks.
- Identify any weakness in these major elements.
- Identify, through a literature review, how to integrate these elements into a single holistic approach.

1.5 Methodology

The methodology used in this dissertation includes several research methods. Much of the content of the framework devised in the study was derived from the literature studied. Accordingly, this section will describe this particular process. Initially, an extensive literature review was conducted in order to gain an understanding of information security. Following this, a comprehensive investigation into relevant literature was undertaken in order to ascertain the current state of phishing.

Identifying Relevant Literature

In order to assist in identifying source material for a literature review, Webster and Watson (2002) recommend the use of a systematic structured approach. They maintain that the major contributions to a particular research area are most likely to be found in *leading journals***.** Journal databases may accelerate the identification of relevant articles. The majority of the literature used in this study comprised journal

articles. With the Association for Computing Machinery (ACM) journal as a starting point, several research articles relating to the information security discipline were studied. Conference proceedings were also studied as they have a reputation for quality. Other journal papers from IEEE Explore, Emerald etc. were also used in the study while certain papers were indexed through specialised search engines, for example, Google Scholar, Emerald, NEXUS and ISI Web of Knowledge.

Webster and Watson (2002) recommend that researchers should work backwards by reviewing the citations of articles that have been identified from the leading journals. Thus, following this recommendation, it emerged in this research study that particular writers are regularly cited in papers. This, in turn, helped to ensure that relevant literature was not unintentionally excluded. Ultimately, when the researcher reaches a point where he/she is not finding any new concepts in a particular area of research, this may serve as an indication that the literature review is nearing completion (Webster & Watson, 2002).

Organising the Literature Studied

Webster and Watson (2002) maintain that a *concept-centric* approach will determine the structuring and organisation of the framework of the literature review. In contrast, certain researchers adopt an *author-centric* approach and present a summary of the relevant articles. However, Webster and Watson (2002) argue that the author-centric approach fails to synthesise the literature studied and they recommend that, in order to make the transition from author-centric to the more suitable *concept-centric* approach, researchers should compile a concept matrix of the articles that have been read. Furthermore, they recommend synthesising the literature studied by discussing each concept which has been identified with units of analysis. In this research study, the concept-centric approach was used mainly in terms of organising the content related to the areas of human, organisational and technological controls in the literature on information security.

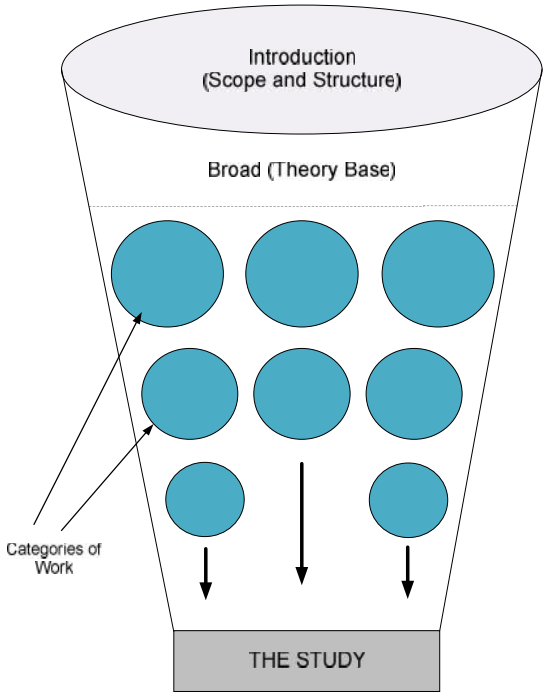


Figure 1.1: The funnel method of structuring a literature review (adapted from Hofstee 2006, p. 96)

Hofstee (2006) recommends using the "funnel" method when structuring a literature review (Fig. 1.1). In order to do this, work may be either grouped or categorised according to commonality. This work includes articles, books or any type of secondary source. This approach is extremely useful when reviewing extensive numbers of articles. In Figure 1.1, as mentioned, the categories of work (balls/circles) that were identified for this specific research project included journal articles, conference proceedings, books and web-based articles. The funnel method was used to identify the problem of phishing that exists in the research area of information security. Thus, it was essential first to understand key concepts in the information security literature before further "funnelling" into phishing. By working backward, as recommended by Webster and Watson (2002), it emerged that phishing is a technique of social engineering.

Figure 1.2 below illustrates the systematic process that was adopted in identifying and organising the relevant literature. Information security literature was initially investigated as the broad research area. It emerged that social engineering

techniques were effective techniques which may be used to acquire information from individuals. Thus, phishing was identified as a sub-component of social engineering.

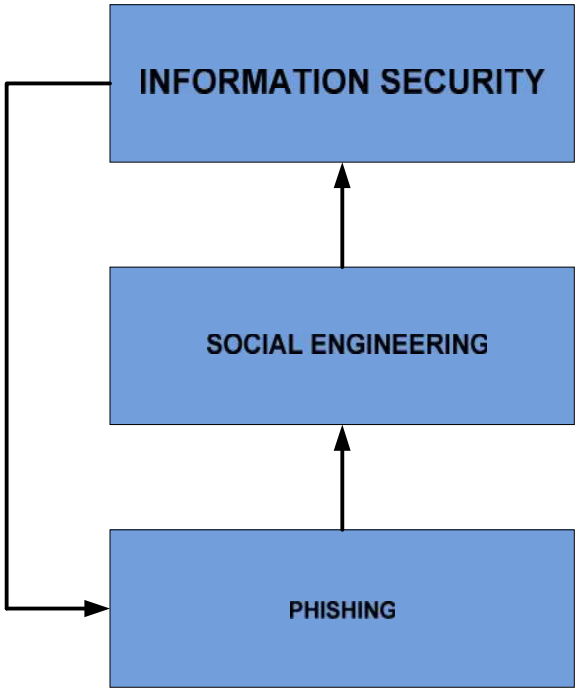


Figure 1.2: The systematic process that was adopted in reviewing key areas in relevant literature

Research Strategy

The research strategy adopted in this study strongly supports that of design science as described by Hevner, March, Park, and Ram (2004). This became evident from the way in which it adheres to the main research guidelines of design science. According to Hevner et al. (2004), design science creates and evaluates the IT artefacts which are intended to address the organisational problems which have been identified. In view of the fact that field studies enable behavioural science researchers to understand organisational phenomena in context, the process of constructing and exercising innovative IT artefacts enables design science researchers to understand both the problem addressed by the artefact and the feasibility of their approach to the solution of the problem.

As the research objective of this research study aims to develop an anti-phishing framework, the design science process will assist in producing the required output to ensure that it results in a trustworthy artefact, thereby meeting the research objective. Table 1.1 below outlines Hevner et al.'s (2004) design science research guidelines as applied to this study. The sentences in bold describe the research study's contribution in accordance with the specific guideline.

Table 1.1: Design science guidelines (adapted from Hevner et al., 2004)

Guideline	Description of guideline in accordance with the study
Design as an artefact	Design science research must produce a viable artefact in the form of a construct, a framework, a method or an instantiation. **This research aims to devise an anti-phishing framework.**
Problem relevance	The objective of design science research is to develop technology-based solutions to important and relevant business problems. **The anti-phishing framework aims to address phishing attacks on an organisational level.**
Design evaluation	The utility, quality, and efficacy of a design artefact must be rigorously demonstrated via well-executed evaluation methods. **The components of the framework were evaluated by three organisations by means of interviews which were conducted**
Research contributions	Effective design science research must provide clear and verifiable contributions in the areas of the design artefact, design foundations and/or design methodologies.
Research rigour	Design science research relies on the application of rigorous methods in both the construction and the

	evaluation of the design artefact. **In this study the framework was constructed by studying literature on information security, as well as internationally accepted best practices and theories**. **The framework was evaluated by means of semi-structured interviews.**
Design as a search process	The search for an effective artefact requires utilising the means available in order to reach the desired ends while satisfying laws within the problem environment. **A thorough research study was conducted over a four year period.**
Communication of research	Design-science research must be presented effectively both to technology-oriented as well as to management-oriented audiences. **This research is to be communicated to those individuals who are responsible for information security. In addition, the results of this research will be communicated at conferences.**

Research Evaluation

The components comprising the anti-phishing framework were evaluated by senior security individuals in three organisations by means of semi-structured interviews. The findings are discussed in section 6.7.

1.6 Layout of the Dissertation

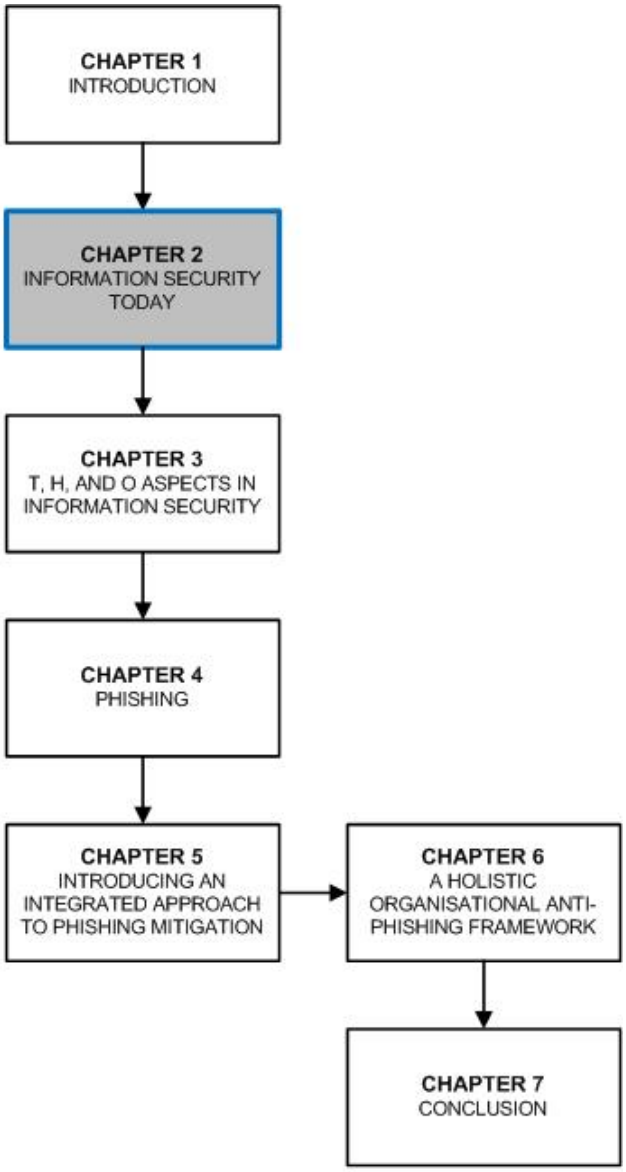
The following table presents a brief overview of the chapters in this dissertation:

Table 1.2: Outline of the dissertation

Chapter	Title	Description
1	**Introduction**	Introduces the research field, problem statement, research objectives and methodology adopted in the study.
2	**Information Security Today**	Focuses on exploring information security, the primary research area of the study. The objective of this chapter is to highlight the importance of information and also the reasons why it should be protected by both organisations and users. Information security threats, controls and best practices are introduced and explained.
3	**Technological Controls, Human Factors and Organisational Aspects in Information Security**	Introduces and explores the three main areas that must be considered within the ambit of information security, namely, technological controls, human factors and organisational aspects.
4	**Phishing**	Describes the most important aspects of phishing and its related techniques. The risk which phishing poses to an organisation and its customers are examined while real-world examples of phishing are discussed. The anti-phishing measures found in literature are categorised into three areas, namely, human factors, organisational aspects and technological controls
5	**Introducing an Integrated Approach to Phishing Mitigation**	Introduces the concept of an integrated human, organisational and technological (HOT) approach in order to address phishing holistically instead of using a single-layer defence model. Three important links between the HOT dimensions are established. Finally, those theories are examined

		which offer guidance in understanding the way in which the relationships between each of the dimensions may be managed more effectively.
6	**A Holistic, Organisational Anti-Phishing Framework**	Describes the educational components required to address the HOT dimensions in each linkage. Human behaviour and some methods pertaining to the way in which human behaviour may be changed are briefly described. Security awareness, training and education programmes are described in detail. Finally, the anti-phishing framework is evaluated by three organisations by means of interviews and the findings discussed.
7	**Conclusion**	Formally concludes the study. The chapters are summarised and further research is discussed.

CHAPTER 2
INFORMATION SECURITY TODAY



CHAPTER 2:

2.1 Introduction

This chapter focuses on exploring Information security - the primary research area of this study. The objective of this chapter is to highlight the importance of information and also the main reasons why it should be protected by both organisations and users. Information security threats, controls and best practices are introduced and explained. In addition, the developmental stages of information security, which shape the context in terms of which technological controls, organisational aspects and human factors, are introduced. The role which these components play in ensuring information security in organisations today is briefly examined as this establishes the foundation for this study.

2.2 The Importance of Information and Information Technology

Before it is possible to understand why information security is essential, we need to understand the importance of information, especially in view of the fact that it is regarded as one of the most vital components of an information system (Whitman & Mattord, 2010). In addition, the role which information technology plays in organisations must also be understood. This section intends to realise these two objectives.

Information today may exist in many forms, including the written form or printed on paper, while it may also be stored and transmitted electronically, shown on films or spoken in conversation (ISO/IEC 27002, 2005, p. viii). For many years, organisations have been digitising their paper-based records in the interests of more efficient and effective storage, despite the fact that certain regulations still require that an organisation retain all physical copies of documents. There are numerous advantages to organisations digitising their files, including the fact that this enables organisations to reuse, modify, transfer and access records more quickly as compared to the traditional file systems. There is also less physical space required to store the organisational and client records in the office. Today, many enterprises, governments, corporations, financial institutions, hospitals and private businesses store their copies of electronic data on computers and networks. These electronic copies may contain confidential information regarding employees, customers, products, research and financial information (Binarycse, 2010, Feruza & Tao-Hoon,

2007). One may argue that, with old filing systems, it was relatively easy to locate data because the data would be found stored by the user in a single location such as a filing cabinet or office drawer. However, digitising data has resulted in a situation in which data may be stored electronically in multiple locations such as hard drive folders, network drive folders, jump drive folders, intranet folders, and email account folders (Wacaser & Mazzeo, 2007). Thus, one begins to realise the need to secure data.

Information refers to processed data that is both meaningful and useful to people (Shelly & Vermaat, 2011). O'Leary and O'Leary (2010) define information as "data that has been processed through a computer system". Although these definitions are correct, they do not reveal the actual attributes of data and, furthermore, they neglect to mention the importance of information. If one understands what data consists of, one may begin to understand the importance of information and the reasons that information may be sought after.

The international ISO/IEC 27002 (2005) standard regards information and the supporting processes, systems and networks as important business assets and also as an essential aspect of an organisation's function. Certain researchers have equated the importance of information with the life blood of an organisation (Von Solms & Von Solms, 2005). Similarly, according to PriceWaterhouseCoopers (2008), "information has become the new currency of business".

Information may be considered personal, confidential and sensitive as it may contain important personal details including, but not limited to, individual information such as race, social security number, credit card number, date of birth, salary, pin number, usernames, passwords, gender, sex, pregnancy status, marital status, ethnicity, social origin, sexual orientation, age, physical and/or mental health, religion, culture, language, birth, medical, criminal or employment history, financial transactions, fingerprints and blood type. On the other hand, information relating to organisations may include design blueprints, formulae, health information, financial records, criminal and employment history and military secrets. Depending on the type of information, it may be in the format of text, images, sound, video and so on. Information is typically stored on information systems. One may imagine the illegal purposes for what such information may be used, should it fall into the wrong hands.

Ultimately, the main purpose for which this information would be used by threat agents would be for financial gain (mydebt.co.za, 2011).

The description of information contained in the previous paragraph may be regarded as referring to 'legitimate' information required by both organisations and their customers. However, not all information is considered as 'legitimate'. In view of the fact that information is easily accessible using the Internet, there are people who are making use of the opportunity to publish and share 'illegitimate' information deliberately. This information may be downloaded from either websites or from peer-to-peer (P2P) software applications. Depending on the intentions of the individual who receives or makes such information available, the information may be used to instruct others in unlawful, immoral or unethical activities. For example, one may find material on, among other things, hacking systems, committing violent crimes and terrorist acts and pornography. Some websites which are known for sharing malicious information include the Church of Euthanasia and The Anarchy Cookbook. People who willingly share this type of information on the Internet may be considered a threat. On the other hand, people who use this information are often inexperienced and, thus, their attack methods may be labelled as 'unstructured attacks'. However, such attacks may still cause serious financial harm to an organisation. Most of the abovementioned examples of sharing illegitimate information emphasise the need to provide suitable protection for information.

For many organisations, information and the related technologies represent organisations' most valuable, but often least understood assets. Successful organisations recognise the benefits of information technology (IT) and use such technology to increase their stakeholders' value (COBIT 4.1, 2007). Since 1994, **Information Technology** (IT) has emerged as a key driving force as regards an organisation's decisions and strategies (King Report, 2001, p. 11). As a result, the organisation's information is among its most valuable assets and is essential to the success and wellbeing of the organisation (Von Solms & Von Solms, 2006). An asset refers to anything which has value for an organisation. Assets may be physical, for example the staff members, computer systems or any other tangible objects (Whitman & Mattord, 2012, p. 9). Alternatively, an asset may be logical, for example, websites, computer programs or information.

The computing environment has evolved from computer-centric to information technology-centric to the current information-centric environment of today (Thomson, 2003). As a result, many organisations today are totally dependent on their IT systems to capture, store, process and distribute company information (Von Solms, 2006). According to Legrisa, Inghamb, and Collerette (2001), there are many reasons why enterprises decide to invest in information systems (IS), including pressure to cut costs, to produce more without increasing costs and to improve the quality of services or products, all with the aim of ensuring that the organisation continues to function. According to Whitman and Mattord (2010, p. 2), "today's global markets, business operations are enabled by technology. From boardroom to mailroom, businesses make deals, ship goods, track client accounts, and inventory company assets, all through the implementation of systems based upon IT. IT is the enabler of the storage and transportation of information from one business to another". These researchers compare this transportation process to a vehicle. If the vehicle breaks down on a crime-ridden road, even for a short period, business transactions will be disrupted. Thus, organisational assets have become more vulnerable to threat agents from both within and outside of the organisation itself and may result in the organisation losing money. Typically, significant attention is focused on those efforts that address the risks which affect business information from an IT infrastructure perspective. This is as a result of the fact that IT has come to play an integral role as regards the storage, processing and transmission of valuable business information assets (Posthumus & Von Solms, 2004).

This section described the attributes of information. It also highlighted the importance of information and, thus, the reason why information is sought after by threat agents. IT plays an important role in the storage and processing of information as well as in the transmission of information from one organisation to another. If the IT infrastructure of an organisation is either disrupted or weakened in any manner, this may compromise the security of the organisation's information. This section also discussed the security concerns that information may also be used for illegal purposes, depending on who has access to the information. The IT environment, which makes this information available, is also used as a channel by threat agents in order to acquire information. The following section discusses information security

and also the importance of information security. Common security threats and the controls used to combat those threats are also described.

2.3 Information Security Explored

The previous section described information and its attributes in detail and also established information as an organisational asset. The role of IT in an organisation's information was also described. This section endeavours to define information security and to describe modern information security threats. The importance of information security is also highlighted.

Section 2.2 established that IT enables the acquisition, processing, storage and dissemination of data (i.e. text, images, video, numeric, sound) through the use of computers and telecommunications. However, it is important that these processes are made secure so that the data is not compromised in any way by people, either intentionally or unintentionally. According to Ai Cheo Yeo, Rahim, and Ren (2009), as the dependence on information processing and the interconnection of various information systems via the Internet increase, so, too, does the risk to information systems. As a result, information is now exposed to a growing number, and also a wider variety, of threats and vulnerabilities than ever before.

Before addressing the issue of information security, it is important to distinguish between a security **threat** and a security **attack**. According to Whitman, Mattord, and Green (2012, p. 8), a security threat is generally a category or object, person, or any other entity that poses a potential risk of loss to an asset while an attack is an intentional or unintentional action that may represent the unauthorised modification, damage or loss of an information asset.

"The quality or state of being free from danger" may be regarded as a general definition of **security** (Whitman & Mattord, 2010, p. 3). On the other hand, **information security** is defined as "methods for protecting information and/or information systems from unauthorized access, use, disclosure, disruption, modification or destruction" (ISO/IEC 27002, 2005). These two definitions are extremely similar. In the first case, the general definition focuses primarily on *humans* being safe and protected from danger while the definition of information

security focuses on protecting *information* and the systems which use, store and transmit that information. It is interesting to note that the latter description neglects the human element. Threat agents target users by exploiting weaknesses in the same systems which aim to protect users. This, in turn, raises the question as to whether information and physical computers should be protected from security threats or whether the humans who use information and systems should be protected from both themselves and from threats. According to Whitman et al. (2012, p. 8), a computer may be the subject of an attack as a computer may be used as the tool with which to conduct an attack. A computer may also be the object of an attack as it may comprise the actual entity which is being attacked. In cyber forensics, where the computer is used a tool with which to commit a serious crime, the information stored on the computer is both vital and useful as it may be used by the investigators as evidence to prosecute the criminal lawfully.

In order to understand the need for information security, the following example is cited. Imagine if one's laptop or external hard drive were stolen by a thief (i.e. security threat). Firstly, there is the considerable inconvenience of having to find a suitable or exact replacement for the stolen asset. This may be costly and the victim may not have the necessary funds at the time. However, even more concerning is the type of information which stored on the device that has been lost. This information may represent many hours of work spent on a task, a customer's financial information, logging in details, personal photographs of a memorable holiday or wedding day and so forth. It is, thus, clear from these typical examples that it would not be possible either to buy or replace with any ease the data or information unless it were backed-up on a separate device. In addition, the information stolen may be of either an extremely sensitive or personal nature. One may imagine the unlawful activities that the thief may carry out using this information. This emphasises that there is greater value in securing information as compared with focusing on the replacement of physical components. It may be argued that protecting the physical assets would, ultimately, secure the information stored on its device. However, in the examples cited above, the asset which is the most valuable is the information and not the laptop itself.

People may not perceive any risk in openly sharing information. For example, imagine removing the garbage from one's house and placing it outside on the pavement for collection. The underprivileged person on the street who rummages through the garbage may not perceive it as 'rubbish' and, indeed, may even take some items, or a single item, that may be of some to use to him/her. In an information security context, the contact number that people often share openly on a social networking website may have more value for the threat agent than one may imagine and it may even create an opportunity for the threat agent to acquire further information by using it to access other areas in the Internet arena. As such, it is essential that organisations and users understand the importance of ensuring that their information is both private and secure.

According to Whitman and Mattord (2010, p. 4), information security includes the broad areas of information security management, computer and data security and network security. The terms 'information security' and 'computer security' are often used interchangeably as they each involve similar aspects. According to Whitman and Mattord (2010), information security has its roots in the history of computer security while computer security began when computers were first introduced into business. These computers were particularly large and, thus, security focused primarily on physically securing the location of the hardware (i.e. the computer itself) and protecting it against threats. Physical controls were used (e.g. locking doors) to protect the location of the computer from unauthorised intruders. Other threats to computer security included natural hazards such as fire and floods, power failures, hard disk crashes and so on, which could damage the computer equipment. It may, thus, be argued that computer security focuses on securing the physical 'computer' while information security, on the other hand, focuses on measures to secure 'information', including physical security and educating humans. Most information today has been digitised and, thus, the need to secure information has increased. It may, however, be argued that the two terms discussed are the same because, ultimately, computers store the information and, therefore, if computers are protected then, naturally, the information on the computers is protected. However, this is not always the case. In the past information may have been restricted to a single computer. However, today information is transmitted over networks and stored on multiple servers in locations that not even the user is aware of. In addition, the

human element also poses a risk as threats may manipulate people instead of computers in order to gain information. The latter will be discussed in section 3.4.2.

The main objective of information security is to protect the confidentiality, integrity and availability of data or information against a wide variety of threats (ISO/IEC 27002, 2005). This, in turn, would ensure business continuity, minimised business risk as well as maximised returns on investments and business opportunities (Whitman & Mattord, 2010). As depicted in Figure 2.1, confidentiality, integrity and availability (also known as the CIA triangle) are widely recognised as the three characteristics that describe the utility of information (Whitman & Mattord, 2010, p. 6), with these three characteristics rendering information valuable to an organisation. The next paragraph distinguishes between each of these characteristics.

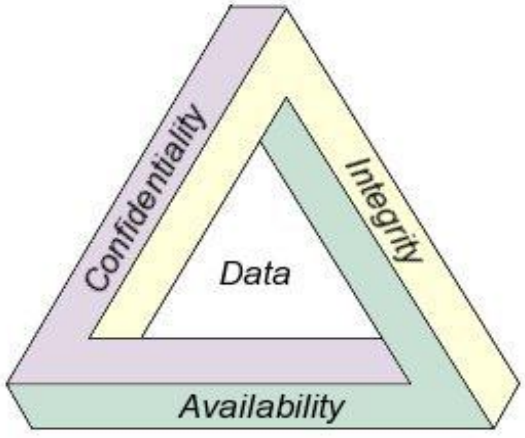


Figure 2.1: The CIA triangle (source unknown)

'Confidentiality' is the term which is used to prevent the disclosure of information to unauthorised individuals or systems. Confidentiality is necessary for maintaining the privacy of those people whose personal information a system holds. For example, a credit card transaction on the Internet requires the credit card number to be transmitted from the buyer to the merchant and from the merchant to a transaction processing network. In this case, the system attempts to enforce confidentiality by encrypting the card number during transmission, by limiting the places where it may appear (in databases, log files, backups and printed receipts), and by restricting

access to the places where the card number is stored. If an unauthorised party obtains the credit card number by any means, a breach of confidentiality may be said to have occurred. Confidentiality breaches may take many forms, including the following:

- Allowing someone to look over one's shoulder at one's computer monitor when confidential data is displayed on the monitor
- Stealing or selling a laptop that contains sensitive information concerning employees
- Divulging confidential information over the telephone, even if the caller is not authorised to have access to the information.

According to Janczewski and Colarik (2007, p. 430), **integrity** is the confirmation that data which has been sent, received, or stored is complete and unchanged by malicious incident. On the other hand, Whitman and Mattord (2010, p. 6) define integrity as the "quality or state of being whole, complete, and uncorrupted". These authors maintain that data integrity is violated when

- an employee accidentally, or with malicious intent, deletes important data files
- a computer virus infects a computer and corrupts data
- an employee is able to modify his/her own salary on a payroll database
- an unauthorised user vandalises a website
- a voter is able to delete a large number of votes in an online poll.

There are other ways in which integrity may be compromised without malicious intent. For example, a user may accidentally type someone's name incorrectly on a system. Faulty programming or noise on the transmission channel or media may also cause data to lose its integrity (Whitman & Mattord, 2010, p. 7).

Lastly, it is essential that information is readily available, particularly when it is needed. **Availability** requires that the computing systems used to store and process the information, the security controls used to protect the information and the communication channels used to access the information, are functioning correctly at

all times. High availability systems strive to remain available at all times, thus preventing service disruptions as a result of power outages, hardware failures, natural disasters, denial-of-service attacks and system upgrades. These service disruptions are often termed 'downtime'. According to Janczewski and Colarik (2007, p. 430), availability is particularly vital in contexts in which communication network failures may cause breakdowns in other critical networks such as air transport or the power supply.

The implementation of a suitable set of controls is required if the vital CIA attributes described above are to be a reality. These controls include policies and procedures, processes, organisational structures as well as hardware and software functions. In addition, it is essential that these controls be established, implemented, monitored, reviewed and improved, when necessary, to ensure that the specific security and business objectives of the organisation are met. This should also be done in conjunction with other business management processes (ISO/IEC 27002, 2005). Security controls are discussed later in section 2.3.3.

2.3.1 Why Information Security is Needed

As discussed earlier, organisations depend on both IT and the information systems to carry out their mission and conduct their business functions successfully (NIST 800-37, 2010). Today, most information is stored electronically on computers and transmitted over both networks and the Internet. However, the information stored on information systems may be subject to a variety of threat agents that may, in turn, have a serious impact on the operations and performance of the organisation concerned (PriceWaterhouseCoopers, 2008). This may further compromise the organisation's mission, functions, image and reputation and organisational assets, as well as individuals, other organisations and nations (NIST 800-37, 2010). Today, organisations and individuals use the Internet in order to offer or perform e-commerce. Financial institutions provide their customers with credit cards which enable them to buy goods and services online. If the customer's credit card details are compromised in any way by a threat agent, this information may be used to steal the victim's money. An increasing number of organisations are allowing their registered members (their clients) to gain access to their personal records through using websites. For example, users have the freedom to access, modify and update

their personal information, including financial investments, telephone accounts, insurance, and so on. However, should this confidential information regarding the business or its customers be compromised, this may lead to loss of business, law suits, mistrust, damaged reputations and even bankruptcy (Feruza & Tao-Hoon, 2007; Sophos, 2005).

In view of the fact that information is regarded as an organisational asset, it is imperative to define, achieve, maintain and improve information security in order to maintain a competitive edge, cash flow, profitability, legal compliance and a positive commercial image (ISO/IEC 27002, 2005). The aim of information security is both to ensure business continuity and to minimise business damage by preventing and minimising the impact of security incidents (Von Solms, 1998). Chapter 3 discusses the way in which organisations achieve this. This subsection highlighted the importance of information security and described how it may result in the protection of the organisation and its customers. The next paragraph describes some common information security threats.

2.3.2 General Information Security Threats

The sophistication and extent of the damage that modern security threats pose to organisations and users will be revealed in this section while general information security threat agents and their attack methods will also be discussed. In addition, the section will also distinguish misconceptions regarding the types of threats.

Today, if one were to enquire randomly of a colleague or friend what they considered constituted a human threat agent to computer systems most would immediately refer to ‘hackers’. It is, thus, a misconception among the general population that all threat agents to computer systems may be regarded as hackers who are, typically, stereotyped as the male teenager with bad skin, long hair and glasses, operating from a cluttered bedroom with the aim of accessing, disrupting and damaging computer systems and networks. Hackers are usually regarded as the perpetrators of serious crimes. However, hackers may feel offended by this misclassification as they often gain unauthorised entry into systems merely for the fun and challenge of doing so. It is believed that hackers are interested in gaining fame or notoriety as a result of their activities. Crackers, on the other hand, gain unauthorised entry into systems and disrupt and damage these systems for malicious reasons (O’Leary &

O'Leary, 2010). Thus, crackers, as compared to hackers, are considered more of a threat as their motives are the more dangerous.

According to Van der Merwe et al. (2005a), historically, most crime committed over the Internet has either been the result of curiosity or malicious technical attacks performed by crackers. According to Janczewski and Colarik (2007, p. 308), crackers use various methods to attack a computer system's security maliciously. A virus is one such method. However, Van der Merwe et al. (2005a) believe that this situation has changed as a result of the immense growth and popularity of using the Internet for financial applications and, thus, a new generation of computer criminals has been born, namely, the spammers and the fraudsters (Levy & Arce, 2004). Spam refers to unsolicited email traffic that is typically used to advertise the availability of products or services from an online vendor (DeFino, Kaufman, Valenteen, & Greenblatt, 2010). Spam is distributed by spammers who acquire lists of legitimate email addresses and exploit an SMTP open mail relay (DeFino et al., 2010). On the other hand, fraudsters are people who involved in Internet fraud - a practice indulged in by individuals who spam potential victims in the hope that they will take the 'bait'. Using social engineering techniques, the bait may be prize winnings, lottery draws or safeguarding the money in an individual's account. One such type of fraud that has shown tremendous growth over the past few years is the practice of 'phishing' (also known as 'spoofing'). Phishing will be discussed later in Chapter 4.

Cyber crime refers to a crime that is committed using digital technology and infrastructure (HTCIA, 2010). Cyber attacks on information systems are often aggressive, disciplined, well-organised, well-funded and extremely sophisticated. Janczewski and Colarik (2007, p. xiii) define cyber terrorism as "premeditated, politically motivated attacks by sub national groups or clandestine agents, or individuals, against information and computer systems, computer programs, and data that result in violence against non-combatant targets". Janczewski and Colarik (2007, p. xiv) distinguish between cyber crime and cyber terrorism attacks using the following scenario:

Imagine that an individual gains access to a hospital's medical database and changes the medication of a pro-business, anti-environmental executive of a Fortune 100 company to one that he or she is allergic to and also removes the allergy from his/her electronic record.

Referring to the Janczewski and Colarik's scenario, if the executive's record were changed intentionally as a result of poor relations between the individual concerned and the victim, then this would be considered murder in addition to cyber crime. However, if the individual changing the records were later to announce that he/she were intent on committing more such acts if his/her demands were not met, then this would be labelled as cyber terrorism. However, if the activities were carried out by an agent of a foreign power, then the action would be labelled as information warfare. Cybercrime is an intercontinental growth business. The US Treasury Department estimates that cyber crime costs the global economy $300 billion, more criminal revenue than the revenue of the international narcotics cartels (Whitehouse, n.d).

Today, malicious code, computer hacking, phishing and denial of service attacks (DoS) have become more common and more ambitious than ever before and also increasingly sophisticated (Geer, 2005; ISO/IEC 27002, 2005; Sophos, 2005). They may be executed in a variety of ways, including computer-assisted fraud, espionage, insider threats, sabotage, vandalism, and fire (ISO/IEC 27002, 2005). Janczewski and Colarik (2007, p. xv) discuss typical modern cyber-attacks as follows:

- **Virus and worm attacks:** A virus is defined as a piece of programming code which is usually disguised as something useful and that causes some unexpected and, usually, undesirable event. A computer virus attaches itself to a program or file and, thus, it may spread from one computer to another, leaving infections as it travels (Janczewski & Colarik, 2007, p. 308). A virus is typically delivered via email attachments, web browser scripts and vulnerability exploit engines. Viruses are capable of preventing an infected computer from booting up. Other malicious objectives of viruses include information theft, rendering hardware useless and corrupting software. Worms may spread across computer networks, but by themselves and without being attached to host files.

- **Denial of service (DoS) attacks:** The attacker sends a large number of information requests to a target. This, in turn, causes the target system to become overloaded that it is not able to respond to legitimate requests for service (Whitman & Mattord, 2012, p. 65).
- **Website defacing:** This involves informational websites that service governmental and commercial interests and results in the spread of disinformation and propaganda, and/or disrupts information flow.
- **Unauthorised system intrusions:** These may lead to the theft of confidential and/or proprietary information, the modification and/or corruption of data and the inappropriate usage of a system for launching attacks on other systems.

According to Janczewski and Colarik (2007, p. xvi), the objectives of the above-mentioned types of attack may vary from revealing the vulnerabilities inherent in systems, political statements about the conduct of the entities being attacked or stealing information. Gorge (2007) further highlights the dangers that cyber-attacks may pose. Gorge cites the example of a threat agent being able to change the formulations of popular prepacked food or prepacked medicine. In order to do this, the threat agent would gain unauthorised entry into the computer systems of either food processing or drug manufacturing organisations and change the formulations. The potential consequences to the population may include

- illness
- commercial impact
- fear
- impact on the trustworthiness of the industry and government.

A report of Deloitte identified the most common external security threats in their annual global security survey (Deloitte, 2009, p. 31). The results are summarised in Table 2.1 below:

Table 2.1: Top 8 repeated external breaches

THREAT	ONE OCCURRENCE (%)	REPEATED OCCURRENCES (%)
Email attacks (i.e., spam)	10	24
Phishing/pharming	7	22
Viruses/worm outbreaks	11	15
Employee misconduct	11	11
Spyware	7	11
External financial fraud using information systems	4	10
Social engineering	5	7
Physical threats	7	6

Source: Adapted from Deloitte (2009, p. 31)

Most information security attacks listed in Table 2.1 evidently involve the use of the Internet. The report also reveals that most of the attacks targeted email. Phishing is also reflected as one of the highest repeated threat occurance. The Internet may, metaphorically, be seen as a highway which threat agents may use to attack their victims. With the increase in the use of networks in order to exchange confidential information between organisations, network breaches are becoming more common. According to Dye, McDonald, and Rufi (2008), the serious consequences to an organisation affected by a network breach may include the following:

- Network outage, causing a loss of communication and business transactions
- Loss of personal or business funds
- Theft of intellectual property for example, project bids, patents, strategic plans, and so on
- Exposure of confidential customer data.

Insider threats are often regarded as posing the most serious security risk which an organisation may possibly face. This is as a result of the fact that insider threats agents may have legitimate access to facilities and information, be trusted and possess knowledge about both the organisation and the location of valuable and critical assets (Colwill, 2010). Johnson (2006) points out that the incidence of insider attacks is greater than all other sources of information security breaches combined. Insiders know how to achieve the greatest impact whilst leaving little evidence. A malicious insider has the potential to cause more damage to the organisation than the outside attacker, as well as possessing many more advantages than the outside attacker. Insiders will know how, when and where to attack and how to cover their tracks. A good example in this regard is the insider sabotage which was committed by the Chief Network Software Engineer of Omega Engineering, Timothy Lloyd (Goertzel, 2008). Omega is a manufacturer of high-tech measurement and control instruments used by NASA and the US Navy. In July 1996, Timothy Lloyd was dismissed from his job after 11 years of service. However, before leaving, he planted a logic bomb (malicious software) on Omega's server and also stole the only available backup tape for the server's data files. The logic bomb was triggered unknowingly three weeks later by an engineer who switched on the computer terminal. The logic bomb deleted all of Omega's design documents, source code and production programs, resulting in millions of dollars in financial losses.

Colwill (2010) maintains that even harmless insider activity may cause serious accidental damage. For example, inappropriate Internet use, which not only wastes an organisation's time and resources, may also contribute to the following:

- Places the organisation's network and systems at risk of virus infections and malware
- Leads to potential lawsuits across a wide range of areas, for example, criminal action, copyright infringement and claims of sexual harassment, racism, bullying or defamation
- Impacts significantly on an organisation's reputation and future revenue.

Unskilled staff may, potentially, become a threat to an organisation, as such individuals may not be able to use their tools and resources correctly. A lack of skilled staff has been identified as the third most significant cause of the failure on the part of users of IT to ensure the security of their physical assets and information (Furnell & Clarke, 2005). As mentioned in section 2.3, the integrity of data may also be compromised as a result of human error or negligence. For example, a user may unintentionally mistype data into a computer system, thus posing a security risk to the organisation. A 2006 Computing Technology Industry Association survey found that security managers attribute approximately 60% of security breaches to human error – an increase of 47% from the previous year (Crawford, 2006). It is, thus, clear that technologies are focusing on becoming automated in order to reduce human involvement. One does not have to look very far to see the implementation of these technologies. For example, the point of sale (POS) terminals at grocery stores includes bar code scanners, which reduce any involvement on the part of the operator in having to insert the price of an item manually.

Piracy is also a concern for information security. Software piracy takes place when an individual, either knowingly or unknowingly, copies a piece of software in violation of the copyright agreement associated with that software. Software piracy costs the IT industry billions of dollars in lost sales each year and it is estimated that piracy cost the software industry a combined $13 billion US dollars in 2002 (National Chamber Foundation, 2005). The piracy challenges that industries face in terms of software, music, movies, games and so on being made available illegally and at no cost on online peer-to-peer sharing websites are well known. Users in general are practising unethical behaviour by sharing such information using networks and the Internet. This, in turn, is cultivating a society in which people may believe that it is the norm to share material that is licensed and owned by organisations. Such activities adversely affect the revenue of the industries concerned, while certain governments have felt the need to intervene in the type of content that is published on the Internet. The United Nations (UN) acknowledges that there are certain types of information on the Internet that should be restricted, including slander and hate speech, while China has banned websites such as Google+ and YouTube for fear that these websites may potentially contain information unsuitable for its people. In some countries,

using the Internet as a means to speak out against the government is an offence punishable by death.

Yet a further information security concern is the fact that threat agents are able to create spoofed websites which are made to appear as legitimates websites. Sophos, an anti-virus company, claims that freely downloadable, do-it-yourself phishing kits exist. If this is true, then anyone with malicious intent may acquire these kits on the Internet. Mitnick and Simon (2002) classify those individuals who make use of these kits as “script kiddies”. The kits are purported to contain all the graphics, web source code and text required to construct spoofed websites which are designed to possess the same look and feel as legitimate, online banking websites. The kits also include spamming software which enables potential fraudsters to send out hundreds of thousands of phishing emails as bait for potential victims (Garera et al., 2007). Combining these kits with certain creative social engineering techniques would enable threat agents to launch their own phishing attacks.

This section described a variety of the threats encountered in today’s digital world. These threats are extremely sophisticated and harmful and far exceed the traditional computer viruses seen decades ago. As an organisation’s dependency on the use of telecommunications and the exchange of information electronically increases, so too do threat attack methods and techniques. Threat agents are using technology to their own advantage as methods or techniques to seek out and acquire confidential information. The technology may, in turn, be perceived as the “middle man” who stands between the two human parties i.e. the victim and the threat agent. It is, thus, essential that information security take into account both aspects, namely, the legitimate people using systems (i.e. the end-users) and those trying to gain unauthorised entry into systems (i.e. the threat agents).

There are a number of techniques that threat agents use in order to acquire information and data from their victims with threat agents creating viruses, malware, spyware, spoofed websites, fake identities, fake emails, and suchlike with the aim of deceiving individuals in order to obtain their personal information. Accordingly, security controls are needed to help protect people and organisations against these threats. The next section briefly describes the controls used to combat general security threats.

2.3.3 Information Security Controls

How does an organisation protect its sensitive information? The answer to this question will be discussed in this subsection. Defenders of information endeavour to prevent attacks by applying controls, safeguards or countermeasures (Whitman et al., 2012, p. 9). Controls, safeguards and countermeasures are all synonymous terms which may be used to describe security mechanisms, policies and procedures. Whitman and Mattord (2010, p. 299) define a control as "a security mechanism, policy, or procedure that can counter system attacks, reduce risks, limit losses, and resolve vulnerabilities". Thus, management implements controls in order to mitigate risks. These controls are necessary to protect organisational information from threats, including accidental human error. According to ISO/IEC 27002 (2005), once information security requirements and risks have been identified and decisions made regarding the treatment of risks, it is essential that appropriate controls be selected and implemented to ensure that risks are reduced to an acceptable level. The selection of security controls is dependent on organisational decisions which are, in turn, based on the criteria for risk acceptance, risk treatment options and the general risk management approach applicable to the organisation concerned. In addition, it should also be subject to all relevant national and international legislation and regulations (ISO/IEC 27002, 2005). The selection and implementation of appropriate security controls for an information system or a system-of-systems are important tasks that may have major implications for the operations and assets of an organisation, as well as the welfare of individuals and nations (NIST 800-53, 2009). Whitman et al. (2012, p. 3) classify general information security controls into the following areas:

- **Network security.** Protecting the networking components and connections
- **Physical security.** Protecting the physical items, objects or areas of the organisation from unauthorised access and misuse. For example, locking doors and employing security personnel to prevent intrusions.
- **Personnel security**. Protecting staff from unauthorised people who wish to gain access to the organisation and its facilities.
- **Operations security.** Protecting the details of a particular operation or series of activities.

- **Communications security.** Protecting the organisation's communications media, technology and content.

Clearly, most of the security controls mentioned above would, inevitably, make use of technological controls. However, this is indicative of the unfortunate situation where information security is treated as a single-layer approach in terms of which an organisation may believe that security threats may be prevented by implementing technological controls (Hinson, 2003). Intrusion detection systems, firewalls, anti-virus software, virtual private networks, encryption and biometrics are all security technologies which are in use today. Network administrators regularly have to investigate different databases in order to ascertain whether there are any new vulnerabilities and then apply patches to their systems in order to avoid attacks. Different security staff is frequently responsible for and dedicated to the monitoring and analysis of the data provided by a single system. However, security staff may not analyse the data on a periodic basis and also not communicate the analysis reports to other staff timeously.

Section 2.3 indicated that it is essential that information and/or information systems be protected from unauthorised access, use, disclosure, disruption, modification or destruction. In order to prevent unauthorised access or use of information, technological controls, including passwords (access control), may be in put in place to ensure that relevant staff only may access and use the information. However, this is not a simple solution. The interconnection of public and private networks and the sharing of information resources increase the difficulty of achieving effective access control (ISO/IEC 27002, 2005). Furthermore, ISO/IEC 27002 (2005) states that many information systems have not been designed to be secure. ISO/IEC 27002 (2005) further states that technical controls provide limited information security.

Physical controls are associated with the physical aspects of security, for example; the lock on the door of an office containing sensitive documents. **Technical controls** are controls of a technical nature, usually software based, for example, forcing a user to authenticate by using a unique username and password before the user is allowed access to the operating system. The third category, **operational controls**,

collectively includes business, administrative, managerial and procedural controls and consists of all those controls that involve human behaviour in one form or another. Thus, these controls include those controls that involve the creation of information security policies and procedures as well as the administration of other controls. Despite the fact that they do not deal directly with operational issues, both physical and technical controls usually require some form of human involvement. Within an organisational context, these controls would, thus, have to be supported by procedures outlining the employees' involvement in the use of these controls.

Having discussed information security and its importance in this section, it is clear that it is essential that the associated threats be controlled in a proper manner. It is evident that each of these controls requires human involvement. The consequences of inadequate controls or the lack thereof may be detrimental to the survival of an organisation. The following section will explain the information security best practices which several organisations currently follow.

2.4 Information Security Best Practices

In general, organisations could manage and protect their information effectively by adopting internationally accepted and recognised Codes of Practice for Information Security Management. For example, the ISO/IEC 27002 (2005) international standard represents one such 'best practice' that establishes guidelines and general principles for initiating, implementing, maintaining and improving information security management within an organisation (ISO/IEC 27002, 2005). The objectives outlined in ISO/IEC 27002 provide general guidance on the commonly accepted goals of information security management. The control objectives and controls indicated in this standard are intended to meet the requirements which have been identified by certain risk assessments. This standard may serve as a practical guideline for developing both organisational security standards and effective security management practices and helping to build confidence in interorganisational activities. Despite the fact that ISO/IEC 27002 is, in general, a widely spread respected standard, Japan is by far the most vociferous advocate of ISO/IEC 27002 (Everett, 2011).

Both Control Objectives for Information and Related Technology (COBIT 4.1, 2007), and King III (2009) also represent international best practices. Adherence to such best practices may play an integral role in protecting organisational information assets. COBIT 4.1 contains good practices across a domain and process framework and presents activities in a manageable and logical structure (COBIT 4.1, 2007, p. 4). COBIT (2007) represents the consensus of experts and is strongly focused on control rather than on execution. According to the standard, the best practices help optimise IT-enabled investments, ensure service delivery and provide a measure against which to judge security incidents. The King III Report gives a summary of best international practices in corporate governance.

However, these best practices, international standards and guidelines are not necessarily a one-size-fits-all solution for organisations to adopt in their addressing of information security challenges. Every organisation is unique and, thus, organisations often tailor their own security frameworks by adopting specific components from these internationally accepted standards (Experian, 2009). Similar to software development versions, these specific best practices, standards and guidelines discussed are updated and then released as a result of the ever-changing nature of businesses and technology. However, the main challenge in ensuring that organisations either apply or follow these standards lies in the fact that that they are not legally obliged to do so and, therefore, it is not incumbent on organisations to comply with these standards. As a result organisations may inadvertently put both their own and their customers' information at risk because of non-compliance. There are, however, laws and regulations, such as the Electronic Communications and Transactions Act, 2002 (ECT), which are legislated and should be adhered to by law. Many organisations in the United States are legally required to protect the security of personal information. The two major federal laws on privacy enacted in recent years include the Gramm-Leach-Bliley Act and the Health Insurance Portability and Accountability Act. These acts include security regulations that apply to a broad range of financial services companies and health care organisations.

Certain organisations are accustomed to adopting popular best practices and standards such as ISO/IEC 27002, COBIT 4.1 and the King III Report. However, not all organisations are applying such measures. Secondly, even if they do have such measures in place, they may not be adhering as strictly to the measures as they had

originally planned to do. This is an issue of some concern. According to Von Solms (2000), in order to manage information security properly an organisation should be able to measure the effectiveness of its information security while making use of best practices and guidelines and international information security certifications and by cultivating an information security culture. In the next section, the developmental history of information security is briefly explained. The stages of information security over several decades is categorised into technological, organisational and human aspects.

2.5 The Developmental Stages of Information Security

In section 2.3.3, information security controls and the importance of these controls were described. However, this section did not broadly categorise the specific types of controls that organisations apply. There are several literary sources which categorise information security controls in various ways although there is some commonality in the specific types of controls used. Von Solms (2000; 2006) discusses the development of information security controls over the past 40 to 50 years by categorising this development into a number of incremental, overlapping waves. These waves include technical, management, institutional and information security governance. The following subsections further describe the technological, organisational and human aspects of information security controls by using adaptations of Von Solms's work.

2.5.1 Technological Controls

Technological controls are implemented in order to protect the integrity of data. Technological controls refer to controls of a technical nature and which are usually software-based, for example, forcing a user to authenticate access to a computer system by using a unique username and password before allowing the user access to that system. This is known as an access control as the operating system's built-in security serves as a technical control. According to Von Solms (2000), these developments constituted as the 'First Wave' which he regards as a *technical wave.* This wave began in the early eighties when computers were mostly mainframe-based. Similar to the previous example, security on this level involved using the built-in facilities of mainframe operating systems such as access control lists, user-ids and

passwords. Technical staff members such as computer security experts, mainly technologists, were responsible for information security issues (Geer et al., 2003) and they implemented the necessary technical controls and also carried out the necessary maintenance. However, other non-technical issues such as best practices and policies were not addressed at this early stage.

2.5.2 Organisational Aspects

According to Von Solms (2000), the technical wave has continued to manifest in the subsequent waves. It is worth noting that, despite the fact that technical controls do not address operational issues directly, the use or implementation of these technical controls usually requires some form of human involvement. Thus, within an organisational context, these controls would have to be supported by procedures outlining employees' involvement in using these controls. Accordingly, Von Solms (2000) maintained that the 'Second Wave', which lasted from the early eighties to the middle nineties, may be regarded as the *management wave.* The development of distributed computing and the later explosion of the Internet, the World Wide Web and e-commerce resulted in the need to address information security concerns on a higher level and, specifically, on the level of top management. This, in turn, resulted in the need for, at the very least, all employees within an organisation to participate in the information security management of the organisation concerned as well as possibly requiring the participation of shareholders, suppliers, specialists, third parties, customers or other external parties (ISO/IEC 27002, 2005). Ohaya (2006) believes that security managers should ensure that the need for privacy and security are perceived at a macro-level within an organisation.

The formulation of information security policies and procedures, the establishment of organisational structures and the appointment of information security managers and staff were the norm at this stage (Von Solms, 2006). Kankanhalli (2003) revealed in his study that management support is positively related to the implementation of preventative security efforts. Kankanhalli also found that financial organisations invest more resources in controls designed to prevent bad security practices in comparison to larger organisations that tend to invest more in preventive measures.

According to Von Solms (2000), the Third Wave started in the late nineties with this wave coming to be known as the 'Institutional Wave'. Aspects such as best

practices, codes of practice for information security management (e.g. COBIT 4.1, ISO/IEC 27002), international information security certification (e.g. CISSM, CISSP), and information security culture and security metrics were evident at this stage.

The 'Fourth Wave' relates to both the development and the crucial role of *information security governance* (Von Solms, 2006). At this stage, top management and boards of directors became personally accountable for the effective functioning of their IT systems of which they based their planning and decision making. As a result, at this stage, the responsibility for information security concerns shifted to the highest level possible, namely, the board of directors. This change is significant, particularly in view of the fact that, during the technical wave, information security was the responsibility of the technical staff only.

In this section, the importance of organisational aspects is further emphasised by indicating the involvement required on the part of top level management as regards addressing information security concerns as opposed to the technical wave which had involved technical staff only.

2.5.3 Human Factors

The human factor is an increasingly popular area of interest that has emerged in information security research**.** Human factors are related to the way in which humans treat and manage information in a secure manner. In this regard, Mitnick and Simon (2002) state that "[h]umans are the weakest link". This, in turn, stems from human related attributes such as behaviour, knowledge and negligence and/or the attitude of the humans involved as regards to safeguarding their information. Consequently, there is considerable information security literature available which has explored the area of human factors (Colwill, 2010, Gonzalez & Sawicka, 2002; Hawkey, Botta, Werlinger, Muldner, Gagne & Beznosov, 2008; Hinson, 2003; Jakobsson, 2007; Kraemer, Carayon, & Clem, 2009; Schneier, 2008). Thus, the area of human factors constitutes another important component of this research study.

In general, the technical controls and organisational aspects mentioned above require some degree of human involvement in the use of these controls. As stated in section 2.3, human error presents a threat to an organisation. Kraemer et al. (2009) identified and characterised elements related to human errors in a conceptual

framework. Their results showed that organisational factors such as communication breakdowns, security culture and policies are frequent causes of errors within an information security context. Thus, in order to address these human factor concerns, education is required and, to do this, organisations usually implement security awareness, training, and education programmes. Such programs are discussed in later chapters.

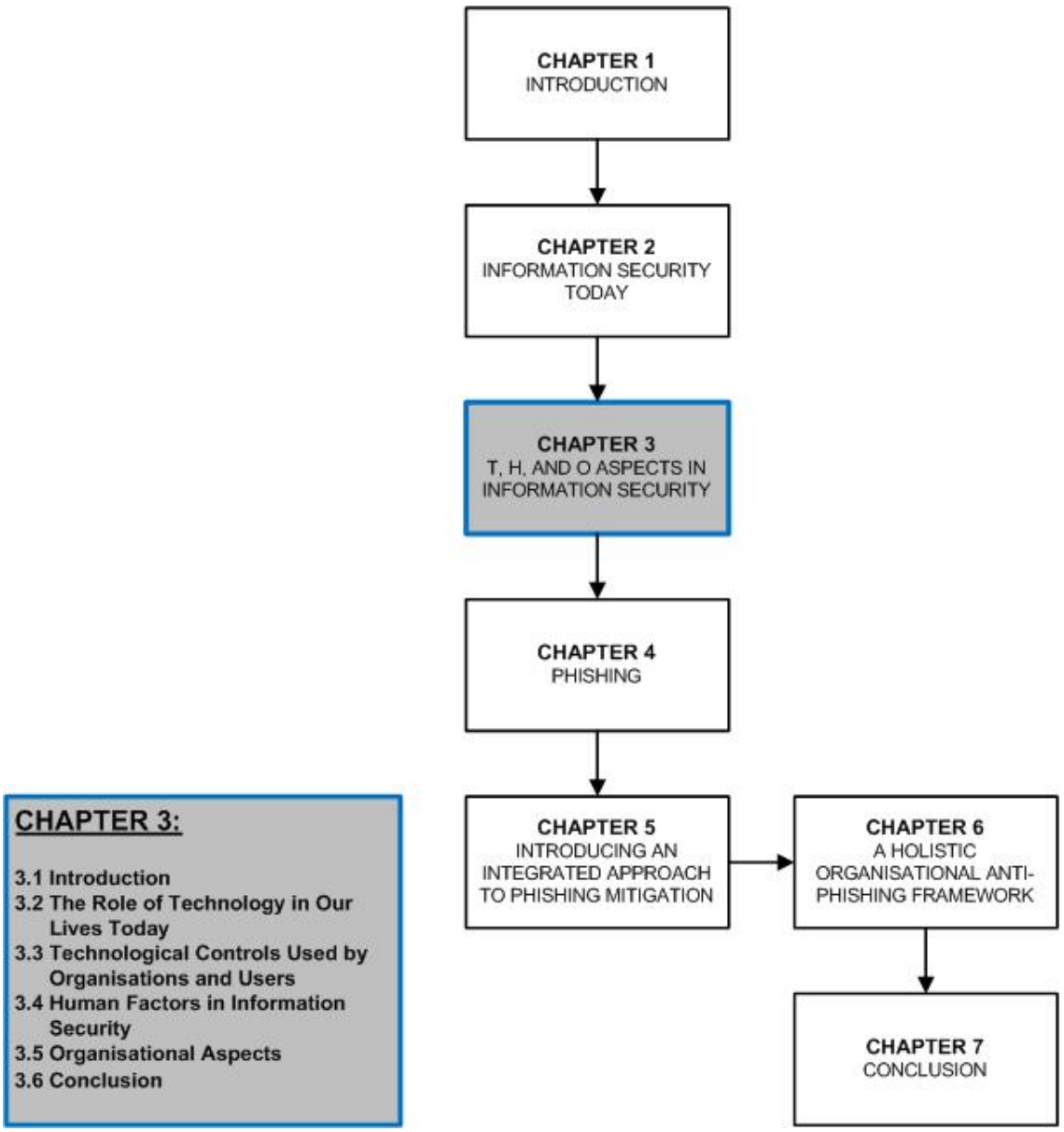
In this section, three main areas, namely, technological controls, organisational aspects and human factors, are highlighted and established as a basis of this research study. As noted by Von Solms, overlaps are evident in each of the waves discussed above. Similarly, human involvement is evident in each of the technological, human and organisational areas. This, in turn, indirectly emphasises that human factors merit the most attention when the issue of information security is addressed. Each of these three areas will be described in further detail in the next chapter.

2.6 Conclusion

This chapter emphasised the value of information by classifying it as an ‘asset’ of an organisation. The chapter further explored the background to information security and also described modern information security threats and controls. It is clear that, in view of the importance and sensitivity of certain types of information, it is essential that information be protected by appropriate methods and controls and that failure to establish adequate protection may have serious financial implications for an organisation and also its clients. Three main areas emerged on this study is based. These areas were categorised as technological controls, organisational aspects and human factors. Of these three areas, literature highlighted the fact that, in general, most of the security controls used by organisations are technological-based. The three main areas are explored in greater detail in the next chapter.

CHAPTER 3

TECHNOLOGICAL CONTROLS, HUMAN FACTORS AND ORGANISATIONAL ASPECTS IN INFORMATION SECURITY



3.1 Introduction

The previous chapter established the important role of information, IT and information security in organisations. The chapter also categorised the general security threats and countermeasures which may be used to combat such threats into three main areas, namely, technological controls, human factors and organisational aspects. In this chapter, these three main areas are discussed in more detail. The chapter begins by describing the general technological controls which are used by both organisations and users in order to counter security threats. This is followed by a discussion of the human factors and finally, the role of organisational aspects, mostly in the form of security policies and procedures, within an organisation. It will become evident from this discussion that these dimensions tend to overlap and that these overlaps are the result of human involvement.

3.2 The Role of Technology in our Lives Today

This section begins by describing the important role played by technology in our daily lives. The technological controls which are to counter security threats are then described. The section aims to argue that technology may be regarded as useful only if users find it easy to use.

From the beginning of time man's quest has been to strive continually to find new ways of improving our lives. Modern technologies, inventions and/or methods have radically changed the world in which we live and individuals are becomingly increasingly dependent on technology to perform many of their routine tasks. In other words, technology has significantly influenced our daily lives, perhaps for the better but perhaps for the worse. The ongoing development and improvement of new technological products offer a wide range of new possibilities to make our daily lives healthy, safe, independent, efficient, entertaining and comfortable. In other words, energy-friendly and sustainable solutions are helping to improve the environment in which we live (TUE, 2012). For example, improved healthcare has resulted in human beings living longer and also receiving effective treatment and complicated surgical procedures which may have been impossible years ago. In addition, technology has provided us with new methods of communication and entertainment (TUE, 2012).

The explosion of the World Wide Web, smart phones, online shopping, social networking sites, 3D television and games etc. have taken the world by storm.

Within an organisational environment, technology is being used by organisations to enhance their business operations and, simultaneously, to protect their systems from security threats. However, there is also a 'dark side' in the use of technology with threat agents also making use of technology for malicious and illegal purposes that may inflict severe damage on both people and information systems. Sexual predators may make use of social networking websites to lure young children into engaging in sexual activity (e.g. sexting) while fraudsters may also use the Internet to lure people into giving up their money to some cause (e.g. scams). All of these threats make use of techniques to inveigle individuals into performing some actions. These techniques will be discussed in section 3.4.

The effectiveness of technology depends on the ability of people to use the technology correctly as well as to trust in its usefulness. Technology is often stigmatised as being too complex to use. To address these concerns, developers require an understanding of both the human and technological aspects of technology. The human aspects would include usability, ergonomics, perception, cognition, decision making, social psychology, consumer behaviour and environmental psychology (TUE, 2012), while understanding the technological aspects requires a comprehensive knowledge of the technical details of the product as well as of the environment in which the product will function. For example, developing software requires that a programmer possess technical knowledge as regards graphical user interface design, programming languages, operating systems and troubleshooting, and so on, while understanding the human aspects requires that the programmer consider the people who are going to be using the finished product. This is extremely important as technology must be easy to use while it must also be of some use or benefit to the users as it will otherwise either not be used correctly or it will not be used at all.

This section indicated that most technologies are designed to support humans in their performing of their tasks. However, it is essential to understand that, although technology has many benefits, it also has limitations, risks and vulnerabilities. There is no perfect technology which exists and, as a result, humans are constantly striving

to develop new technological products with the aim of improving previously released versions (e.g. cell phone functions, software updates). Thus, technological development is an ongoing process which is constantly seeking for new improvements. This, in turn, also affects the human element as humans need to be educated as regards any new technological development in order to operate the technology correctly.

The next section describes some of the common technological controls which are used by organisations and users to help protect their information.

3.3 Technological Controls used by Organisations and Users

The previous section pointed out that technology is used across many domains and also that it has both benefits and drawbacks. This section discusses some of the common technological controls which are used by organisations to protect both their information and their information systems. Some of the limitations in these technological controls are also revealed.

Generally, information security controls may be subdivided into the following three categories, namely, physical controls, technical controls and operational controls (Thomson, 1998, p. 29; Van Niekerk & Von Solms, 2004a). Information security literature often refers to technological controls as 'technical controls' and includes both hardware and software aspects in the concept. Technological controls may be defined as those control measures that either use or implement a technical solution in order to reduce the risk of loss within an organisation (Whitman & Mattord, 2010, p. 335). Section 2.2 established that information is an organisational asset and, thus, organisations tend to use technical controls to protect their both information and their computer systems from threats. However, section 2.3.2 pointed out that threats also use technology but for alternative motives such as carrying out attacks on victims. This may be one of the reasons why most organisations treat information security as a technical issue solely and why organisations expend a large portion of their resources on implementing technological controls. It is generally believed that technical solutions such as firewalls, anti-virus programs etc. are sufficient to secure information (Hinson, 2003; Whitman & Mattord, 2012).

Technological controls do play an essential role in the protection information as these technological measures are able to control access and to protect information to some extent. However, it is often overlooked that technology are used and relied upon by people (Hinson, 2003; Mann, 2008). In addition, the manner in which technological controls are used and managed by people presents another cause for concern. This point is emphasised by Hinson (2003) who states that few organisations understand their information security problems in sufficient detail to ensure that they specify the appropriate technical solutions aligned with their requirements. The following subsection briefly discusses common technological controls which are applied at an organisational level.

3.3.1 Access Controls

Access controls typically involve four key processes, namely, identification, authentication, authorisation and accountability. Identification involves identifying the entity that is requesting access to a logical or physical area (Whitman & Mattord, 2010, p. 335). This is a single piece of unique information such as a name or initials and a surname. Authentication involves confirming the identity of the entity seeking access to a logical or physical area and usually involves verifying either a password or a private identification number (PIN). Once authentication has taken place, authorisation determines the actions which the entity is allowed to perform in the logical or physical area. One of the most common methods of authorisation is performed by a system which verifies the entities details and then grants access to resources or privileges based on the access rights (Whitman & Mattord, 2010, p. 336). Finally, accountability documents the activities, through system logs, of the authorised entity and systems. The management of these access controls is documented in a formal access control policy with this policy dictating the way in which access rights are granted to both entities and groups.

Organisations also usually apply access controls in the physical environment. In this context the processes of identification, authentication, authorisation and accountability may be described using a practical example. An individual enters a building and will have to be identified by security personnel as either a visitor or a member of staff (identification). The individual provides his/her name and surname to the security personnel. The security personnel then verify the individual's details

(authentication) and offer the individual permission to enter the building. The security personal will also direct the individual to certain parts of the building which the individual is allowed to enter (authorisation). This may be enforced by using a card which allows the individual access to certain areas of the building. The security personnel also records the individual's name as well as the date and time of entry in a log book (accountability).

Several other forms of technology are available to protect information but they are usually used to identify and restrict outsider access. The latter statement is supported by the following. An information security breaches survey which was carried out by United Kingdom government Department for Business Enterprise and Regulatory Reform (BERR, 2008). This survey reveals the following in respect of the businesses surveyed:

- 55% have a documented security policy in place
- 40% provide ongoing security awareness training to staff
- 14% use strong, multifactor authentication
- 11% have implemented BS7799/ISO27001
- 99% back up their critical systems and data
- 98% use software that scans for spyware
- 97% filter incoming email for spam
- 97% protect their websites with a firewall
- 95% scan incoming email for viruses
- 94% encrypt their wireless network transmissions.

This survey reveals that technological controls are used mainly to prevent outsider access. However, the survey also reveals that organisations appear to have neglected potential insider threats. Social engineers would almost certainly take advantage of the opportunity offered by this omission.

3.3.2 Firewalls

A 'firewall' is a term which is often used in the engineering discipline. A physical firewall is a concrete or masonry wall which is constructed in buildings and which is

used to restrict a fire from spreading to other parts of the building (Whitman & Mattord, 2010, p. 345). Firewalls are also used in the aircraft and automotive industries where a firewall typically comprises insulated metal/material which keeps the heat from the engine compartment separated from the interior where the passengers are seated.

In the context of information security, firewalls are used by organisations for the purposes of network security. As such, firewalls may protect the computers on an organisational network from unauthorised intrusions. The firewall may be either a physical computer terminal (e.g. proxy server) or a software program. Microsoft operating systems have built-in firewall software. Firewalls include technologies such as packet filtering which examines every incoming or outgoing packet header, thus preventing specific types of information from moving between the outside world (mistrusted public network such as the Internet) and the organisation's internal network (trusted internal network such as the Intranet). These packets may be accepted as necessary or rejected by a filter. Filtering may be based on IP address, packet type, port request, and so forth (Whitman & Mattord, 2010, p. 346).

The selection of what the filter must accept or reject is determined by its configuration rules. These rules may be automated to block suspicious websites and to restrict certain websites from being accessed by the employees within the organisation. The web filter software may classify prohibited websites into categories for example, pornographic websites, unethical, phishing, and so forth. In addition, the firewall may also block users from both excessive downloading and the use of instant messaging services and video streaming. Configuring firewalls is an important and complex task which is performed by IT/technical staff members who have usually undergone specialised training in network administration.

3.3.3 Intrusion Detection and Prevention Systems

Intrusion detection and prevention systems (IDPSs) act in the same way as burglar alarms in the real world (Whitman & Mattord, 2010, p. 353). For example, if a building window or door is broken then an alarm is activated. This alarm may be either audible (noise or beeps) or visible (lights flashing). However, the alarm may also be silent but inform the security company concerned. In the context of

information systems, technical staff members configure the alarm and its alarm levels. The alarm may also be configured to notify an external information security service organisation. There are several different and complex IDPS configurations, namely, host-based, network-based, signature-based and statistical anomaly-based (Whitman & Mattord, 2010, p. 355). Whitman and Mattord (2010 p. 354) maintain that a system which incorporates IDPS technology should prevent attacks by accomplishing the following:

- Terminate the network connection or the threats user session when attacked
- Change the security environment by reconfiguring network devices such as firewalls, routers and switches to block the threat from gaining access to the system
- Change the threats content to render it benign. For example, remove an infected email attachment before the email reaches the recipient.

3.3.4 Remote Access Protection

Before the Internet, organisations and individuals were able to connect with each other through the use of private networks (Whitman & Mattord, 2010, p. 357) through dial-up or leased-line connections. Dial-up connections are less sophisticated than Internet connections as a simple username and password are sufficient for authentication and, as a result, there was a need to strengthen this authentication process. Technologies which have improved this process include RADIUS systems, Challenge Handshake Authentication Protocol (CHAP) systems and other systems which make use of strong encryption technologies. According to Whitman and Mattord (2010, p. 357), the most prominent of these approaches are RADIUS and TACACS.

3.3.5 Wireless Networking Protection

Computer networks have evolved from the traditional physical connections which used cables to the wireless connections of today. The modern smart phone is a good example of this radical change. According to Whitman and Mattord (2010, p. 359), wireless network technology is an issue of concern for information security professionals. Wireless networks are of benefit to organisations as they are

extremely cost effective as compared to cables. However, security threats also take advantage of the fact that there are no physical connections. Certain threats to wireless networks are known as ‘war driving’ (Whitman & Mattord, 2010, p. 359). The threat moves/drives along a geographical area or building scanning for any open or unsecured wireless network. It is, thus, essential that an organisation ensure that it uses relevant encryption protocols to secure its wireless network (e.g. Wired Equivalent Privacy, Wi-Fi Protected Access). VPNs and firewalls may also be used to safeguard the wireless network (Whitman & Mattord, 2010, p. 361).

At this stage, the technological controls which have been discussed are at the organisation level. Mitnick and Simon (2002, p. 16) believe that these controls are necessary to a corporate security programme. The next paragraph discusses the technological controls which are often applied at the user level, for example, security on the individuals’ own personal devices.

3.3.6 Anti-Virus Solutions

As a result of the general lack of information security knowledge, end-users tend to think any computer-related problem is caused by viruses and, thus, most end-users are familiar with the role of anti-virus programs. Traditionally, anti-virus programs were limited to detecting and removing viruses only. However, modern anti-virus programs have become extremely sophisticated in their defence mechanisms. It is common for these mechanisms to be set active automatically and, thus, they do not require very much human involvement.

Depending on the protection level of anti-virus software (e.g. Internet Security) and the manufacturer (e.g. Kaspersky), most anti-virus programs incorporate a variety of integrated defence tools. For example, Avast Internet Security 7 includes controls, namely, a firewall, mail shield, script shield, web shield, file system shield, P2P shield, instant message shield, behaviour shield and network shield (Hubpages, 2012). These shields are also not uncommon in other anti-virus programs. Some anti-virus programs may also remove malware. The hyperlinks contained in phishing emails may be infected with malware. Mail shields are capable of detecting and removing phishing emails and spam (Hubpages, 2012). Figure 3.1 below illustrates that the ‘web shield’ control is able to scan websites automatically and to display the

results to the user. This, in turn, assists end-users in identifying whether a website may be regarded as either a legitimate (safe) or a spoofed website (forged) based on the web shield's rating.

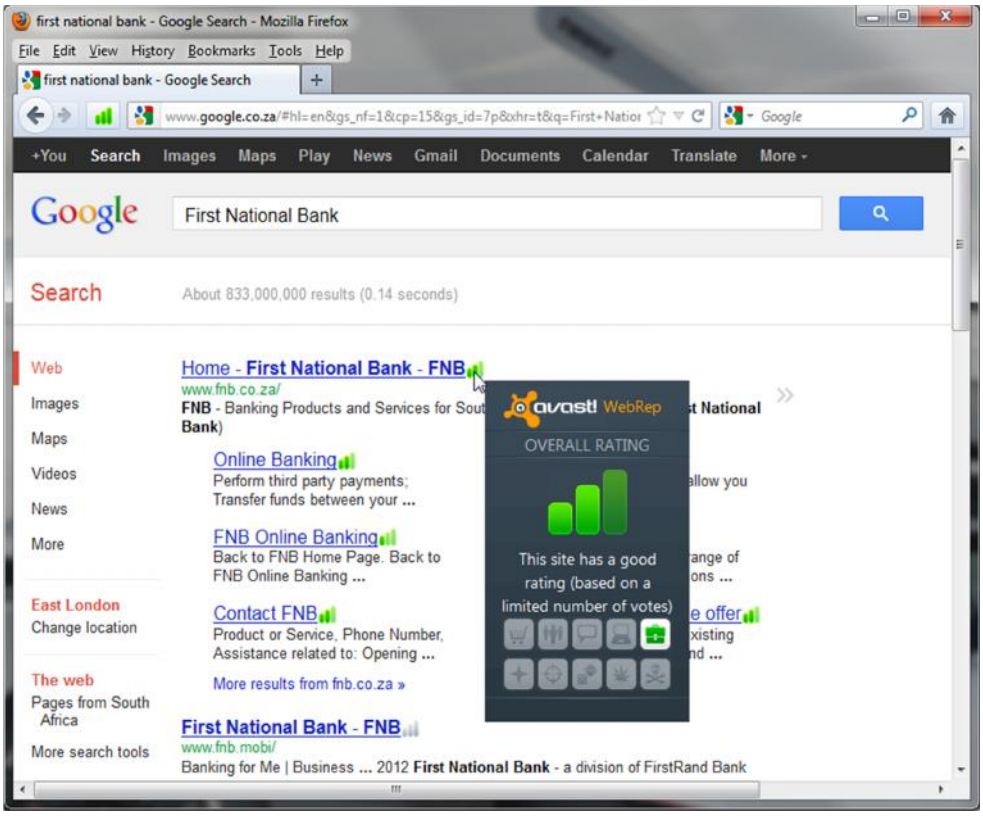


Figure 3.1: Web link scanner integrated in anti-virus program

3.3.7 Web Browsers

Web browsers enable users to navigate through web pages. However, Wadlow and Gorelik (2009) believe that web browsers also pose security problems to developers and users. There are a variety of popular web browsers, for example Microsoft Internet Explorer, Mozilla Firefox, Opera, Apple Safari, Google Chrome and so on. Most of these web browsers are similar in functionality, but they are also competitive as far as security is concerned as most have similar built-in technological defences against threats (Accuvant Labs, 2011). Browser developers have devised several ways in which to combat security threats, especially phishing attacks with developers

focusing primarily on heuristics in order to detect an attempted visit to a fraudulent site, phishing website warnings and an increase in login security (Wadlow & Gorelik, 2009).

Plug-ins is programs which extend the capability of a browser are often used to enhance multimedia (Shelly & Vermaat, 2011). Most browsers, for example, Mozilla Firefox, have made provision for browser plug-ins or add-ons. Should users require additional functionality or security protection, they are able to download plug-ins for free. Popular browser plug-ins include: Adobe Acrobat Reader, Adobe Flash Player, Java, Quicktime, and Microsoft Silverlight (Shelly & Vermaat, 2011). However, web browser plug-ins also has security weaknesses. According to a report by Alfreds (2012), Adobe Flash is one of the programs which are the most vulnerable to threats on Windows-based computers. The literature has indicated several developments which have focused on browser security and especially involving browser plug-ins. A Mozilla Firefox and Google Chrome web browser plug-in termed Adblock Plus automatically blocks unwanted advertisements (known as adware) from appearing in web pages. If these advertisements are clicked on they may, potentially, redirect users to harmful websites.

Most web browsers incorporate phishing filters and pop-up blockers. Another security feature in web browsers is warning alerts. These alerts display information to the user. An example of a web browser warning is illustrated in Figure 3.2 below. In this example, the URL <http://www.yotube.com> was used instead of <http://www.youtube.com>. These are techniques which are often used by phishers and which rely on negligence on the part of the user as regards paying adequate attention to the structure of URLs. In this example, the web browser served as an effective security control as it had detected the URL <http://www.yotube.com> as a spoofed-website.

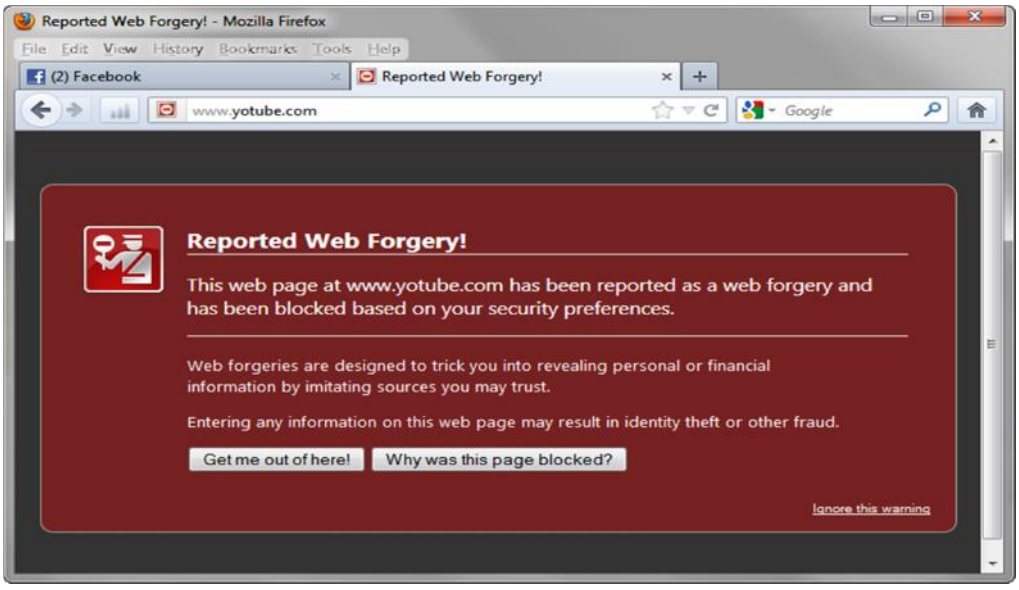


Figure 3.2: Web browser security warning

When browsing the Internet, the web browser may require cookies to be enabled. According to Wadlow and Gorelik (2009), a cookie is a legitimate mechanism for storing information about either a user or a session. E-commerce websites allow users to purchase goods and services online using credit cards or digital cash. E-commerce websites are popularly known to store user data as cookies, for example, when users log onto websites using their usernames and passwords. However, cookies also pose security risks as the information may be stolen, forged, poisoned, hijacked or abused as regards denial of service attacks by threats (Wadlow & Gorelik, 2009). In order to control this, it is recommended that users remove this information stored by the web browser. This process is known as 'clear history and cookies' and most browsers have easy to use functions to achieve this. According to Ollmann (2008), most web browsers should

- disable all window pop-up functionality
- disable Java runtime support
- disable ActiveX support
- disable all multimedia and auto-play/auto-execute extensions
- prevent the storage of non-secure cookies

- ensure that it is not possible to run any downloads automatically from the browser and that downloads must instead be downloaded onto a directory for anti-virus inspection.

3.3.8 Email Client

The email client is one of the most frequently used software applications on the computer systems of users and is used to transmit messages electronically over the Internet. However, some messages may, potentially, contain security threats. Most email clients are capable of automatically blocking emails containing 'dangerous' attachments and suspicious images, thus preventing users from executing or viewing harmful content (Ollmann, 2008). These images may contain embedded hyperlinks and, if clicked on by the user, may direct them to either spoofed or malicious websites. Email clients, such as Microsoft Outlook, maintain a list of 'dangerous' attachment formats and are able to prevent users from opening them (Ollmann, 2008). In order to ensure that the email client continues to do this, it is essential that users ensure that their software is regularly updated. Email clients may also include digital signatures. According to Shelly and Vermaat (2011, p. 395), digital signatures are often used to ensure that an imposter is not participating in an Internet transaction. The purpose of a digital signature is to verify whether the sender is whom he/she claims to be. This is made possible by an encrypted code attached to an email in order to identify the sender.

Popular web-based email clients such as Google Mail and Yahoo Mail may be subject to a wider variety of security threats, for example phishing, spam mail, viruses than email application clients. The use of an organisationally accepted email client gives trained technical staff the opportunity to increase security as they are able to configure the email client to block unwanted or suspicious emails. Technical staff should disable HTML functionality in all email client applications which are capable of either accepting or sending Internet emails (Ollmann, 2008). Security may also be further enhanced if emails are in plain-text format while, ideally, the font style should be fixed as 'Courier' (Ollmann, 2008). Ollmann (2008) further adds that users should not be able to use other email rendering options such as Rich-text format or

Microsoft Word editors as these formats possess security flaws which may be exploited by phishers. Ideally, users should not be able to access the contents of the email attachment directly from within their email client application (Ollmann, 2008).

3.3.9 Software Updates

Updating the software on a computer system may also be regarded as a control measure designed to prevent viruses from exploiting any software vulnerabilities in a computer system. It is essential that programs be updated often in order to increase the protection level against modern security threats. These updates include enhancements to security, modifications to device drivers, bug fixes (code errors), application software and, most importantly, the web browser and email client (Shelly & Vermaat, 2011). Typically, most application programs, including operating systems, have an automatic update feature (Shelly & Vermaat, 2011). For example, Microsoft Update not only seeks updates for Microsoft-related products but also for the manufacturers of other application programs which may be installed on the user's computer system. This feature is also evident in mobile phone platforms. For example, Blackberry® smart phones alert users with notifications of the available software updates for applications installed on their device. In addition, users should ensure that their computer update settings are configured to be set to update on the Internet automatically in order to reduce the risk of users forgetting to update their software manually.

3.3.10 Password Manager Software

Password manager software may also serve as an effective technological control, especially as users often forget their passwords and unsuspectingly submit sensitive information to spoofed websites as a result of ignorance. A popular password manager application, for example LastPass, allows users to create different user profiles for each website. As a result, the password manager application is able to fill in the user's personal information automatically on websites, both accurately and safely. An added benefit is that the password manager will perform such activities on legitimate websites only and not spoofed websites. As such, it protects users against identity theft as the personal data is encrypted on the user's computer.

3.3.11 Hide IP Address Software

Threat agents may gain access to a user's computer by using the computer's Internet Protocol (IP) address. However, software programs exist which are designed to conceal one's computer's IP address. This, in turn, allows one's online identity to be kept a secret as the program creates a fake IP address.

3.3.12 Utility Security Suite Software

It is common practice today to find computer devices being sold with security software having been preinstalled by the manufacturer, for example, Hewlett Packard security suite. Using this software, users are able to encrypt their hard disks, backup the data, and increase the system access security with fingerprint scanners or face recognitions. However, this, in turn, emphasises the importance of users being knowledgeable about how to use these programs.

It emerged from this section that there is a wide variety of technological tools available with which to combat security threats and protect systems on both a personal level and an organisational level. However, there are many more technological tools which exist other than those discussed in this section and this growth is expected to continue. In this vein, Mitnick and Simon (2002, p. 13) indicate that developers will continually invent improved security technologies, thus making it increasingly difficult for security threats to exploit technical vulnerabilities. However, in each of these controls there are a few potential problems. Firstly, there are potential problems in the technology itself (i.e. software vulnerabilities) which threat agents seek to exploit with each new feature creating more security problems and additional complexity (Orgill et al., 2004).

Secondly, all of these technological controls are operated and managed by people and, as a result, there is a reliance on these people possessing the required skills to use these technological controls correctly. However, this is difficult to manage especially in view of the fact that technology is changing rapidly. Thus, in order to address this concern, many software developers are focusing on automating technology (Herath & Rao, 2009). This, in turn, again emphasises the need for technology to function correctly. Clearly, these two problems mentioned above

provide threat agents with an opportunity to exploit the human element (i.e. the operator behind the technology) in order to acquire information. The human factors will, thus, be discussed in the following section.

3.4 Human Factors in Information Security

Mitnick and Simon (2002, p. 25) state powerfully that "[d]espite our intellect, we humans - you, me and everyone else - remain the most severe threat to each other's security". Thus, this section will discuss the role that human related factors play in information security. In order to do this, social engineering techniques will be discussed in detail as an understanding of social engineering techniques will reveal the human attributes that are vulnerable, in particular to both social engineers and to phishing threat agents. This section will also reveal the involvement that exists between technology and humans.

Every individual in this world is unique with all individuals being characterised by different experiences, knowledge, interests, emotions, cognitive abilities, culture and personality traits which, ultimately, shape their behaviour. Thus, if people are not currently demonstrating the correct behaviour, it is an extremely challenging task simply to alter this behaviour. This, in turn, emphasises the important role played by human factors – an issue which is of key importance to this study. Human factors play a significant role in information security and, thus, for many years human factors have been the focus of a great deal of interest in the information security community. In much of the literature on information security which has been published the writers consistently reiterate that humans are the weakest link in information security (Mitnick & Simon, 2002; Schneier, 2000). Ironically, humans are often both the cause for security incidents, which are caused by their unacceptable behaviour and lack of knowledge, as well as functioning as security control measures. Accordingly, security awareness, training and education are often proposed as a solution to addressing the problem of human behaviour and also to equip these human beings with the requisite knowledge to deal with security threats. The next subsection elaborates on the attributes of human behaviour and knowledge.

3.4.1 Human Behaviour and Knowledge

Many of the security-related problems in organisations have been linked to employee behaviour (Thomson, Von Solms, & Louw, 2006) with the behaviour and actions of employees determining, to a large extent, the effectiveness of information security practices (Dhillon, 2001, p. 165). The actions and behaviours of employees are particularly important as almost all information systems rely on the human element (Berti & Rogers, 2004).

As many as 80% of all major security failures may be the result of poor security behaviour on the part of employees rather than poor security solutions (Leach, 2003). Studies conducted by Lim, Chang, Maynard, and Ahmad (2009), Lim, Ahmad, Chang, and Maynard (2010) support the contention that the main threat which agents pose to information security arises as a result of careless employees who do not comply with organisational security policies and procedures (Pahnila, Siponen, & Mahmood., 2007; Workman, Bommer, & Straub, 2008). As such, it is essential that organisations realise that they must not rely on merely implementing technological controls and organisational policies in order to prevent security threats. This, in turn, has emphasised the need to understand human factors.

According to Van Niekerk (2005, p. 21), human factors may be classified into the following two dimensions, namely, human cooperation (behaviour) and knowledge. To a large extent, human cooperation depends on the attitudes of individuals and, thus, it is essential to ensure that the attitude of individuals is such that it results in the desired behaviour (Van Niekerk, 2005). This, in turn, requires that individuals are in possession of knowledge relating to *what* they should do and *how* to perform their security related functions. This further requires that individuals understand their roles and responsibilities and that they are adequately trained to perform these roles and responsibilities (NIST 800-16, 1998, p. 3). This aspect will be further explained in section 3.5.4.

In order to address the issue of human behaviour at an organisational level, numerous researchers have recommended the establishment of an information security culture. Information security culture may be defined as “the totality of patterns of behaviour in an organization that contribute to the protection of information of all kinds” (Dhillon, 1997). Such a culture may come about if employees

begin practising information security unconsciously or, in other words, when practising information security becomes a natural aspect of the daily activities of every employee (Schlienger & Teufel, 2003). However, this would, in turn, require a change of behaviour so that employees would then demonstrate the correct attitude. In addition, employees must be trained so that they acquire the relevant knowledge which is needed to practise information security, for example, security education in organisational policies and procedures. However, more importantly, it is essential that the members of senior management demonstrate their support for information security by being involved in security activities. If employees observe other colleagues habitually practising security, this will help to influence them to do the same unconsciously.

The next subsection discusses social engineering. Once social engineering is understood, the human factor concerns will emerge.

3.4.2 Social Engineering

Social engineering is regarded as an *art, method* or *technique* which is used to manipulate people into performing actions (DeFino et al., 2010). Mann (2008) defines social engineering as a *practice* that may be used to manipulate people, by using *deception* as the primary method, to influence the *decisions* and *trust* of victims in such a way that they either give out information or perform certain actions. It is apparent in both these definitions that psychological methods are being used by social engineers to gain information from their victims.

It is due to the hacker turned security consultant, Kevin Mitnick, that the term ‘social engineering’ became commercialised. Mitnick was most famous for using social engineering techniques, instead of hacking, to extract information from unsuspecting individuals. Mitnick later wrote a controversial book entitled *The Art of Deception*, in which he describes, based on his own experiences, how and where he applied these techniques (Mitnick & Simon, 2002). The book reveals how simple it is to trick people into divulging information and particularly insiders in an organisation, despite their technological protection. The book also gives many other real-world accounts of the ways in which humans beings may fall victim to social engineering attempts.

Social engineering may be broadly categorised as human-based and computer-based (DeFino et al., 2010). As pointed out earlier, threat agents may attempt to exploit vulnerabilities in either the hardware or the software in order to gain information. However, they may also attempt to exploit vulnerabilities in human behaviour in order to do the same (Microsoft, 2009). The latter may be considered as an attack against the human interface of the targeted system (Microsoft, 2009) and is regarded as the most effective and most convenient method for threat agents. Thus, social engineering may be considered as a hacking technique against humans rather than against systems.

Section 2.2 described how organisations have been affected by IT as a result of the rapid expansion of organisational networks and the Internet. Consequently, many working individuals are not given the opportunity to communicate directly with others and vice-versa. Most individuals now sit for long hours in front of their computer devices, busy with activities involving email, social networking websites or instant messengers. However, this, in turn, may result in people becoming complacent and overlooking certain security risks. This then creates an opportunity for the social engineer to use these same technologies to trick users into either performing certain actions or disclosing information. The next subsection discusses some of these social engineering techniques.

3.4.3 Social Engineering Techniques

There are a number of intelligent social engineering techniques that threat agents use in order to gain personal information from their victims. Some of these techniques may be combined with technology to enhance their effectiveness (Orgill et al., 2004). This, in turn, results in another common form of social engineering which is referred to as *phishing.* Phishing usually happens through email and phishers are most interested in obtaining passwords as well as credit card and account numbers. Phishing will be discussed in depth in the next chapter.

Mitnick and Simon (2002) classify social engineering attacks into the following three main approaches, namely, direct requests, contrived situations and personal persuasion. They believe that ‘direct requests’ are the least successful approach because the threat agents will clearly and directly ask for the information they

require. However, this may cause the victim to become suspicious. On the other hand, the 'contrived situation' approach is more enhanced in comparison to direct requests as it involves the threat agent fabricating a story to make the story appear more convincing. This, in turn, causes less suspicion than the previous approach because of the creative aspect of the attacker's story (Mitnick & Simon, 2002). 'Personal persuasion' is more complex as the attacker aims to manipulate the individual into believing that he/she is actually providing the information willingly to the threat agent. As a result, the victim does not perceive any risk (Mitnick & Simon, 2002). Applications of social engineering techniques which may be used to acquire personal information or to elicit certain actions from individuals are described below.

3.4.3.1 Pretexting

Pretexting is a hacking technique involving the telephone (DeFino et al., 2010). It involves the act of creating and using a preconceived scenario to engage a targeted victim in such a manner that will increase the chances of the victim divulging information or performing actions that would not usually take place under normal circumstances or conditions. Today, many sales and other transactions are conducted over the telephone, primarily because the telephone is so very convenient. Organisation representatives authenticate the clients to whom they are speaking by quoting their social security numbers, physical addresses and other personal details. However, this approach also enables a threat agent to use social engineering techniques to carry out such transactions.

This technique requires prior research into and information of the targeted victim in order to establish credibility and legitimacy effectively in the victim's mind so that the threat agent gains the victim's trust. For example, this technique may be used to trick an organisation into disclosing customer information. The threat agent may pose as a private investigator in order to obtain telephone records, utility records, banking records, etc. from the organisation's employees. This, in turn, enables the threat agent to target a larger population group than would otherwise have been the case. Pretexting may also involve impersonating co-workers, police officers, financial institutions, and suchlike or any individual who is in a position of responsibility, authority or power. The victim is then deceived by the threat agent as he/she may

feel obligated to disclose confidential information. In terms of this method, an authoritative voice, an authoritative tone, quick thinking and physical appearance are all factors which are considered to increase the effectiveness of the method.

3.4.3.2 Diversion Theft

This technique is usually used against organisations that either transport or deliver properties or goods. Social engineers persuade the authorities responsible for a delivery to transport it elsewhere. With the property redirected to a different recipient, the social engineers/thieves persuade the driver to offload the package near to or away from the new recipient's address in the guise that the package is either being sent out or it is urgently required somewhere else. In this instance, the social engineering techniques applied by the thieves are both well rehearsed and effective.

This section presented social engineering as the basis for acquiring confidential information from users without having to resort to technical methods such as hacking. The section also revealed that social engineers are able to carry out their attacks in a number of different ways, for example, they may telephone or email users, pretending to be an official or legitimate entity in order to gain illicit access to systems. The next subsection aims to discuss those factors that render humans beings susceptible to social engineering techniques.

3.4.4 What makes Humans Vulnerable to Social Engineering Techniques?

Understanding the human mind is one of the most challenging research areas. It is not possible to programme humans merely by the push of a button. This section will discuss some of psychological components that are triggered by social engineers. Gragg (2002) believes it is essential to understand these psychological aspects as it will convey why and how humans are falling victim easily to social engineering techniques. Accordingly, the following paragraph categorises and describes those psychological triggers which may be used to persuade and influence people.

- **Strong affect** is introduced when the social engineer makes a statement at the beginning of the interaction that triggers strong emotions on the part of the victim. This strong emotion may include, panic, fear and even excitement. For

example, it may be the promise of a prize worth thousands of dollars or panic that a bank account is about to be terminated.

- **Overloading** is used on victims in order to create confusion. The social engineer will provide the victim with too much information to deal with quickly. This, in turn, affects the victim's logical functioning and may produce 'sensory overload'. Gragg (2002) further states that, with too much information to process, people become 'mentally passive'.
- **Reciprocation:** According to Gragg (2002), it is common in social interactions to find that, if someone gives us something or promises us something, individuals are inclined to return the favour. Reverse social engineering makes use of the reciprocation trigger with the hacker appearing as a hero who is ready, willing and able to solve the target's problems. Thus, even before the problem is resolved the target feels indebted to the hacker.
- **Authority:** People are more willing to respond to requests when it stems from someone who is in a position of authority. For example, a policeman asks a driver to show the policeman his/her driver's license. However, it is essential that the authority figure appear legitimate based on both appearance and behaviour.

Each of these abovementioned triggers which are used by social engineers aim to instil trust in their victims. Trust through deception is an important component if social engineering is to be effective. For example, in the real world, if a well-dressed, attractive individual approaches one for directions, one would probably be willing to help this individual. Few people wish to be unhelpful and, when people are placed under pressure to perform actions, they generally lack the appropriate assertiveness to refuse (Parsons, McCormac, Butavicius, & Ferguson, 2010). Mitnick and Simon (2002) point out that it is an integral part of human nature to trust others, especially when there is no apparent reason to be suspicious. However, if a stranger requests personal information one may become increasingly suspicious. Nevertheless, if the individual requesting the information were wearing a uniform, one would feel safer in sharing such information while, if an individual were wearing tattered clothing and had a scarred face, one would probably try to escape as quickly as possible.

According to Workman et al., (2008), susceptibility is significantly associated with the likeability and trustworthiness of individuals. Within an information security context, if a phishing email or spoofed website appears legitimate, then it would probably not arouse the victim's suspicions. On social networking websites such as Facebook this approach may be made even more effective. The threat agent would have to create a profile, put up an attractive profile picture (which would most likely not be their personal picture) and begin randomly sending out friend requests using their false profile as bait. Once the users have accepted the request, the threat agent may then establish a relationship of trust with his/her victims.

Deception manipulates the human mind as it focuses specifically on the attributes of human decision-making known as cognitive biases. A social engineer exploits these decisions or tendencies of humans by using techniques that exploits either emotions or cognitive or cultural biases. The effectiveness in using social engineering techniques, rather than the older, conventional methods, arises from the fact that that no technical cracking knowledge or hacking experience is required. Social engineers have realised that it is far easier to obtain personal information through deception than by spending excessive time, resources and money on hacking into a system (Mitnick & Simon, 2002). According to a report by Gartner (2005), "Many of the most damaging security penetrations are, and will continue to be, due to Social Engineering, not electronic hacking or cracking… Social Engineering is the single greatest security risk in the decade ahead."

This section revealed that humans may be easily manipulated into trusting entities based on the appearance of those entities and the use of fabricated stories. This, in turn, is made possible by social engineering techniques which focus on specific psychological triggers of the human mind. However, this poses security risks to organisations and has resulted in the need to change the behaviour of users. The next section will discuss organisational aspects. The influence of human behaviour on the organisation will be evident in this next section.

3.5 Organisational Aspects

The previous section described human factors. Humans are involved in using technology and they are also involved in various activities related to organisations.

Predictably, human factors are once again going to constitute a security issue that will have to be addressed in this section. The section focuses on two parties, namely, the organisation and its employees. Accordingly, this section will discuss the way in which human factors may be managed by the organisation.

ISO/IEC 27002 (2005, p. 23) regards most of the components specified in this section as managing human resources. Senior management is responsible for the welfare of the organisation. However, typically, in larger organisations with the sheer number of employees, it is difficult for management to ensure that employees follow orders and behave securely (Von Solms & Von Solms, 2004). This situation is further exacerbated by the fact that the size of the organisation may result in limited communication between senior management and employees on the operational level. Consequently, organisations are forced to communicate their rules and regulations by establishing of policies. Von Solms and Von Solms (2004) believe that policies may be perceived as communication documents from management. As such, the next section will define and discuss organisational policies.

3.5.1 Organisational Policies and Procedures

Whitman and Mattord (2010) define a policy as “the set of organisational guidelines that describe acceptable and unacceptable behaviour of employees in the workplace”. One of the reasons for organisational policies is to enable management to direct appropriate behaviour on the part of both its employees and external parties involved with the organisation. Procedures, on the other hand, refer to methods which are put in place by the organisation to enable employees to accomplish the objectives of the organisation (Whitman & Mattord, 2010, p. 517).

Von Solms and Von Solms (2004) believe that policies are particularly important as they provide the foundation from which security programmes and security practices may be derived. Organisations may have in place several different types of policies including recruitment policies, acceptable usage policies, employment policies and so forth. It is interesting to note that Barman (2001) believes that organisations may often have comprehensive employee policies but they do not necessarily have ‘information security’ policies. Furthermore, he states that when organisations do

have an information security policy, such a policy is often extremely minimal as compared to the organisation's their other policies. In this study, policies are related to information security and the next subsection will discuss this issue.

3.5.2 Information Security Policy

Mitnick and Simon (2002, p. 245) define organisational security policies as clear instructions that provide guidelines for employee behaviour as regards safeguarding information, while Danchev (2003) states that developing a security policy is the first measure which is needed to reduce the risk of the unacceptable use of an organisation's information resources. According to ISO/IEC 27002 (2005, p. 7), the objective of an information security policy is to "provide management direction and support for information security in accordance with business requirements and relevant laws and regulations". However, before this process may begin, it is essential that senior management demonstrate its commitment to and support for information security.

Leadership is important in this regard because, if senior management does not demonstrate its support, then it unlikely that the rest of the staff would demonstrate the required behaviour (Leach, 2003). However, if management is to demonstrate its commitment and support, then the organisation's security policy document must include a statement of management's intent, supporting the goals and principles of information security aligned with the business strategy and objectives (ISO/IEC 27002, 2005, p. 5). It is imperative that employees be educated about it and that they are aware of organisational policies and procedures and, most importantly, the information security policy of the organisation. Accordingly, the policy must be communicated to all the employees of the organisation using a method that is relevant, accessible and understandable to the intended audience (ISO/IEC 27002, 2005, p. 7).

However, as pointed out by Von Solms and Von Solms (2004), despite the fact that employees may be informed about the policies, they may not necessarily obey them. In order to address this issue, Von Solms and Von Solms (2004) recommend that a group culture be cultivated so that employees will comply with the vision of management. This may be done by expressing collective values, norms and

knowledge by defining specific policies and procedures. These policies and procedures should reflect the underlying assumptions and beliefs of management (Von Solms & Von Solms, 2004). Education will play a role in this regard and will, thus, be discussed in subsequent chapters.

The information security policy will serve as a centralised document which defines the organisation's critical information assets and methods which the policy aims to protect. ISO/IEC 27002, 2005, p. 7 states that the information security policy may form part of a general policy document. However, it must also include security education, training and awareness requirements. Von Solms and Von Solms (2004) recommend that the information security policy should be "short and sweet" and that it should address only security principles and technical and business details which change frequently. According to Johnson (2006), the information security policy document should not exceed five pages and should include the following components:

- Letter of commitment or support from management and/or the CEO as regards the information security of the organisation
- Scope and objectives describing the necessity for such security policies. The goals, scope and objectives should be outlined
- Clarification of information security aspects and definitions
- Security philosophy and definitions
- Responsibilities of each member of the organisation, particularly executive management, security professionals and line managers
- Compliance and measurement and the consequences of non-compliance.

3.5.3 Recruitment and Selection of Suitable Employees

Within an organisation, the human resources department is responsible for the identification and appointment of suitable candidates, either locally or countrywide (Kirsten, 2001, p. 24). Staff members are selected based on their skills and expertise regarding the task at hand. If candidates are incompetent or they lack the necessary skills to perform tasks correctly, they will pose a security risk for the organisation. It is

thus, essential that candidates possess the abilities and attitudes needed to assist the organisation in achieving its objectives. However, if the recruitment process is to be successful, a recruitment policy is needed. Such a policy should be drawn up by the management of the organisation. From the organisation's perspective, the policy will provide objectives and guidelines regarding managing and governing the recruitment process (Kirsten, 2001, p. 24). According to Kirsten (2001, p. 25), the recruitment policy should include information on the following:

- **Employing suitable candidates.** Qualified or experienced staff members to enable the organisation to achieve its objectives
- **Structure of the organisation.** Products or services, technology and production processes determine the type of candidates to be employed
- **Encouragement of team work.** Conflict may arise in an organisation, especially if there are diverse cultures, personality differences, communication barriers and varying leadership styles. It is important that new candidates be able to adapt and work together in the organisation as a team
- **Legal requirements.** Government legislations must be adhered to when appointing candidates and there should be no discrimination based on gender, race, religion, ethnic-background, sexual preference or health.

As part of this process, it is also important to **screen** employees prior to employment because, as Johnson (2006) points out, the greatest source of information security breaches is the employees within an organisation. Accordingly, the organisation should screen applicants in order to eliminate individuals with personal characteristics which do not match the minimum requirements as specified in the job description (Kirsten, 2001, p. 34). Background verification checks of candidates' academic qualifications, professional qualifications, character references, identity, criminal records and past working history should be carried out on all candidates, including contractors and third party users (ISO/IEC 27002, 2005, p. 23).

Screening should be carried out ethically according to existing laws and regulations and proportional to the business requirements, the classification of the information to be accessed and the perceived security risks (ISO/IEC 27002, 2005, p. 23). Candidates should be informed beforehand that screening activities will be

conducted. In addition, screening may also help the organisation to determine whether a particular candidate may require further training. This, in turn, may help determine whether specific candidates may be vulnerable to security threats and also to identify any other security risks which candidates may pose to the organisation. The latter may be done by adopting methods such as competency testing, aptitude testing, intelligence testing, interest testing, personality testing, psychological testing and trainability testing (Kirsten, 2001, p. 38). These tests may be important because, although candidates may possess the suitable qualifications for the job description, they may lack other skills or attributes which the organisation may deem necessary. For example, some employers may indicate that they prefer employees who are passionate, dedicated and motivated in their work. If the organisation has carried out the recruitment process correctly, then the organisation should be able to trust its employees.

3.5.4 Roles and Responsibilities of Employees

It is important that employees are clearly informed about the roles and responsibilities which an organisation prescribes for them. In other words, employees must understand what the organisation requires of them and how to carry out their tasks. On the other hand, the organisation must ensure that the employees' roles correspond with their abilities and skills. This should have been ascertained in the recruitment process. According to ISO/IEC 27002 (2005, p. 23), employees should be aware that it is their responsibility to protect organisational assets from unauthorised access, disclosure, modification, destruction or interference while a knowledge of policies and procedures will enable employees to have an understanding of what is considered as acceptable and non-acceptable behaviour with regard to carrying out their tasks in the workplace. Employees understand they are paid to perform their tasks. Unfortunately, some individuals may be tempted to abuse the organisation's time and/or resources by carrying out personal activities which are unrelated to their roles and responsibilities. As a result, personal activities during work time are considered unacceptable and may result in disciplinary action (see section 3.5.7). If employees have completed their tasks according to schedule, they should not seek alternative activities which are unrelated to work in order to keep themselves occupied for example, using social networking websites, and downloading music from websites. Employees should, thus, be made aware that

their work performance is monitored and evaluated on a regular basis. Furthermore, employees must be informed that disciplinary action can result from engaging in activities that is not supported by the organisation.

3.5.5 Induction Programme

Once employees have been appointed to their respective positions, they may need to go through a formal induction process. Activities in the induction process is driven by awareness and is designed to welcome employees into the organisation and involve them by providing them with basic information, including information on the values and the attitudes expected in the organisation (Kirsten, 2001, p. 51). It is recommended that an organisation introduce its policies and procedures as part of the induction process. It is also vital that information on the organisation's security policies and expectations be provided before access to information or services is granted (ISO/IEC 27002, 2005, p. 26). An induction process represents a form of education as it typically aims to achieve the following (Kirsten, 2001, p. 52):

- Enable the employee to settle comfortably in his/her new working environment
- Engender a positive attitude to the organisation and/or employer
- Help create realistic employee expectations
- Prevent accidents (e.g. ineffective use of machinery, wasting of materials)
- Ensure that the employee becomes productive as soon as possible
- Promote a culture of continuous training for the future.

Some employees have reported that they enjoy work when it gives them a sense of meaning and purpose (centreforconfidence.co.uk, online); for example striving for a goal larger than themselves gives them job satisfaction. Unfortunately, organisations today often discourage employees from this approach (centreforconfidence.co.uk, online). The induction process should also, if necessary, aim to change the attitude of its employees to believe that working may be enjoyable and that working should not be perceived as a robotic activity which is performed for the sake of earning an income. This, in turn, will require employees to be motivated and passionate about their work (see section 3.5.6). Some employees may not be satisfied with their roles in the workplace despite meeting the requirements for the position and this may

affect job attitudes. Wipawayangkool (2009) maintains that job attitudes influence the perceptions of users from their training and the way in which they react to training. Harrison et al. (2006) determined from their attitude engagement model that job satisfaction and organisational commitment constitute the underlying dimensions of job attitude.

3.5.6 Motivating Employees

In general, one often hears about employees who complain that they are not paid enough in their work, for example an employee whose work involves demanding physical labour, such as digging up trenches. This employee may have a negative attitude towards an employee who works in a comfortable office environment while the physical labourer may also be paid far less for his/her work than the person working in the office. The labourer may feel that, because they are performing much harder work which demands physical strength while they are also at risk from hazards, they should be paid more than the office employee.

On the other hand, the office employees may believe that they are justified in being paid more than the labourers because they are educated and because they may possess a formal university qualification and that they are, therefore, being paid to make important educated decisions. Both parties may argue their cases convincingly. In addition, the labourer may become demotivated because he believes he is not being fairly compensated by his employer in relation to his efforts. As a result, the labourer may purposely start being lazy in his/her work as well as developing lax habits and a negative attitude towards his employer (i.e. the organisation). This, in turn, may affect the organisation as far as security and productivity are concerned. It is, thus, clear that employee motivation may have a significant impact on the wellbeing of the organisation.

If the organisation does not assign clear roles and responsibilities to employees then incompetence and a lack of motivation may emerge. Motivating employees usually takes the form of some reward or compensation for the employee. The latter falls in the area of compensation management and refers to the system in terms of which individuals are rewarded with money for their work, performance level and diligence (Kirsten, 2001, p. 76). This compensation is perceived as a reward and is typically

used by organisations in order to shape individual and group behaviour (Kirsten, 2001, p. 76).

Compensation motivates employees to be more productive in the organisation while it also satisfies their needs and expectations. Kirsten (2001, p. 76) points out that employees will not be prepared to work unless they are assured that they will receive compensation for their efforts and that they are being treated fairly because they are being rewarded for their efforts. This, in turn, affects employee attitudes and behaviour and, ultimately, motivates employees to work towards the goals of the organisation. It is important that the organisation compensate its employees regularly on the date specified in the job contract. If employees are not satisfied with their compensation, they may resort to either strikes or protests. It is, thus, essential that compensation details be covered in detail in the employment contract.

Incentives are also used by organisations to motivate their employees to produce results. Incentives refer to rewards and usually take the form of time off, social get-togethers, salary increases, stationary and equipment, etc. Incentives are also used to motivate individuals in other domains. For example, the South African athletes competing in the 2012 London Olympic Games stood to receive R400 000 for every gold medal they won (Lewis, 2012) while a university may have in place incentives for academics to the effect that, if they publish research articles in accredited journals, they are granted money for each publication and may be promoted. In both these examples, the individuals concerned would be motivated to work harder in order to realise their goals and, in turn, the organisation concerned would benefit. Raghu, Jayaraman, and Rao (2004) suggest that employee behaviour is affected by explicit incentives that both the employees and organisations understand. Team building exercises may also help motivate employees through building confidence and trust in their colleagues. This, in turn, may help strengthen existing work relationships and also create new relationships. These exercises may be held in a location distant from the organisation itself, such as a holiday resort or a lodge. It is important that these exercises are fun and, more importantly, that management be more flexible and forthcoming than usual to their employees during these events. As a result, any negative attitudes towards the organisation and management and amongst the employees themselves may diminish.

Although this paragraph highlighted the fact that organisations should motivate their employees primarily by means of remuneration, there are other factors which have an influence in this regard. Kirsten (2001, p. 77) points out these factors may include legislation, the organisation's remuneration policy, the worthiness of the employee, the cost of living and, most importantly, the financial position of the organisation. If organisations decide on a salary increase, they need certain criteria in order to determine the worthiness of the candidate. This may be achieved by some form of performance monitoring. If organisations are in a position where they are not able to afford salary increases, it is important that they communicate this to their employees on a regular basis. If employees are not aware of the prevailing situation, they may make their own assumptions about not receiving any salary increases and, as a result, they may develop negative attitudes towards the organisation.

Within an information security context, it is important that employees be motivated to safeguard the organisation's systems and information. This viewpoint is supported by Siponen (2000) who points out that, even if employees are educated about information security, they may not adhere to its procedures as a result of a lack of motivation. If employees are demotivated, apart from not carrying out their work tasks efficiently, they may develop a 'don't care' attitude and, as a result, place the organisation's information assets at risk. If employees are acknowledged and rewarded for their hard work and compliance, this may make a significant difference within the organisation itself and the working environment. Rewarding employees for desirable behaviour and punishing them for undesirable behaviour are both considered to be vital factors in influencing employee compliance with information security (Gonzalez & Sawicka, 2002). Mitnick and Simon (2002, p. 245) further add that organisations should institute a reward programme for those employees who demonstrate good security practices or for those who report security incidents. The process for punishing undesirable behaviour is described in section 3.5.7. Compensation and incentives are strong motivators for productiveness and adherence to security policies and may also change employee attitudes towards both their work and their employer.

3.5.7 Disciplinary Process

Every organisation usually has a formal disciplinary process in place. For example, if an employee arrives at work under the influence of alcohol, a legal process should be followed to ensure that the correct action is taken and that the individual is fairly treated. Mitnick and Simon (2002, p. 245) believe that employees should be advised of the consequences for failing to comply with security policies and procedures and, thus, a set of appropriate consequences for violating the policies should be formulated and communicated to employees. Organisations typically have in place a disciplinary process to handle such misdemeanours. The disciplinary process should be described in the organisation's policy documents. With regard to information security, employees who have committed a security breach and/or who are suspected of committing a breach of security should also be subject to such a disciplinary process (ISO/IEC 27002, 2005, p. 26). It is essential that employees understand that, if such policies are either ignored or violated, there will be consequences. A formal disciplinary process should take into consideration a number of factors, including, among other things, the nature and gravity of the security breach and its impact on the business, whether or not this is a first or a repeat offence, whether or not the transgressor has been properly trained, relevant legislation and business contracts (ISO/IEC 27002, 2005, p. 26). Depending on the nature of the misconduct, the disciplinary process may call for instant removal from duties, loss of access rights and privileges and, if necessary, immediate eviction from the premises (ISO/IEC 27002, 2005, p. 26).

From the perspective of the organisation, an indirect benefit of the disciplinary process is the fact that knowledge of the consequences may serve as a deterrent to prevent employees, contractors and third party users from violating organisational security policies and procedures and from committing any other security breaches. This, in turn, may help shape the behaviour of employees who will wish to ensure that they are not affected by any such consequences.

3.5.8 Termination or Change of Employment

Termination of employment may be the result of employee misconduct (see section 3.5.7). The human resources function is usually responsible for this process although the process may also require the involvement of either a supervisor or a manager of

the employee concerned (ISO/IEC 27002, 2005, p. 26) as well as the involvement of other departments within the organisation, for example, ICT staff withdrawing network access rights (passwords) from an employee. The latter is important because, if not done, the employee concerned may continue receiving information in his/her emails and he/she may then use this information that belongs to the organisation.

It is essential that the termination process be formalised to include the return of all previously issued software, corporate documents and equipment. Other organisational assets, including mobile computing devices, credit cards, access cards, access rights, manuals, and information stored on electronic media would also have to be returned. The access rights that should be either removed or adapted include physical and logical access, keys, identification cards and information processing facilities. Depending on the level of risk, access rights to information assets and facilities should be either reduced or relinquished before employment is terminated (ISO/IEC 27002, 2005, p. 28). It is important that the organisation conduct the termination process correctly and thoroughly. As pointed out in the Omega example in section 2.3.2, disgruntled employees, contractors or third party users may deliberately either damage and corrupt information or sabotage information processing facilities.

It is evident from this section that policies and procedures exert a significant influence on the way in which people are managed in an organisation. This section not only emphasised the importance of an information security policy but it also described other policies which may influence the management of employee behaviour. It is evident that employees may, knowingly or unknowingly, transgress policies and, thus, it is essential that they be made aware of the consequences of such transgressions. This section also further recommended that employees be rewarded for displaying acceptable behaviour as this may motivate employees and help sustain such behaviour.

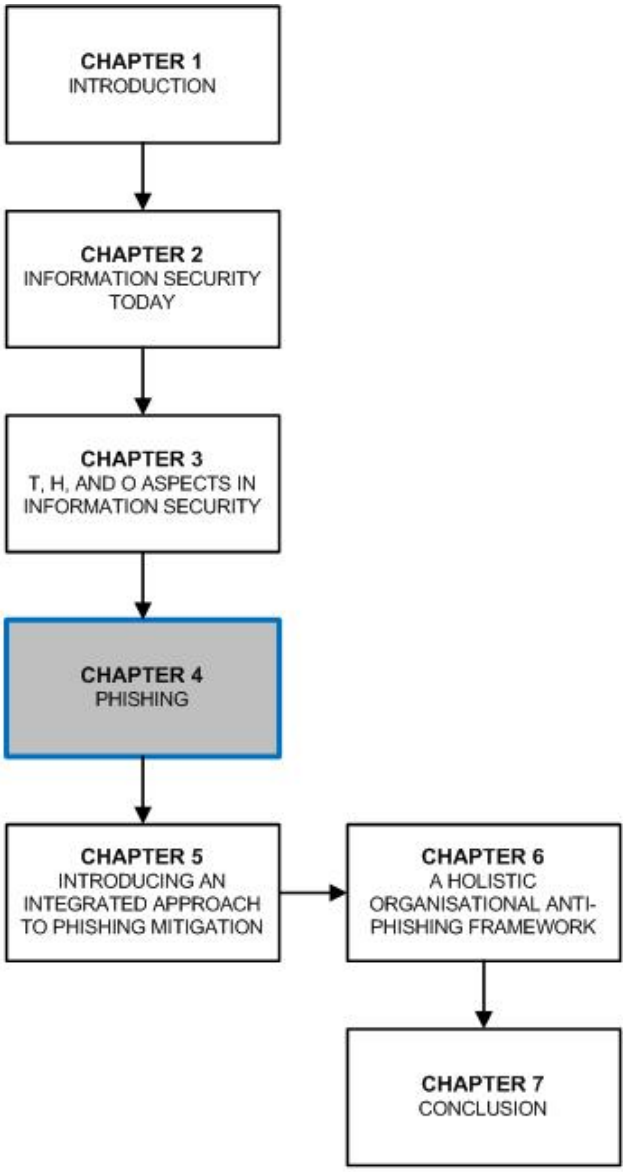
3.6 Conclusion

This chapter classified information security controls into three main dimensions, namely, technological controls, human factors and organisational aspects. Despite

the fact that organisations make use of all these controls to combat threats, technological controls are used the most. This is, however, a matter for concern in view of the fact that human beings constitute the greatest security risk because of their lack of knowledge and undesirable behaviour. Humans make use of technology and, thus, if they are unable to use it correctly then the technology may be considered inadequate. The organisational aspect dimension takes into account components related to managing the employees of an organisation. In general, policies and procedures are used to do this. However, in this instance human behaviour also poses a risk as these policies are often ignored by employees and, thus, it is essential that organisations ensure that they also put in place other measures including recruitment, induction programmes.

Motivation plays a key role in ensuring that employees have the correct attitude and behaviour as regards their work. It is evident that human factors are present in each of these dimensions and, thus, it is clear that each of these dimensions is linked by human involvement. Social engineering attacks pose a significant security threat as they exploit the human factors to the full. This, in turn, heightens the concern that, if human factors are not managed, a social engineer may target any of these dimensions as they are each characterised by gaps which are caused by human factors. Phishing involves the use of the social engineering techniques described earlier and is the research problem which needs to be addressed in this study. The next chapter will discuss phishing in great detail. Predictably, human factors will again emerge as an area of weakness which phishers will exploit.

CHAPTER 4
PHISHING



CHAPTER 4:

4.1 Introduction

In the previous chapter, information security controls were categorised into three main areas, namely, technological, human and organisational aspects. These aspects were all discussed in detail. Phishing is a component of social engineering. Therefore it was critical to understand the components of social engineering as it provided insight into the reasons why people fall victim to social engineering techniques. This will help to understand how to address the problem of phishing. The chapter begins by describing the most important aspects of both phishing and its related techniques. The risk which phishing poses to an organisation and its customers are also examined. The chapter concludes by classifying the anti-phishing measures found in literature into three areas, namely, human factors, organisational aspects and technological controls.

4.2 Phishing Explored

Chapter 3 described social engineering and its variations. It emerged from this discussion that humans tend to trust entities and suchlike easily, based on their appearance. Furthermore, humans are inclined to be helpful towards others, even towards strangers. Phishers takes advantage of these human factors by making effective use of social engineering techniques in order to gain the trust of their victims as quickly as possible. This section begins by providing a brief history of phishing and its techniques. This is followed by examples of actual phishing emails.

'Phishing' is a term that was introduced in the United States (US) when hackers began, metaphorically, to 'fish' illegally for confidential information from people. They did this by creating fake emails and websites which functioned as the 'bait' while the victims' information was the 'fish' (phish) caught in the phishers' net (Sophos, 2005). The 'ph' spelling of phishing originated in the 1970s when the first hackers began breaking into the US telephone system in order to make free telephone calls, an activity which they termed 'phone phreaking'. In this instance, the most notorious 'phreaker' was John Draper, famously known as Captain Crunch (DeFino et al., 2010). John Draper used a toy whistle which was packaged in the Cap'n Crunch cereal box to emit a tone of precisely 2600 hertz. This frequency allowed him to make free telephone calls, using the AT&T long lines, from any telephone point in

the US. The term ‘phishing’ became internationally recognised in 1996, after America Online (AOL™) and its corresponding customer accounts had been affected by phishing attacks (Ollman, 2008). Phishing activities began to be more noticeable on the Internet in late 2003 (Microsoft, 2008 with those people who tricked individuals into providing their information through using computers becoming known as ‘phishers’.

There are at least two parties involved in every phishing attack, namely, the *phisher* who sends an email or an instant message and the *victim* who receives the email or message. The most effective phishing attacks have been initiated through email (Ollmann, 2008). Typically, the phisher sends a phishing email to the victim containing a fabricated story, warning the victim of a potential threat or danger that is imminent. For example, the victim may be warned that his/her account may be compromised as the organisation concerned has been experiencing either fraudulent activity or a security breach. The victim is required to click on a hyperlink embedded within the email which directs the user to a spoofed website in order to verify their personal particulars. In addition, it may be stated in the email that, should the victim decide to ignore the request, this may result in either their account or their membership being suspended or terminated. Users often fall for this technique and obey the request. They then unsuspectingly log-in to the website with their personal account information (e.g. username, password, credit card number). The victim’s personal information is then captured by the phisher to be retrieved for illegal purposes.

These activities are possible because the phisher makes use of social engineering techniques and, thus, phishing may be considered as a subcomponent of social engineering. A phisher attempts to steal confidential information from users or employees by disguising him/herself as a legitimate entity (Kumaraguru et al., 2007). These entities which are imitated are usually well-known financial or e-commerce organisations. A few high profile and popular cases of organisations that have fallen victim to phishing attacks include PayPal™, eBay™, American Online™, ABSA™ (Mittner, 2007; Sophos, 2005), Standard Bank™ (Expertron, 2009, Pickworth, 2009), Google™, Microsoft and the South African Revenue Services (Fin24.com, 2009, SARS, 2009). Made possible through the Internet, there are no geographical

boundaries to phishing attacks and, as such, phishing is a problem which is affecting most of the world. In view of the fact that it is a form of identity theft phishing is considered as fraud with the phisher intentionally posing as a trustworthy source which he/she is not. Phishing may also be considered to be a subset of spam as, firstly, the recipient does not know the sender and, secondly, the recipient did not request such emails to be delivered to his/her email account. The main objective of phishing is to obtain the victim's personal information fraudulently in order to extort money (Vegter, 2005). Although most of the cases affected by phishing are financially related, phishing may also include unauthorised access to all types of other personal and financial data.

Generally speaking, phishing websites (spoofed websites) are discovered and shut down relatively quickly (Sophos, 2005). However, within the limited time period available, phishers try desperately to gain the trust of recipients as quickly as possible. The longer a phishing attack remains active, the more money the victims and targeted institutions lose and the more money the phisher is able to make (Aaron, 2010). The strength of phishing lies in its ability to exploit the human tendency to trust email messages and websites based on their appearance despite the fact that there is nothing trustworthy in the actual appearance of the spoofed websites (Downs, Holbrook, & Cranor. 2006). Instead of phishers taking advantage of system vulnerabilities, phishers focus on taking advantage of the way in which humans interact with computers or their interpretation of messages (Schneier, 2000). In other words, phishing exposes the human factor the most.

Phishers are aware that users may have technological controls in place, such as spam filters, anti-virus programs and so on, to detect phishing emails. As a result, phishers also use technological methods (e.g. HTML based emails, hidden characters, encoded URLs, and so forth) to avoid detection by the victim and his/her technological defences. According to Ohaya (2006), in some cases, phishers may also take advantage of software vulnerabilities, especially vulnerabilities in popular web browsers. For example, by exploiting the weakness in the web browser, an entry point may be created to install malicious software (e.g. key logger virus). This, in turn, will allow the phisher to capture or log all the keys secretly which a user enters when he/she log-ins to a particular website. As a result, phishers are able to use these details to log into websites of the victim on other occasions. Such an

instance would be considered as identity theft. Phishers may even download specialised programs that are able to change a user's browser proxy settings, thus redirecting all Internet requests and responses to pass through spoofed websites owned by the phishers. Phishers also acquire the email addresses of potential victims from a variety of sources including websites, social networking websites, trade journals, professional directories and newspapers (Ohaya, 2006). It emerged from this section that, in the main, phishers target the human element. The aim of these phishing techniques is usually to gain the trust of victims so that the victims provide sensitive information willingly. It is evident that phishers take advantage of any potential weaknesses in a system. As pointed out in the previous chapter, technology is characterised by weaknesses in the form of software vulnerabilities i.e. bugs, as they are developed by humans. In addition, humans may use technology incorrectly either intentionally or unintentionally. Thus, phishers exploit these weaknesses from both the technological and the human perspective.

4.2.1 Phishing Variations

The previous section described typical email phishing scams. However; there are other techniques which phishers use and, besides their predominant use of email and spoofed websites, in modern times phishing techniques have become increasingly sophisticated (Kirda & Kruegel, 2006; Sophos, 2005). Phishers are also making use of a range of modern and popular technologies such as Internet Relay Chat (IRC), Social Networking websites (e.g. Facebook, MySpace, Twitter and Friendster) and instant messengers (IMs) in order to lure their victims (Butler, 2007; Ollmann, 2008). Phishing may also be conducted through viruses, key-loggers or a Trojan horse (Sophos, 2005) which may be sent through attachments in emails or downloaded from websites (Drake et al., 2004). Besides these technological approaches, phishers may also contact their victims directly by using a telephone to seek personal information. Some phishers may pose as interested employers and contact and email people who have listed themselves on job search websites. These examples are described in the following paragraphs. However, all of these variations are extremely similar as they all make use of social engineering principles.

4.2.1.1 Spear Phishing

Spear phishing represents a more targeted form of phishing and is not regarded as a 'general' phishing scam. As the term 'spear' suggests, its differentiation focuses on a single user or on a department within an organisation. It will appear as if the phisher is legitimately positioned within the victim's organisation, usually in a position of trust. The phisher may request employees to update their username and passwords. For example, should the phisher have knowledge that the victim is a client at a particular financial institution, for example, First National Bank™, the phisher would probably use the institution's image as a lure (the bait) and include the victim's name in the email message in order to enhance the fictional legitimacy of the email. The strength of spear phishing attacks lies in the timing and context in mimicking an authentic situation (Jakobsson, Tsow, Shah, Blevis, & Lim, 2007).

4.2.1.2 Whaling

According to Fulks (2010), whaling is difficult to detect as the efforts of phishers in this regard are more focused in comparison to typical phishing. Similar to spear phishing, whaling involves the threat targeting specific individuals and creating messages that appeal to that specific target. In many cases, the person being 'whaled' is usually a high profile executive or powerful figure who potentially stands to lose more financially. Evidently, the term 'whaling' describes going after a 'bigger fish' which, fittingly, would be a company executive. Similar to spear phishing, when a victim is being 'whaled', the first contact from the threat may not be the usual generic 'Dear user' or 'Dear sir/madam' message but, instead, the message may include the victim's name, financial institution, job title. The use of the Internet enables threats agents to gather considerable information about high ranking corporate executives with ease and then to use this information to tailor their messages specifically to those people in order to gain their trust.

4.2.1.3 Wi-phishing

This technique is similar to the spear phishing technique but with the difference that the phishers target the users of wireless network devices such as cell phones and PDAs. Wi-phishing tricks users into submitting their personal information via wireless Internet connection. Internet hot spots at hotels, restaurants, airports, cyber cafés

and libraries often offer customers wireless Internet access that is convenient to users, but also provides an excellent opportunity for threat agents to use wi-phishing. The CEO of Ciron, Nicholas Miller, is credited with coining the term “wi-phishing” and metaphorically describes it as “somebody walking through Grand Central Station with papers blowing out of the back of their briefcase all over the place, for anybody to read. With over 100 million wireless laptops in use today and growing, wi-phishing is projected to get worse” (Pipline, 2005).

4.2.1.4 IVR/Phone Phishing or Vishing

This technique uses a rogue Interactive Voice Response (IVR) system to recreate the legitimate sound of an institution’s IVR system. The victim is prompted, usually by means of a phishing email, to contact the institution in order to verify his/her personal information. Typically, the system will purposefully continually reject log-ins, thus ensuring that the victim enter their personal credentials multiple times. More advanced systems may transfer the victim to the attacker, who poses as a customer service agent, for the purposes of further questioning. Vishing sometimes uses fake caller-ID data to create the impression that the calls originate from a trusted organisation.

4.2.1.5 Mishing

This technique is very similar to phishing although it targets cell phone users. In today’s world it is common for end-users to perform transactions on their mobile cell phones, including purchasing goods or services, and mobile banking. Almost all smart phones are packaged with a mobile web browser and, as a result, these users are potentially exposed to mishing scams. For example, a typical mishing call or text message will involve a scammer, posing as an employee from the victim’s bank and claiming to need the victim’s personal details. Scammers are extremely creative and they are able to fabricate numerous stories in order to gather personal information. Mishing may also be delivered in a SMS which lures the user either to click on the hyperlink or to reply to the message and provide personal information.

4.2.1.6 Baiting

This technique relies on the curiosity or greed of the victim. For example, the threat may place a malware/virus infected floppy diskette, CD, DVD or a USB flash drive in

a location where it is intended to be found by the victim. The threat agent entices the victim by ensuring that the object has a legitimate looking label (e.g. a company logo, budget report, executive salaries) and then waits for the user to use the device. If the user does not hand it in, curiosity may result in the victim inserting the device into his/her computer with the result that malicious software (malware) is automatically installed on the victim's computer. This, in turn, enables the threat agent to gain system access to the user's infected computer or, at worst, an entire organisations internal network. Baiting may also occur via email (see section 4.2.3) which lures the victim to open an attachment. If a recipient takes this bait and his/her computer becomes infected, the criminals may access the computer device remotely, steal the personal information stored on it and intercept passwords and online transactions (Aaron, 2010). The criminals may even log into a victim's computer device to perform online banking transactions while posing as the victim by using the victim's account details. As a result, it is extremely difficult for the banks to detect this fraudulent activity while the victim would also struggle to prove the absence of negligence.

4.2.1.7 Pharming

According to Shelly and Vermaat (2011, p. 405), pharming also involves the perpetrator attempting to obtain personal and financial information. However, pharming is performed using spoofed websites. Typically, a user types a web address (URL) but is redirected to a hoax web site that appears to be legitimate. The hoax website prompts the victim to enter confidential information which is then captured by the phisher.

It emerged from this subsection that, in the main, phishers make use of technology to carry out their attacks with effective use being made of the technology in order to gain the victim's trust. This enables phishers to exploit human weakness, specifically their behaviour and trust. In this study, the focus of phishing will be on those attacks which are carried out through the use of email. The next subsection provides a systematic description of the way in which email phishing attacks are carried out.

4.2.2 Characteristics of a Phishing Attack

Section 4.2.1 described a number of variations regarding the ways in which phishing may be carried out. From the description of phishing above, it is clear that phishing

typically makes use of a variety of social engineering techniques to lure unsuspectingly victims into providing their personal information. Section 3.4.4 discussed psychological triggers affected by social engineering techniques. These triggers will be evident in the subsequent sections. Understanding the way in which these techniques are used will help users to distinguish phishing emails from legitimate emails. Based on the literature studied, Frauenstein and Von Solms (2011) classify five factors that must be present if such an attack is to be carried out successfully:

1. **Planning:** During this stage, the phisher determines the method (e.g. spear phishing, whaling) to be used, the intended victim as well as the type of information to be gained from the victim. Some researchers term this process the reconnaissance stage. DeFino et al. (2010, p. 35) maintain that Google search engine may be used as a tool by threat agents to profile and map their targets. According to Orgill et al. (2004), there are two aspects to social engineering attacks that are designed to obtain the desired information from the victim – the physical aspect and the psychological aspect or a combination of both. The physical aspect is usually decided upon as the environment in which the victim feels the most secure, relaxed and comfortable. This is often the workplace, over the telephone, instant messengers, email, text message and online. Such physical factors provide the victim with a false sense of security and complacency which assists the social engineer to achieve his/her objective. Thus, during this phase, the 'phisher' will decide which medium (bait) is best suited to entice the victim into releasing information.
2. **Authentic looking email:** The phisher usually establishes the first contact with the victim through email with this process being termed the attack phase. Thus, in this stage, the appearance and content of the email are critical to the phisher with a reputable or well-known organisation often being imitated in the email (Van der Merwe et al., 2005a). This is intended to gain the victim's trust. The illusion, based on the appearance of the email (e.g. email address structure, subject header and content), is made to appear more legitimate by using institutional logos, terminology, etc. This is often done by the phisher using URL obfuscation techniques (Ollmann, 2008). Phishers utilise well known flaws in the common mail server communication protocol (SMTP) and

are, therefore, able to create emails with fake “Mail From:” headers and impersonating any organisation they choose (Ollmann, 2008). The email subject header/line also attracts the victim’s attention for example, Tax Refund Notification, Important Claim, Warning etc. This technique is used to enhance the authenticity and urgency of the email in the mind of the victim.

3. **Fabricated story:** Typically, a fabricated story is used to gain the victim’s attention with the email usually warning the victim of a supposed problem or threat which exists for example, customer accounts have been hijacked, a security breach or to update details. Thus, lured by the fake story, the user is required to click on a hyperlink which is sometimes disguised as either text or an image for example, Click here for verification. Alternatively, the phisher may choose to provide a file attachment which the user must download to his/her device. This file may either contain a virus or it may contain information which instructs the user to perform further actions. The tone of the email is perceived as either friendly or helpful tone, for example thanking you for your cooperation. In this instance, the phisher makes effective use of reverse psychology against the victim as, before the victim has reached a decision as whether or not to respond to the request, the victim may already feel indebted to the phisher. The strength lies in the psychological aspect, which preys on human emotions and specifically on the human tendency to be helpful to others even if they are strangers.
4. **Threatening tone and/or consequence:** In order to ensure that the victim responds to the phisher’s demand, the phisher will try to add a threatening element. For example, the victims are warned that, should they not verify their particulars, this may lead to the suspension or even termination of their accounts. Again, reverse psychology is used as victims are afraid to ignore the request. Ironically, it is typical of ‘human nature’ not to want any further undesired consequences or complications for example, renewing accounts, and registration and so on.
5. **Spoofed website:** This stage involves the final activity which involves the use and understanding of technology on the part of the victim. The first such activity was the email. Once the user has clicked on the hyperlink provided in the email message he/she is redirected to a spoofed-website. The spoofed

website appears authentic and legitimate as it usually contains institutional logos. There is almost no difference, in appearance, between the legitimate (original) website and the spoofed website. As a result, the victim tends to trust the website and will enter his/her credentials which are then, unbeknown to the victim, captured by the phisher. The phisher uses this information to steal money, fraudulently purchase goods on the victim's account and/or commit identity theft. Ohaya (2006) maintains that if the website appears authentic, then users will have confidence in the website as they will not be able to distinguish between a genuine or a spoofed website. In some cases, the users' ignorance plays into the phishers' hands. Patrick, Briggs, and Marsh. (2005) maintain that "the importance of visual appeal in the early stages of interaction with a website is not unexpected given that, in face-face interaction, people make judgements on the basis of the attractiveness of an individual".

Van der Merwe et al. (2005a, 2005b) describe the characteristics of a phishing email as follows:

- "There is always some kind of company that is imitated, often from the financial sector
- The email often includes a security breach, warning customers to log-in and verify or renew their details
- There is always a link that the user needs to follow in order to complete the process
- The graphics used are often identical to the original website."

As stated earlier, according to some researchers, the effectiveness of using social engineering techniques does not depend entirely on the phisher's possessing much prior technical knowledge or education regarding hacking information systems and, instead, a mixture of manipulation, human emotion and technical deceit is used to trick victims into willingly giving up their personal information (Ollmann, 2008). An anonymous phisher once posted online that there must be no limit to phisher's

creativity. In view of the fact that there is no face-to-face human interaction in a phishing attack, the appearance of the phishing email and spoofed website is used to replace this face-to-face interaction.

The next subsection will provide examples of real-world phishing emails. This should indicate the strength of phishing which stems from the appearance of the email combined with social engineering techniques.

4.2.3 The Anatomy of Phishing Emails and Email Scams

Section 4.2.2 described the characteristics of a phishing email and how such an attack is typically carried out. This subsection will illustrate the way in which social engineering techniques appear in phishing emails. Actual examples of phishing emails which were directed to the researcher's personal email account will be presented and examined. In addition, the psychological triggers, discussed in section 3.4.4, will be highlighted in each example. There are evidently similarities between email scams and phishing emails and, thus, this section will distinguish between these similarities by presenting the information in two parts, namely, phishing emails and email scams.

Phishing Emails

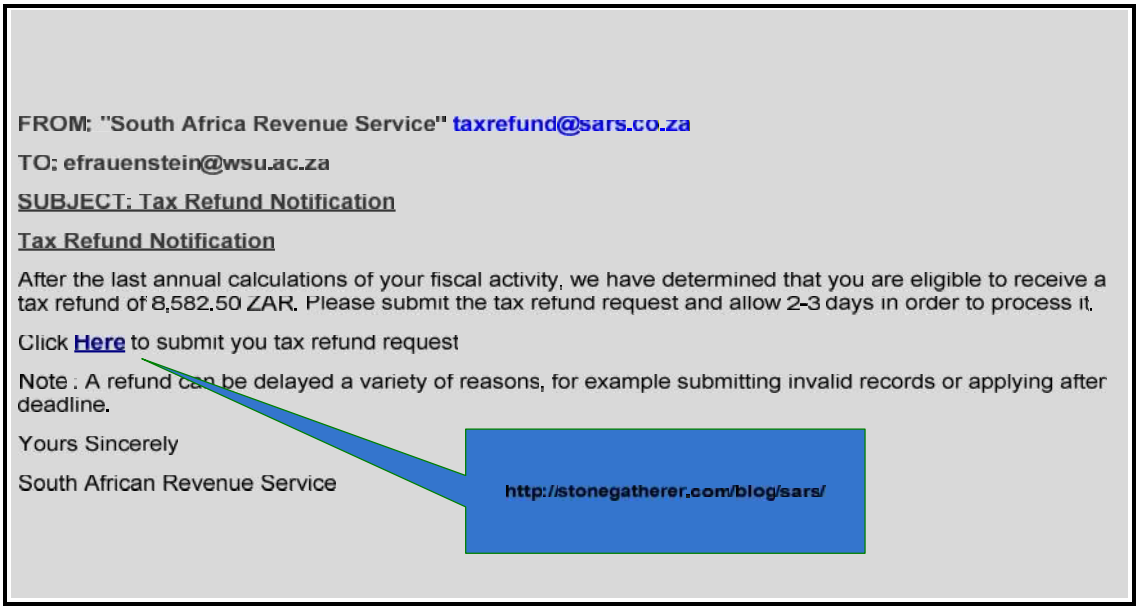


Figure 4.1: Phishing email using a refund to gain the victim's attention

The receipt of any email which states that one is about to receive a tax refund is sufficient to attract anyone's attention. In this example, the context of this email would appear as even more trustworthy for South African citizens. However, as one may see from the description of the link, the email is not directing the user to a legitimate financial authority, in this instance SARS. The psychological triggers of strong affect ('*tax refund of R8.582'*) and overloading ('*2–3 days to process'*) are used in this example.

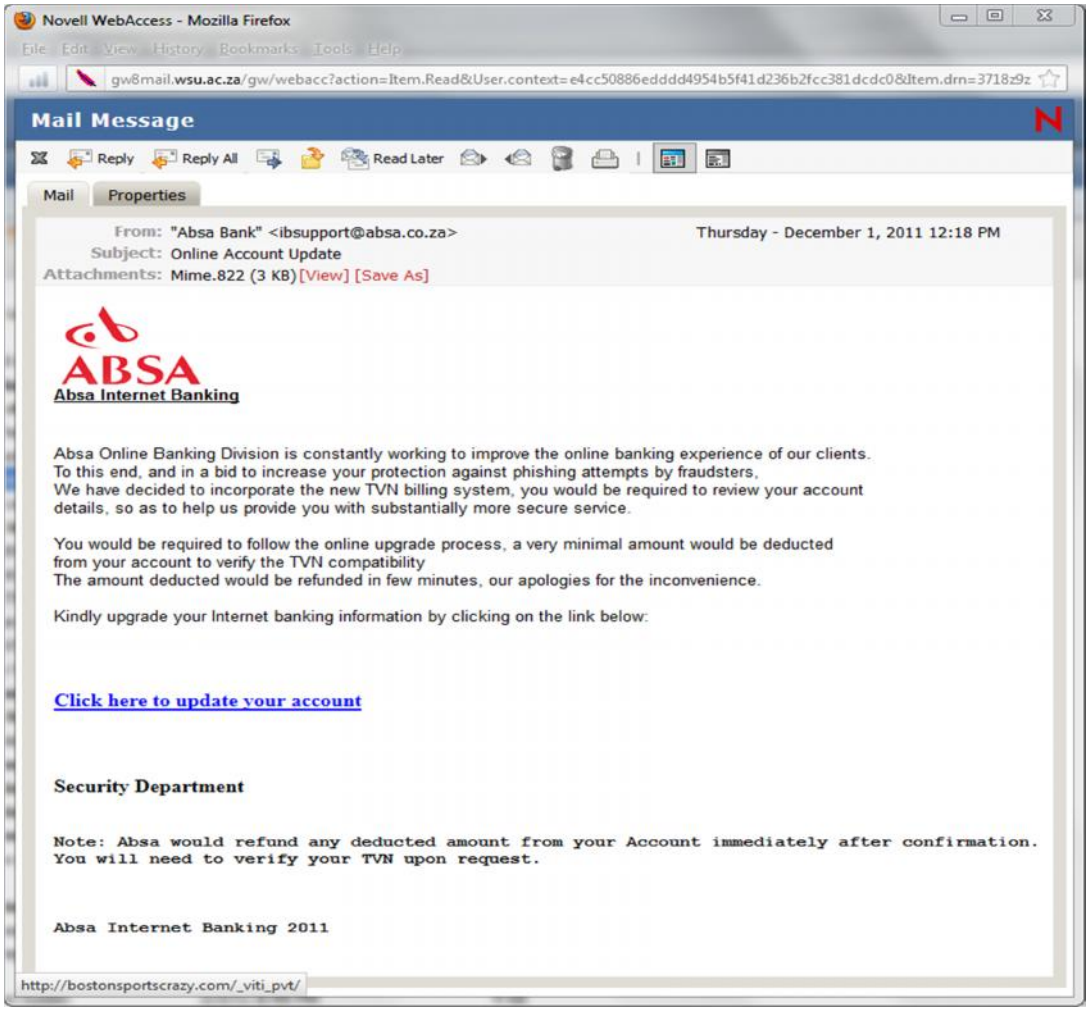


Figure 4.2: Phishing email ironically using a phishing warning

In Figure 4.2, the legitimate institutional logos of Absa Bank are used to make the email appear more trustworthy. In this example, a reciprocation psychological trigger is used, as the threat has already warned the victim of phishing risks. As a result, the victim will be less suspicious and, as such, be led into believing that the threat's intention is to be helpful by offering this fabricated security service.

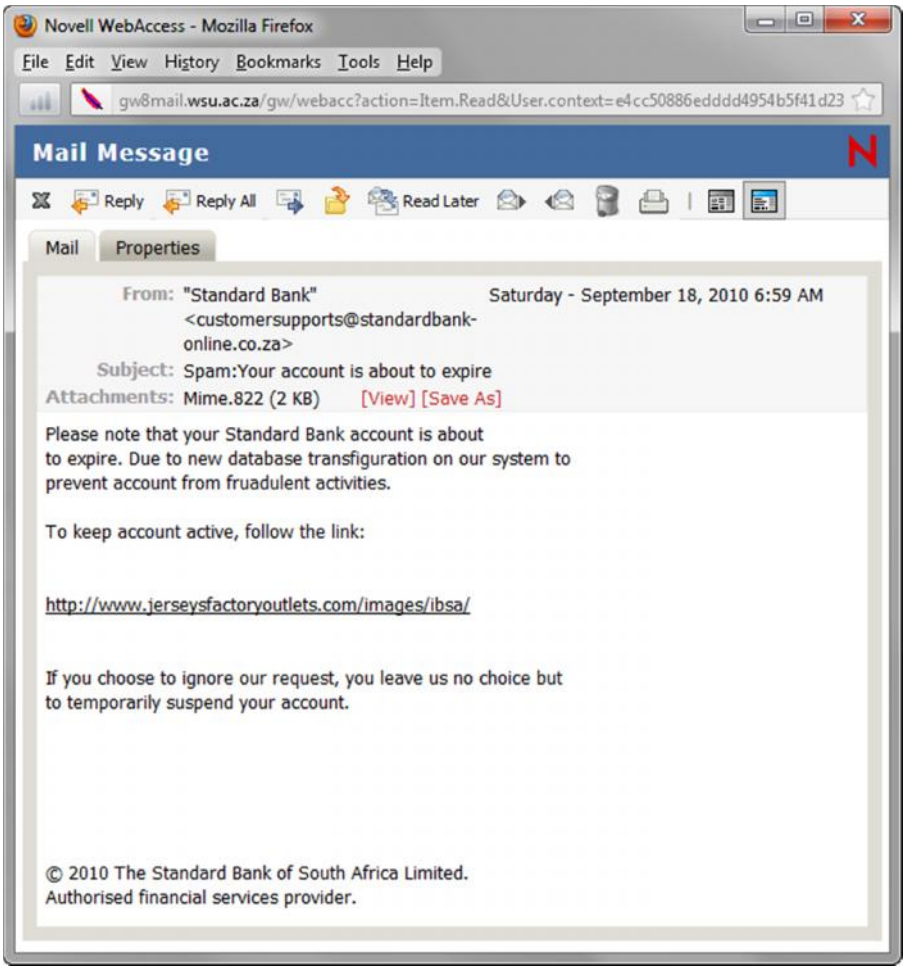


Figure 4.3: Phishing email using an expiration warning to create urgency

In Figure 4.3, a psychological trigger of 'strong affect' is used. As the victim does not want their bank account to be suspended, they will probably obey the request. In this example, there is a spelling mistake, that is, in the word 'fruadulent'. Moreover, the

hyperlink contained in the email is obviously suspect. Users need to identify these errors as this can help them to recognise such emails for what they are.

Users should be aware that phishers may send emails requesting the user to download or update their software, and for which purpose they provide a hyperlink. Figure 4.4 below, which requests users to update their Adobe product software, demonstrates this particular scam. As Adobe is a popular and reputable software enterprise, there is a great probability that users will recognise the name. Accordingly, this might result in users believing in the authenticity of the email. In this example, the psychological trigger of authority is used.

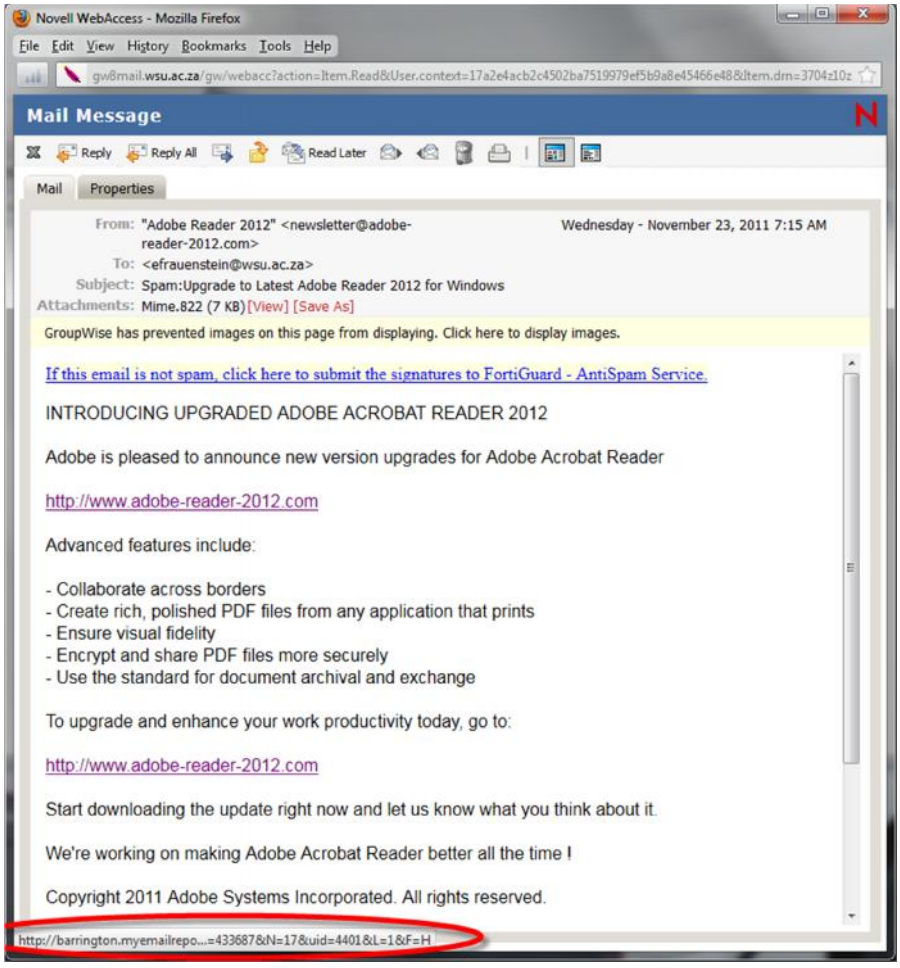


Figure 4.4: Email scam informing the user of a new version of software

The benefits mentioned in terms of the software upgrade also to gain the victim's attention. In Figure 4.4, it is evident in the status bar (bottom left-hand corner) that the hyperlink does not redirect to Adobe's official website but rather to a spoofed website (http://barrington.myemailrepo...).

There are many phishing examples that could be mentioned. From the real-world phishing email examples discussed, one can understand why people fall victim to these techniques. The fabricated story (evident in all the examples) may seem valid especially when a spear-phishing technique is used. In some cases, the institution's logo is used (particularly in Fig. 4.2) to increase its authenticity in the victim's mind. Furthermore, other features of the email address structure (domain name) create the illusion that it originated from a legitimate institution (e.g. ibsupport@absa.co.za., customersupports@standardbank.co.za).

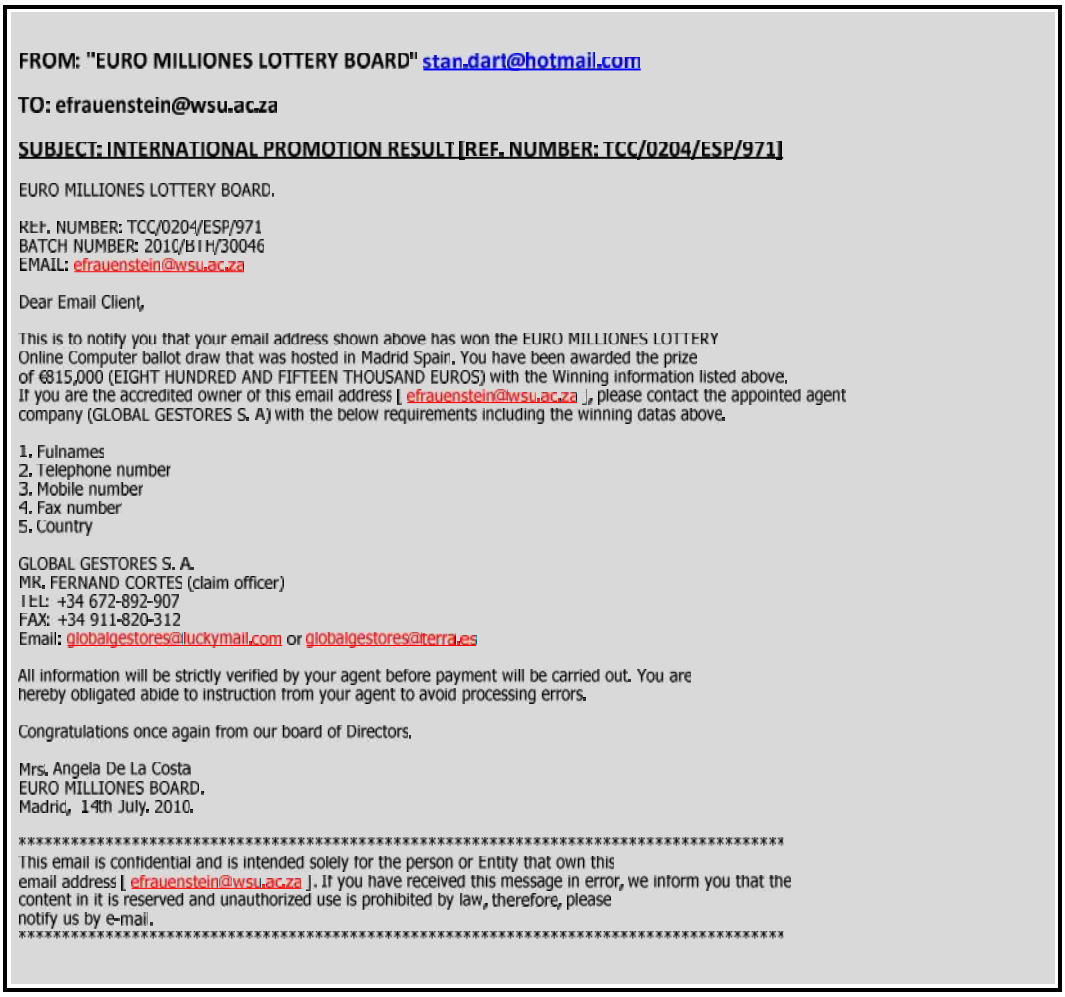
Some phishers have sophisticated technical knowledge (i.e. programming background) and are able to make more use of more sophisticated methods to deceive their victims. For example, if phishing emails are sent in Hypertext Markup Language (HTML) format, they can be disguised to appear as plain-text, which makes it much harder for victims to identify the hidden 'qualities' of the emails dynamic content (Ollmann, 2008). Phishers sometimes purposely change the characters in the email body to avoid detection by many standard anti-spam filters, and, thus, fool the recipient into misreading them. For example, the popular American Online (AOL) website can be spelt by the phisher as: www.aoI.com. In this example the character 'L' was replaced with a capital 'I', which could easily be overlooked. In some phishing cases, there may also be random words hidden in HTML emails. This can be done by using a white font colour on the white background of the email, which would not be visible to phishing victims. The purpose of this activity is to avoid detection by standard anti-spam filters (Ollmann, 2008).

In most of the examples, the URL link is made to appear from a legitimate website but in fact points to an escape-encoded version of the URL. In Figure 4.1, this was highlighted with a blue speech bubble. Accordingly, users should be educated so as to be able to determine whether the website provided in the email corresponds with the website being imitated. In all of the examples, the victims were not addressed by

their name and, typically, a generic “Dear Customer” is used. Some legitimate organisations include hyperlinks in the emails they send out to their clients to, for example, allow their clients to download financial statements. There are also cases where users are requested to click on a hyperlink to complete a registration process on another website. This is to verify that the email address provided by the user is legitimate. One cannot therefore state that all emails containing hyperlinks are phishing attempts.

Email Scams

As previously stated, phishing is merely a component or subset of spam. After obtaining personal information from victims, phishers developed follow-up scams to transfer stolen monies safely from their accounts out of the country (Orgill et al., 2004). An increasingly popular method for doing this is by means of fake job scams. Other spam emails include advertisements or scams offering products, rewards or prizes that seem too good to be true. As with phishing emails, trickery and deception are also used. One difference between phishing emails and scams can be seen below:



FROM: "EURO MILLIONES LOTTERY BOARD" stan.dart@hotmail.com

TO: efrauenstein@wsu.ac.za

SUBJECT: INTERNATIONAL PROMOTION RESULT [REF. NUMBER: TCC/0204/ESP/971]

EURO MILLIONES LOTTERY BOARD.

REF. NUMBER: TCC/0204/ESP/971
BATCH NUMBER: 2010/BTH/30046
EMAIL: efrauenstein@wsu.ac.za

Dear Email Client,

This is to notify you that your email address shown above has won the EURO MILLIONES LOTTERY Online Computer ballot draw that was hosted in Madrid Spain. You have been awarded the prize of €815,000 (EIGHT HUNDRED AND FIFTEEN THOUSAND EUROS) with the Winning information listed above. If you are the accredited owner of this email address [efrauenstein@wsu.ac.za], please contact the appointed agent company (GLOBAL GESTORES S. A) with the below requirements including the winning datas above.

1. Fulnames
2. Telephone number
3. Mobile number
4. Fax number
5. Country

GLOBAL GESTORES S. A.
MR. FERNAND CORTES (claim officer)
TEL: +34 672-892-907
FAX: +34 911-820-312
Email: globalgestores@luckymail.com or globalgestores@terra.es

All information will be strictly verified by your agent before payment will be carried out. You are hereby obligated abide to instruction from your agent to avoid processing errors.

Congratulations once again from our board of Directors.

Mrs. Angela De La Costa
EURO MILLIONES BOARD.
Madrid, 14th July. 2010.

****
This email is confidential and is intended solely for the person or Entity that own this email address [efrauenstein@wsu.ac.za]. If you have received this message in error, we inform you that the content in it is reserved and unauthorized use is prohibited by law, therefore, please notify us by e-mail.
****

Figure 4.5: Email scam involving a large sum of money won in a lottery

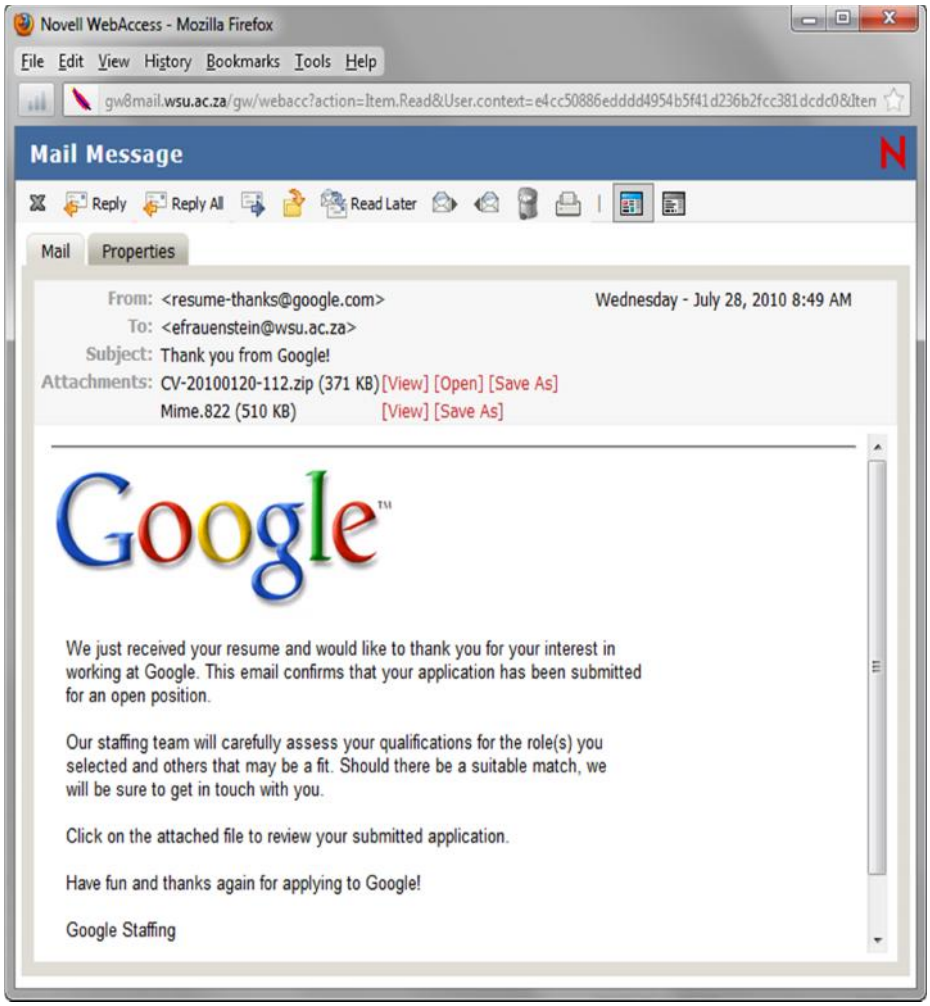


Figure 4.6: Email scam luring the user to open an attachment provided in the email

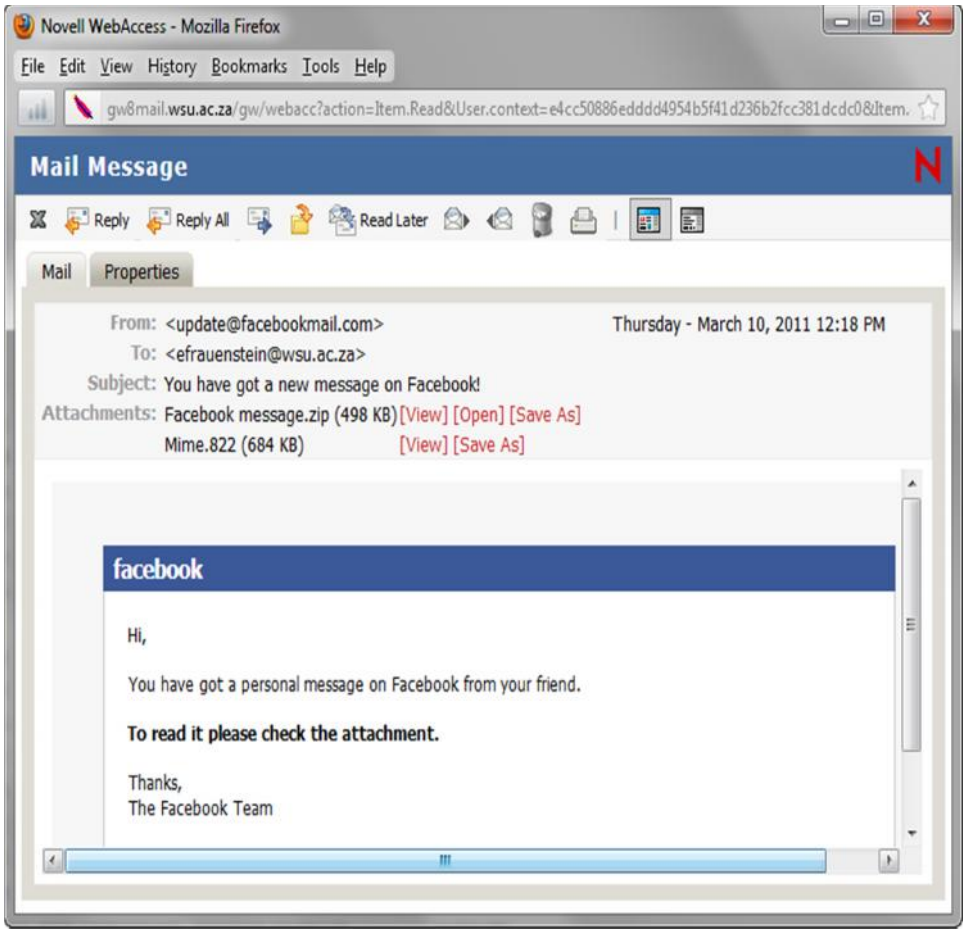


Figure 4.7: Email scam taking advantage of the popularity of social networking websites

The scam illustrated in Figure 4.7 can be quite effective considering the popularity of Facebook. As there is a high probability that the email recipient is registered on Facebook, this increases the chances of the victim falling for this particular scam. The victim is required to open an attachment (a virus) which they think originates from a Facebook friend. The Facebook branding and logos are used in this scam to enhance its authenticity.

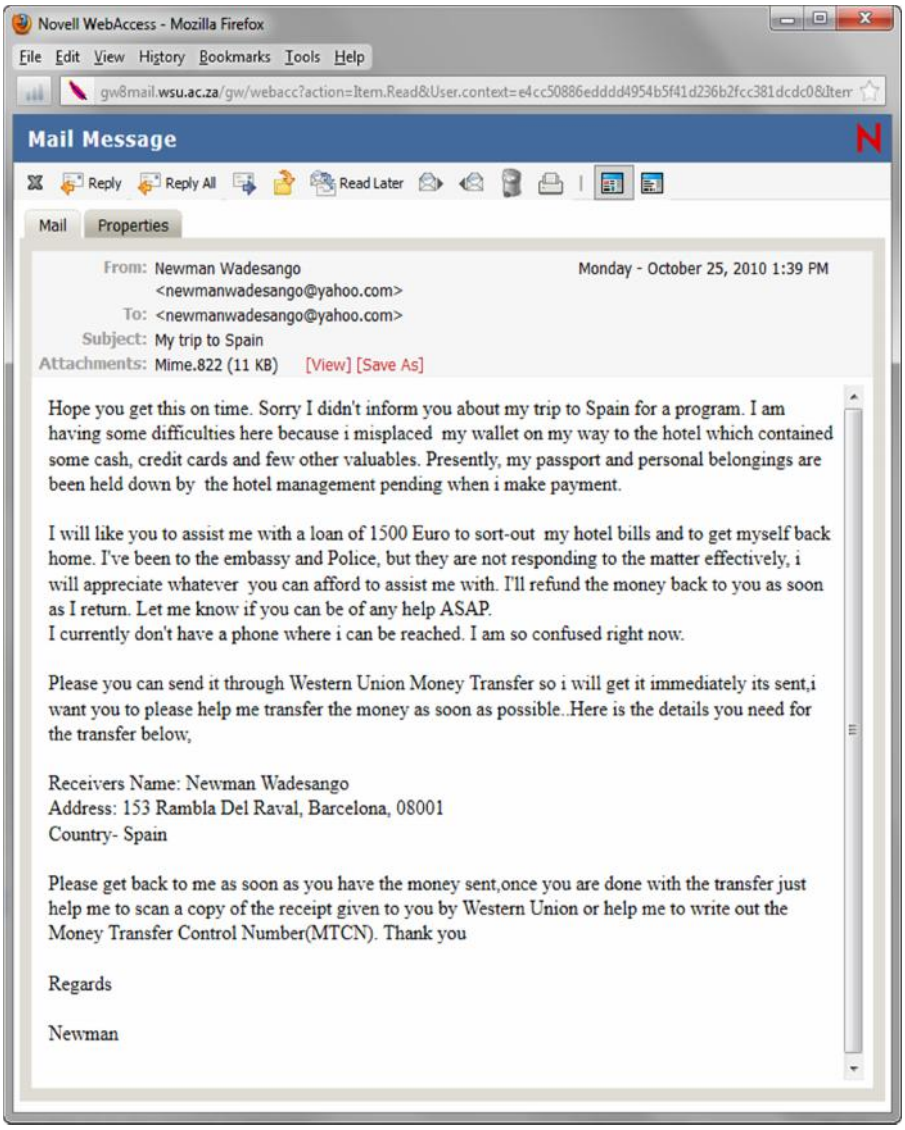


Figure 4.8: Email scam originating from a legitimate entity

The scam in Figure 4.8 originated from an actual work colleague. The email address, name and surname are correct thereby increasing the likelihood that the recipient will trust the authenticity of the message. In this instance, maybe as a result of software vulnerability, the victim's email account was vulnerable to the threat. Consequently, access was gained to the victim's email account and requests were sent to the victim's contacts, in this instance requesting financial aid.

In light of the examples cited above, it is obvious why they are so effective. Such emails attract users and convince them that they have been selected to receive irresistible offers, which, in most reported cases, usually constitute large financial rewards. This section pointed out that phishers are able to employ technical mechanisms to avoid detection by technological controls. Email scams usually appear in non-risk attachment form, for example, documents or images. However, some scams require a user to *open* an attachment or a zip file that may contain a virus or malware. Email scams can also be directed to cell phone users in text message form.

Many scams manipulate human emotions; for example, they make an appeal on behalf of parents who are in desperate need of funding to have their baby's tumour removed. Such scams are enhanced by, say, a picture of the baby. Phishing emails also use some of the scam techniques just discussed and are also considered a subset of spam. Having described the manner in which phishing is carried out, it is incumbent to describe the risks that may result from these attacks, as the combination of phishing and malware, advertised by spam, has become one of the most deceptive combinations on the Internet (Aaron, 2010). The next section emphasises the significant danger phishing poses to both consumers and affected organisations.

4.3 Phishing: A Threat to Users and Organisations

Section 2.3.2 described the dangers that general information security threats pose to organisations. This section highlights the serious threat phishing poses to organisations and users.

As section 2.2 revealed, organisations are becoming increasingly dependent on IT to facilitate the functioning of their business operations (ISACA, 2009). Flowerday and Von Solms (2005) assert that the majority of organisations today are totally dependent on their information assets. Using information and communication technologies (ICTs), these assets are stored, processed and communicated electronically within information systems. However, this very same technical environment is ironically what phishers use to gain access to organisational assets. As a result, ensuring sufficient network security is one of the major concerns for

organisations and users. To ensure business continuity, information resources have to be protected, especially since information is considered the lifeblood of most organisations (Von Solms & Von Solms, 2006). The fact that information workers (Von Solms & Von Solms, 2009) are vulnerable to social engineering techniques places organisations at risk and, as a result, the literature commonly refers to people as being the weakest link in the information security chain (Mann, 2008; Russell, 2002), particularly in an organisational context. Since organisations possess beneficial financial information they are naturally the targets of phishers.

Victims, in the form of organisations and individuals that have fallen prey to phishing, have been affected by, among other things, large financial losses, damaged reputations and identity theft (Sophos, 2005). For example, Mi2G, a company that sells products related to electronic banking, became a victim of a phishing scam in 2003. It subsequently estimated its economic damage as being between $32,2 billion and $39,4 billion US dollars.

In 2003 alone, Gartner estimated that 57 million American adults received a phishing email and more than half of the respondents were also identity theft victims (Litan, 2004). In 2005, Gartner estimated total losses to $1 billion (Litan, 2005). One year later, financial losses reached $2,8 billion (Litan, 2006). These statistics point to the fact that phishing is on the increase.

In South Africa, approximately three million attacks were launched in the first three months of 2012 (Alfreds, 2012). Alfreds (2012) further states that users were targeted by both offline and online malware spread through storage devices (e.g. removable USB drives, CDs and DVDs). Despite South Africa not having the same exposure to threats as more developed societies, 37,4% of users were attacked by local threats (Alfreds, 2012). According to Drake et al. (2004) and Aburrous, Hossain, Dahal, and Thabtah (2010), security threats may threaten e-commerce because such threats cause people to lose their trust in online transactions for fear that they may also become the victims of fraud. Many people believe that the use of online banking may increase the likelihood of their becoming victims of identity theft, even though online banking offers more secure identity protection than paper and mail-based systems (Van Dyke, 2004).

There are a variety of threats that seek to obtain sensitive information (Janczewski & Colarik, 2007), which gives organisations even more reason to protect themselves. According to Sophos (2005), consumers are the main target of phishers. Nevertheless, the impact of phishing extends beyond the consumer, as organisations' public image, consumer confidence and reputations can also be damaged in the process (Colwill, 2010; Frauenstein & Von Solms, 2010; Sophos, 2005). Organisations have clients, and if their clients suffer losses then such organisations will also be affected possibly even bringing the functioning of the organisation to a standstill (Von Solms & Von Solms, 2009).

In recent times, the use of social networking websites has become increasingly popular for phishers as a source of personal information (Bilge, Strufe, Balzarotti, & Kirda, 2009; Brown, Howe, Ihbe, Prakash, & Borders, 2008; Frauenstein & Von Solms, 2010; Gibson, 2007; Leavitt, 2005; Ohaya, 2006; Unisys, 2008). This substantiates the point that threats are constantly seeking to exploit new weaknesses in humans (Orgill et al., 2004) and, therefore, are seeking to use modern technology to carry out their attacks. Users of social networking websites unwittingly share too much of their personal information which phishers conveniently use. This is mainly due to such websites allowing registered members to share certain types of information about themselves, for example, birth date, email address and pictures to develop their online social networking profile (Gross & Acquisti, 2005). The latter inadvertently encourages registered users of these websites not to understand the importance of making their personal information private. This lack of good practice cultivates weak information security behaviour (Thomson et al., 2006) on the part of both the individual and, arguably, the organisation (i.e. the website itself). Since popular social networking websites (e.g. Facebook, MySpace, and Twitter) are certainly addictive for some members, employees may spend excessive amounts of time on these websites during working hours – insecure behaviour which could potentially place the organisation at risk. Frauenstein and Von Solms (2010) list these threats and risks as follows:

- puts the reputation of both the employee and the organisation at risk
- may constitute anti-social behaviour
- makes the system vulnerable to viruses, phishing and scams.

Van der Merwe et al. (2005a) noticed a responsibility shift with regard to security issues. They state that, previously, security was always the responsibility of the organisation or service provider. As a result of phishing attacks, however, the responsibility of security has shifted to the user who engages in an online transaction. If one analyses this assertion more closely, in light of a real-world example, one begins to see the validity of this claim. Should an account holder have money deducted from their bank account without their knowledge, they would contact the bank. However, financial institutions do not generally accept responsibility for losses resulting from client negligence. Although institutions usually have technological protection measures in place, for example, access control by means of a card, pin, biometric scanner or password, to safeguard accounts from unauthorised access, the account holder in this instance may not have followed these procedures correctly. For example, they may have not protected their pin, they may have fallen victim to a phishing email, they may have not logged out of an online banking website or computer terminal correctly, or a Trojan virus may have monitored keystrokes from the user's keyboard (Sophos, 2005). The only support a financial organisation can provide, in this regard, is to warn the public at large of the dangers of phishing. This is usually done through awareness campaigns on television, websites and mobile alert notifications**.**

According to Butler (2007), phishers are successful in carrying out their attacks because consumers are not adequately informed about the risks of disclosing their personal details online. Similarly, Cobb (2010) argues that the organisation's clients are the first and last line of defence against phishing, and any effective solution must include them. Organisations may not feel that it is their responsibility to educate their clients about online security, but ensuring that clients are educated to recognise phishing attacks is a cost-effective strategy that will help to defend the reputation of the business.

In this section, it was emphasised that phishing attacks pose a significant danger to both users and organisations and can result in large financial losses. Another reason for concern is that phishing techniques are evolving with technology, for example phishers increased interest in using social networking websites to reach their victims.

Drake et al. (2004) believe fraudsters will continue to adapt and expand their methods to reach and defraud their victims. Another matter for concern is that humans are not demonstrating security-conscious behaviour, which presents organisations with a serious challenge to protect themselves. In the next section the literature on developments in combating phishing and some methods for protection against phishing in terms of human, organisational and technological aspects will be discussed.

4.4 Developments to Combat Phishing

This section addresses some developments in combating phishing threat agents, as contained in the literature studied. These developments are categorised into the main areas of technology, human and organisational aspects.

4.4.1 Technological Controls

The previous chapter established that organisations focus a great deal on applying technological controls to combat general security threat agents. This is also evident in phishing protection. There are many advantages and disadvantages to the use of technology. Some tasks still rely on humans to make correct decisions or judgements based on their knowledge and/or experience, which is difficult for any computer to match. For example, in comparison to computers, humans tend to be better at distinguishing faces in crowds (e.g. friends from strangers) or noticing suspicious behaviour in humans (Schneier, 2003). However, one cannot ignore that technology performs a vital role in the functioning and protection of a system against phishing attacks. The following paragraphs describe some of the technological controls used to combat phishing.

4.4.1.1 Website Controls

After falling victim to phishing attacks, high profile organisations such as PayPal™ and AOL™ have provided educational information on their websites to educate their customers on the dangers and identification of phishing emails. Furthermore, AOL™ for example has implemented automatic anti-phishing controls among others on its website to protect its customers.

Specialised anti-phishing websites, such as PhishTank, are dedicated to assisting users to identify spoofed websites by assisting users to verify whether a website is genuine or not. PhishTank also allows a community of registered users to contribute suspected phishing websites to PhishTank's database, which makes a contribution to the battle against phishing. Other popular websites dedicated to reporting and educating users on phishing include the Anti-Phishing Working Group (APWG) and SonicWall.

4.4.1.2 Web Browser Security Plug-ins

A great deal of literature is focused on the development of web browser plug-ins to combat phishing. Garera et al. (2007) studied the structure of URLs evident in various phishing attacks. Fette et al. (2007), on the other hand, present a method for detecting phishing emails by using a specialised filter, designed to focus more on phishing emails than other general purpose spam filters. Their results show that over 96% of phishing emails were correctly identified by the filter and only 0,1% of legitimate emails were incorrectly classified.

Kirda and Kruegel (2006) developed a free Mozilla Firefox web browser plug-in called AntiPhish. This plug-in aims to protect inexperienced users against phishing websites, keep track of the users' sensitive information and generate warnings if users type their personal information in a spoofed website. In line with Kirda and Kruegel's research, Yue and Wang (2008; 2010) developed a Mozilla Firefox web browser plug-in known as BogusBiter, which feeds a large number of fake (bogus) credentials into a suspected phishing website and conceals the victim's true credentials amongst the fake credentials. This also enables the genuine website being threatened posed to identify when a phisher is using stolen credentials.

Yue and Wang (2010) concede that there are indeed a few limitations to BogusBiter's effectiveness: phishers may decide to use JavaScript attacks to evade detection by BogusBiter or they may steal a user's credential directly using keystroke monitoring techniques. Phishers may also use non-standard login pages to evade BogusBiter; for example, they may use irregular HTML login forms, use CAPTCHA on login pages, or create the entire login webpage in Flash format. This demonstrates that phishers are constantly seeking new techniques to counter the technology controls that are in place.

Krammer (2006) developed a Novel client-side web browser plug-in called Quero, which implements several techniques to protect the user against visually indistinguishable address manipulations.

4.4.1.3 Web Browser Warnings

As stated in Chapter 3, many studies have pointed out that web browser plug-in developments are common and are useful tools in the battle against phishing. One would assume that web browser security, specifically toolbars and warning alerts, is sufficient to warn users against entering their details in spoofed websites. However, Yue and Wang (2008) and Wu, Miller, and Garfinkel (2006) disagree, stating that studies have demonstrated that neither server-side security indicators nor client-side toolbars and warnings have proven to be successful. Various authors, including Dhamija, Tygar, and Hearst (2006), Downs et al. (2006), Egelman, Cranor, and Hong (2008) and Florencio and Herley (2005), express the same opinion. They substantiate this view by stating that even when users are presented with security indicators or warnings, they simply ignore them.

Wu et al. (2006) conducted two user studies to test three security toolbars, as well as other browser security indicators (i.e. browser address and status bars), and found them to be ineffective in preventing users from falling prey to phishing attacks. These authors state that the study participants disregarded the toolbar warnings even after they were asked to pay particular attention to them. They also found that many users did not understand what a phishing attack is and how sophisticated they can be. Moreover, they found that users did not constantly check the security indicators of their web browsers for warnings, as they felt this was not part of their primary goal in accomplishing their work tasks. This would reveal that users do not understand their responsibilities relating to security for themselves and the organisation.

Wu et al. (2006) add that when users noticed suspicious activity as evidenced by the indicators, they did not interpret the warnings correctly. Wu et al. (2006) believe that, in order to address this challenge, an active interruption such as pop-up warnings would be more effective than passive warnings displayed in the web browser toolbars. However, Wu et al. (2006) acknowledge that even pop-up confirmations may become less effective over time. As there are many pop-up boxes evident in application software packages and some are part of operating systems, this may

prove to be true as users may become irritated by these warnings and simply ignore them as they are too concerned with completing their primary tasks. Wu et al. (2006) suggest that Internet-based organisations can play a unique role in enabling users to distinguish their organisation's website from a spoofed website by following some standard practices. Wu et al. (2006) elaborate on this, stating that organisations should use a single domain name that uniquely matches their brand name. In addition, rather than using IP addresses or multiple domain names for servers, they should use SSL to encrypt their websites.

This subsection highlighted the fact that technology is most predominant, method for protecting users and organisations from phishing attacks. To a certain extent, this is to be expected, considering that, as discussed in Chapter 3, the majority of general information security threats are controlled using technology. In this subsection, much research focused on web browser security, specifically identifying phishing URLs, web browser extension/plug-in development and web browser warnings. Other technical areas which may be considered but have not been discussed include network security (i.e. firewalls) and anti-virus software.

As humans are considered the weakest link in any security initiative, it is evident that most of the technology discussed in this section can be perceived as a way to reduce human involvement. This is substantiated by Patrick et al. (2005), who state that "current security systems are often seen as difficult to use, as getting in the user's way, or confusing the issue. It is not enough to design systems that are theoretically secure without taking into account the end users."

Technology can be used as a tool to help users identify spoofed websites and phishing emails, but unfortunately, as the literature points out, humans do not know how to use these tools correctly, do not feel it is their responsibility to use them, and in general do not understand phishing. The human weakness discussed here is a double-edged sword, as people not only create the technology but also use it. Threats expose the flaws in technology that are a result of human error in its development process. They also expose the danger posed to information systems by human behaviour as a result of a lack of knowledge in using technology and technology controls correctly. Therefore, human involvement has not been totally eliminated from both perspectives. Section 4.4.2 expands on some of the points

mentioned above, in particular educating users in the identification of phishing emails.

4.4.2 Human Factors

Section 3.4.2 discussed human behaviour and social engineering techniques in detail. The following paragraph will discuss the educational developments aimed at addressing the human element in phishing.

4.4.2.1 Security Awareness, Training and Education

Researchers regard education as a solution to address the human factor in phishing. In this regard, organisations typically conduct information security training workshops. Downs, Holbrook, and Cranor (2007) suggest that in order for anti-phishing tools to be effective, they should consider *how* and *why* people fall victim to phishing. Their study surveyed 232 computer users to provide more insight into why users fall victim to phishing emails and why they trust phishing emails. The results of their study suggest that users may be more vulnerable to phishing attacks as their awareness of the risks involved are not linked to the perceived vulnerability in identifying phishing emails. Therefore, users will have to be trained in understanding the risks of phishing. However, according to Ogren (2009), even if users receive on-going user education on phishing, it is necessary to test employees and customer awareness by giving them at least three anti-phishing messages before they depart for the holidays. Furthermore, an anti-phishing educational campaign should be created that reaches its audience via email, video snippets and social communications such as blogs, social networks and websites (Ogren, 2009).

Van der Merwe et al. (2005a, 2005b) compared the nature of phishing attacks with the guidelines of the security service. Accordingly, they identified five issues related to the characteristics of a phishing attack that an organisation should be aware of. These issues are listed below:

- **Education**. Users should be educated on prevention techniques and provided with a strategy for preparing to avoid phishing attacks.
- **Preparation.** This consists of the process of thinking and stipulating what one would do in the event of a phishing attack.
- **Avoidance.** This includes activities that evade the onset of an attack.
- **Intervention.** This involves activities where the user/organisation involved in a phishing attack intervenes or steps in to affect the outcome of the attack.
- **Treatment.** This includes the activities needed to effect recovery after a phishing attack has been experienced.

As they point out in the guidelines above, Van der Merwe et al. (2005a) recommend that all users, on both a business and a personal level, be educated to be aware of the above-mentioned issues.

4.4.2.2 Security Training in Web Browsers

As section 4.4.1.3 shows, researchers support the notion that web browser security warnings have been proven to be ineffective in phishing prevention. Agarwal, Renfro, and Bejar (2007) suggest that the solution to this problem is to educate users to examine existing web browser indicators 'attentively' (e.g. URL, SSL indicators and optional toolbars). Agarwal et al. (2007) maintain that these indicators are restricted by three issues:

- "Users do not know which indicators are trustworthy;
- Browser indicators can be easily spoofed (e.g. by including them in the page or painting over them with chrome-less windows);
- Users do not look outside their primary areas of interest."

Drake et al. (2004) and Ohaya (2006) also point out that users, specifically naïve users, require more understanding of security indicators in an online environment. Cobb (2010) adds that "clients should be informed in how to check the security settings of their web browsers, how to check for the 'padlock' icon and certificate signature on pages, as well as tips such as not sharing passwords, pin or account

numbers with anyone". The latter point is also supported by Downs et al. (2007) and Ohaya (2006). Drake et al. (2004) further suggest that education should aim to address users' understanding of the risks rather than merely warning them about the risks.

Dhamija et al. (2006) conducted a laboratory study in which 22 participants had to distinguish from twenty websites which were spoofed websites. In this study most of the participants gave attention to the web browser indicators (e.g. address bar, status bar), with 23% looking for security indicators only in the website content. The authors concluded that browser security indicators are frequently misunderstood or ignored, and that many users do not notice them.

The padlock icon at the bottom of a web browser bar indicates that the website is in a secure state. However, Jakobbson (2007) states that threat agents may also place the padlock icon in the content of the page, whether victims intend to establish an SSL connection or not. He argues that educating consumers on the padlock will not eliminate the problem and that studies have proven that users are unable to distinguish a valid certificate from one that is invalid or self-signed and may not even be able to detect the absence of indicators. This is supported by a recent study by Jakobsson and Ratkiewicz (2006), which indicated that "while users often detect the presence of incorrect information, they almost never detect the absence of correct information".

4.4.2.3 Training in the Identification of Phishing Emails

Downs et al. (2006) conducted a laboratory study in which they interviewed 20 non-expert computer users in order to determine their decision-making strategies when using email. In the interview, participants were required to role play and respond to a set of legitimate and fraudulent email messages directed to an email inbox. The study revealed that many participants were unable to distinguish legitimate emails from phishing emails. The study further revealed that even participants who were knowledgeable in distinguishing phishing emails were not able to apply this knowledge to unfamiliar attacks.

The Drake et al. (2004) study explored the tricks used by phishers in emails. These tricks are classified according to whether they are used in fraudulent emails or in the

spoofed websites accessed from the hyperlink contained in the email. These researchers developed a system known as MailFrontier. The MailFrontier index detected that one out of ten participants who evaluated a phishing email fell victim to a phishing attack. In common with users who ignored web browser phishing warnings, users also ignored MailFrontier's warnings. Drake et al. (2004) add that most phishing emails use generic greetings such as "Dear Customer" or "Dear Member", or the victim's email address is inserted as a greeting. They insist that by educating organisations to address their customers by name would allow their customers to identify these generic emails as fraudulent.

4.4.2.4 Training Conducted through Gameplay and Training Systems

Some researchers have made use of technology to help educate users. To increase the effectiveness of information security education, some researchers have incorporated a fun aspect by developing educational games. Gameplay can be effective in increasing user participation during training. If training is considered fun, then users may enjoy it and, more importantly, remember what they have learnt.

Some researchers further discuss using a game theory strategy to teach users about avoiding threats attack (Shing, Shing, Chen, & Lee, 2010). Sheng, Holbrook, Kumaraguru, Cranor, and Downs (2010) designed an interactive online game known as Anti-Phishing Phil, which educates users on good habits that help them to avoid phishing attacks. The game had three objectives, namely, to teach users how to identify phishing URLs, to identify cues in web browsers and the use of search engines in finding legitimate websites. Sheng et al. (2007) state that, "after less than 15 minutes of training via the anti-phishing game, study participants improved their ability to distinguish legitimate and fraudulent websites considerably". The results of their study revealed that implementing an educational strategy into interactive games is an effective method for teaching people how to avoid phishing attacks.

Kumaraguru et al. (2007) designed an embedded email training system known as PhishGuru. PhishGuru educates people about phishing during their normal use of email. Users were sent simulated phishing attacks and trained after they became victims of the attacks. Prior studies tested users immediately after training and demonstrated that embedded training improved user's ability to identify phishing emails and spoofed websites. In Kumaraguru et al.'s (2007) study it was found that

- "Users learned more effectively when the training materials are sent by email (non-embedded);
- Users retain and transfer more knowledge after embedded training than after non-embedded training;
- Users with higher Cognitive Reflection Test (CRT) scores in comparison to lower CRT scores are more likely to click on links in the phishing emails perhaps due to their curiosity."

Furthermore, Kumaraguru et al. (2009) investigated the demographic factors that influence training and their general phishing susceptibility. The results of their study have revealed that the following:

- "Users trained with PhishGuru retain knowledge even after 28 days;
- Adding a second training message to reinforce the original training decreased the likelihood of people submitting information to phishing websites;
- Training does not decrease users' willingness to click on links in legitimate messages."

In Kumaraguru et al.'s (2009) study, researchers found no significant difference between males and females in terms of the tendency to fall for phishing emails both before and after the training. However, they found that participants in the 18 to 25 age group are more vulnerable to phishing attacks in comparison to older participants.

This subsection revealed that education is necessary to help users identify phishing emails and spoofed websites. It is evident that much research focuses on improving user education on the technical aspects of the web browser. The literature also describes a variety of techniques to enhance user education, with some studies using technological tools such as email systems and gameplay to educate people on phishing. The next subsection discusses aspects related to the organisation in the context of information security.

4.4.3 Organisational Aspects

Section 3.5 discussed in great length the organisational aspects related to protecting organisations against general security threats. These aspects include organisations paying attention to processes for managing employee behaviour in this regard. As the strategic responsibility for an organisation lies with top-level management, that is, the CEO, and because information is an organisational asset, it is the board of directors' responsibility to ensure that the assets are protected as these will ultimately assure success (Von Solms & Von Solms, 2006). Many organisations are aware of the importance information security and have, thus, adopted standards and best practices such as ISO/IEC 27002, King III, the NIST frameworks and COBIT 4.1 (Von Solms & Von Solms, 2009). These standards and best practices encapsulate various methods and guidelines for helping to keep information secure. Although these best practices provide guidelines for managing general information security threats, they unfortunately neglect to include phishing. Accordingly, no preventative measures for dealing phishing are referred to at any point in these standards and best practices.

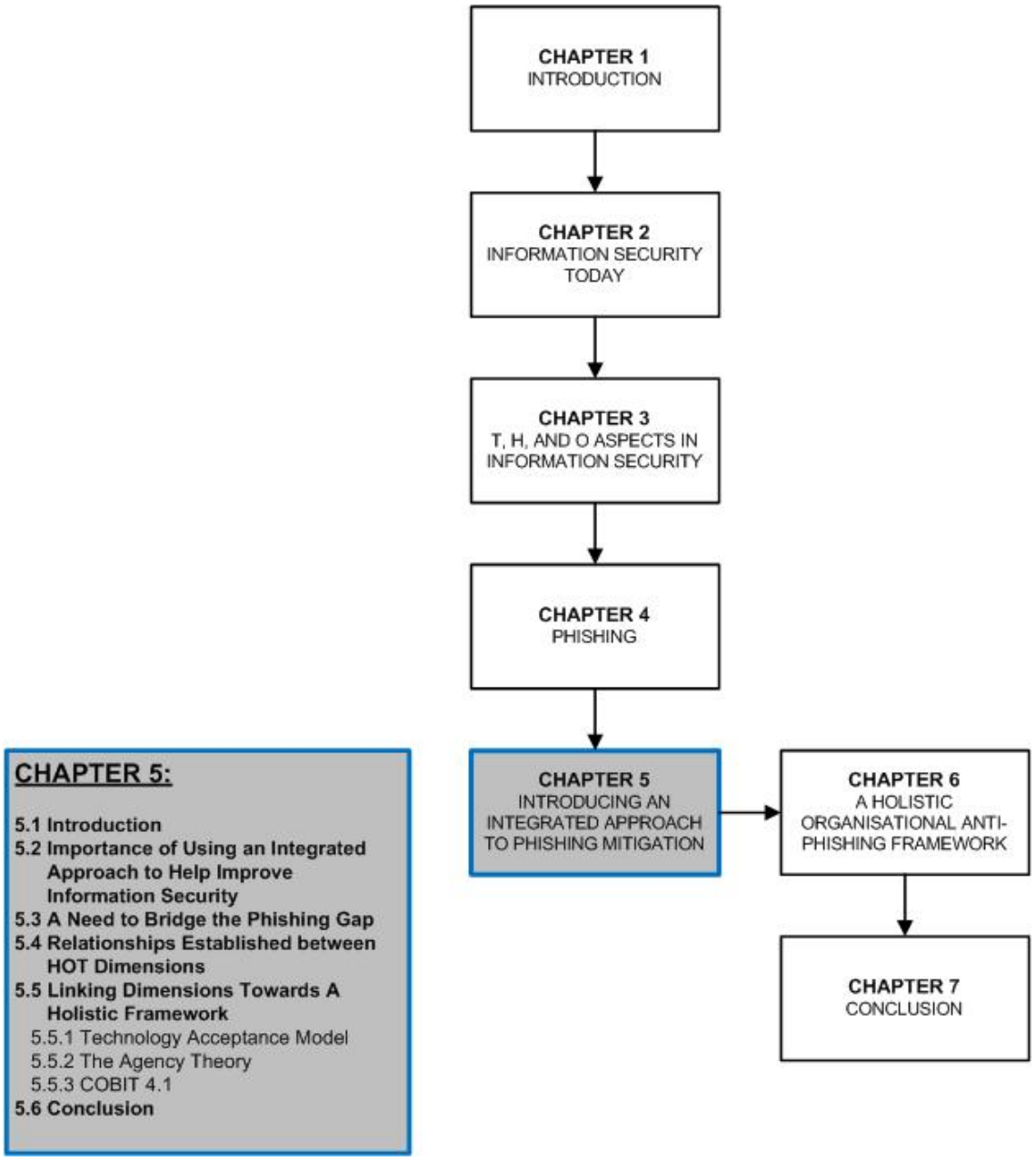
This section established that humans exert a major influence in terms of their use of technological controls in organisations to combat phishing threats. Even if certain technological controls are in place, if they are not understood and used appropriately, both the technology and the humans using it can become vulnerable to phishing threats. There is a paucity of literature describing standards and best practices that specifically address phishing attacks, even though such standards should as a matter of course be in place to govern the use of technology and human involvement in organisational processes. Organisations can implement security policies and procedures with regard to managing phishing attacks. Nevertheless, such policies can be, unintentionally or intentionally, ignored and neglected. The common element in all the processes is that all the dimensions that have been mentioned involve humans.

4.5 Conclusion

This chapter described phishing and the techniques it employs. The systematic steps phishers use to lure their victims were also described. In section 4.3, phishing was described as a threat to both users and organisations. However, most of the literature studied does not address phishing in terms of protecting organisations, but rather in terms of protecting users on a personal level. For example, general user education on the secure use of personal email at home or in the workplace is addressed, but the effects of phishing on the organisation are generally ignored despite the fact that its demise would affect both its clients and its employees.The literature does, however, highlight a number of areas exploited by phishers, which, coincidentally, are also the controls that assist organisations to safeguard themselves against phishers. These areas were categorised as human, organisational and technological dimensions. Of these, two areas that receive the most attention are technological controls and human factors, with the organisational dimensions, specifically with regard to phishing, being neglected. Humans still cannot conclusively identify phishing emails and spoofed websites despite the technological tools available to assist in this regard. The literature revealed that even when users are trained, they still fall victim to phishing. As such, human factors are said to pose the greatest risk to organisations. This is not coincidental, as these were referred to earlier as being the greatest risk to general information security. To address these human factors, much research has been placed on security awareness, training and education, policies and procedures and, finally, the implementation of technological controls. Nonetheless, it would seem that these three dimensions have not been satisfactory harmonised or aligned. For example, organisations either apply technological controls or they educate their staff on how to use these technological controls, they seldom do both. As a result, an opportunity (i.e. gap) is created for phishing to proliferate and subsequently to compromise the other dimensions.

The next chapter introduces the concept of an integrated human, organisational and technological (HOT) approach to address phishing holistically, instead of using a single-layer defence model as is currently the case. The chapter also elaborates on the gap between the dimensions which phishers aim to exploit.

CHAPTER 5
INTRODUCING AN INTEGRATED APPROACH TO PHISHING MITIGATION



5.1 Introduction

In the previous chapter, the effectiveness of phishing attacks and the techniques that are used were described in detail. Furthermore, the three dimensions identified when addressing such attacks, namely, technological controls, organisational aspects and human factors, were examined. It would seem that these three dimensions act in a synchronised manner both as barriers against phishing and as areas for phishers to exploit. Moreover, each of these dimensions has weaknesses that expose the organisation to phishing attacks, and therefore also affect the other related dimensions. To reduce this security gap, a holistic approach is required whereby *all* dimensions are integrated to form a stronger barrier of defence. This approach requires management, particularly in strengthening the links, or relationships, between each of the dimensions. The achievement of a managed approach is one of the core objectives for this study, as this could eventually result in a holistic anti-phishing framework. Accordingly, an examination of existing theories related to information systems research, might assist in understanding how these relationships can be integrated and managed.

The objective of this chapter is to introduce the concept of an integrated HOT approach in order to address phishing holistically, instead of using a single-layer defence model. In doing so, three important links between the HOT dimensions will be established. Finally, theories will be examined in order to guide an understanding of the way the relationships between each of the dimensions can be managed more effectively.

5.2 Importance of Using an Integrated Approach to Help Improve Information Security

The previous chapters categorised areas of information security and phishing into three dimensions, namely, **H**uman factors, **O**rganisational aspects and **T**echnology controls (HOT). This section provides a brief literature background substantiating the notion that, in order to improve information security, an integrated approach is required. This preoccupation with an integrated approach stems from the concern that general information security practices are usually applied using a single-layer approach (e.g. applying only technical controls), as described in previous chapters.

The aim of using an integrated approach is to increase the level of protection against phishing attacks. Accordingly, an integrated approach should consider the three above-mentioned dimensions.

The HOT concept is not new and its application has not been restricted to the IT discipline. According to Berglund and Karltun (2007), the concept of HOT was developed during the 1980s in the nuclear power industry in order to improve safety. Initially, safety in this industry was addressed through technical advances, which reduced the number of near-accident incidents caused as a result of technical failures. However, it later became evident that the majority of reported accidents were caused by humans rather than the technology. After a period during which the focus fell on the field of potential 'human error', safety was further improved. At that time it became apparent that it was also necessary to consider organisational aspects such as policies and procedures. Subsequently, this led to the realisation that all three HOT dimensions in the system needed to be considered in order to improve safety comprehensively (Eklund, 2003).

Coincidentally, in an information security context, the literature also points out that technological controls are used mainly to resist general information security threats (Beznosov & Beznosova, 2007). According to ISACA (2009), this is because some regard information security solely as a technical discipline. Beznosov and Beznosova (2007) support this by stating that "public research related to computer security has been overwhelmingly focused on technological aspects, leaving human and social dimensions mostly uncharted". As a result, organisations are dedicating large amounts of money to technical solutions, while neglecting the other dimensions in the organisation that may be exploited by security threat agents.

Chapter 3 discussed various applications of technical solutions in detail. However, the literature also recognises that technology is not the only way to manage general information security related risks (Gonzalez & Sawicka, 2002; ISACA, 2009; Parsons et al., 2010). Subsequently, human factors became another important focus of information security research (Parsons et al., 2010). Furthermore, to understand why users behave and react in certain ways when presented with difficult situations, human psychology (Jakobsson, 2007; Schneier, 2008; West, 2008), human-computer interaction, user security awareness (Dodge Jr., Carver, & Ferguson,

2007; Thomson & Von Solms, 1998), attitudes and behaviour (Downs et al., 2007; Stephanou & Dagada, 2008), and organisational culture (Cabrera, Cabrera, & Barajas, 2001; Helokunnas & Iivonen, 2003; Schlienger & Teufel, 2003; Thomson et al., 2006) are all distinct areas of interest in the area of human factors.

In the literature studied, the main developmental areas of *technological controls, human factors* and *organisational aspects* are often treated as separate entities. This subsequently exposes a possible gap in protection for threat agents to target. Cabrera et al. (2001) emphasise that technology and people are only two of the several subsystems that function within the organisation. They suggest that in order to understand the interconnections between technology and people, a broader scope which describes the relationships between the two and other important subsystems needs to be employed.

Besides technology, Werlinger, Hawkey, and Beznosov (2008) see a need to understand the impact of human and organisational factors. They state that few researchers have provided a comprehensive integrated overview of the challenges faced by security practitioners. Furthermore, they add that "a better understanding of how different human, organisational and technological elements interplay could explain how different factors lead to security breaches and vulnerabilities within an organisation". As such, their study involved the development of a framework to assist organisations in identifying their limitations with regard to implementing security standards.

Human factors and organisational aspects have also been found to be important areas in the effectiveness of other critical systems, such as safety and accident mitigation (Rasmussen, 1994). Similarly, Dhillon and Backhouse (2001) suggest that a socio-technical approach needs to be adopted that addresses both the human and organisational aspects. Besnosov and Beznosova (2007) recommend that future research should focus on examining the *relationship* between organisational processes and behaviour in the effectiveness of security defences. They elaborate further, saying that one could study decision-making processes and operational routines within organisations to improve understanding of the way they influence the security position of the organisation. The current study discusses a holistic approach to addressing phishing threat agents in an organisation; the following paragraph

describes how the elements of an information system are closely related and dependent on each other.

The five main elements of an information system are people, procedures, data, hardware and software (Shelly & Vermaat, 2011; Whitman & Mattord, 2003, p. 15; O'Leary & O'Leary, 2010). Fundamental to an information system is the *people* element, which has a major influence on all the other parts of the system. People are considered to be the most important organisational resource as they have both a direct and an indirect involvement with all the other parts of the system (Patterson, West, Lawthom, & Nickell, 1998). At the same time, it is significant that people are regarded as the weakest link in any information security context (Deloitte, 2009; Ernst & Young, 2010; Nelson, 2011), as people use hardware and software for their daily tasks. Moreover, it is people (normally management) who develop the organisational policies and guidelines that define acceptable and unacceptable employee behaviour in the workplace.

Hardware and *software* can be viewed as technological components of the **technological controls** dimension, while *policies and procedures* can be considered to be part of the **organisational aspect** and *people* fall under the category of the **human factors** dimension**.** Finally, another important component and asset of the organisation, as established in section 2.2, is *data or information*.

Each of these five components of an information system has its own inherent strengths and weaknesses. Each has its own procedures and security requirements which can be followed or neglected, intentionally or unintentionally, by the people who use them (Whitman & Mattord, 2003, p. 15). It is humans (the users) who have to ensure that all the previously mentioned aspects are operating correctly. If the organisations' policies and procedures are obeyed and understood correctly, it will help to ensure that, ultimately, all elements work in synergy with one another and the system performs securely, productively and accurately. This will help ensure that the organisation's information is protected from unauthorised access, use, disclosure, disruption, modification or destruction. However, should one of the elements be compromised, this may result in the organisation's data being put at risk and/or damaged.

For example, in an information security context, the *software* element is not a sufficient defence on its own if it is not regularly updated, maintained or used correctly by the people using it. Software can also be affected by viruses or contain bugs caused by programmer coding errors.

Procedures are the methods, rules or guidelines that are developed to direct *people* in accomplishing organisational objectives. Procedures can help coordinate the information system elements and, if defined properly, can together with suitable technological controls reduce the threat of a breach in an information system, regardless of the method of attack.

In an organisation, *people* make up the staff, end-users, managers and decision makers among others who are involved in the information system to make it more productive. Figure 5.1 below presents the Business Model for Information Security (ISACA, 2009), which features similar core elements to the ones identified here, that is, people, organisation and technology (POT) and describes the interdependencies between these elements.

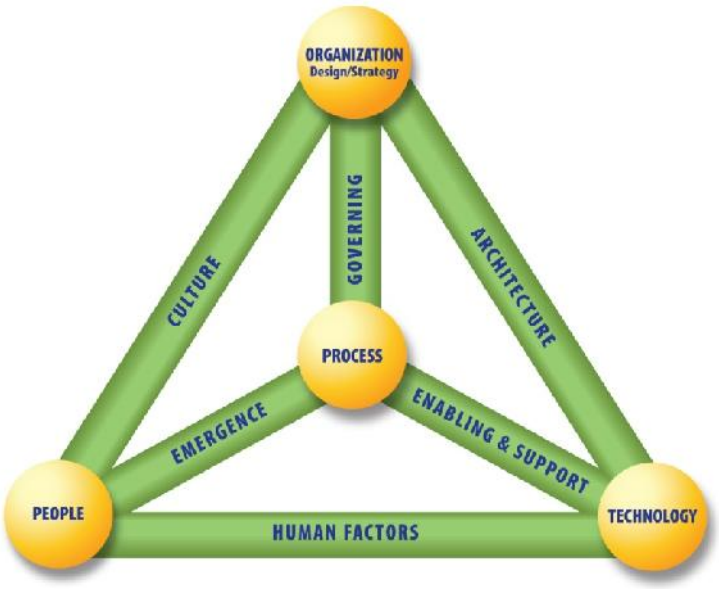


Figure 5.1: Business Model for information security (extracted from ISACA, 2009)

This model can be used to predict the way in which technology, process, organisation or human resource is affected by culture, human factors or other dynamic interconnections. This existing model is further evidence for the relationships between dimensions. Werlinger et al. (2008) explicitly highlight the HOT dimensions as an approach to addressing information security and specifically focus on the need to manage the interconnections between each dimension.

Werlinger et al. (2008) further define the organisational challenges each of the dimensions face. They identify the attributes of each of the dimensions, as described in Table 5.1 below:

HUMAN ASPECTS	ORGANISATIONAL ASPECTS	TECHNOLOGICAL ASPECTS
• Related to the cognition of individuals • Culture • Interaction with other people	• Structure • Size • Managerial decisions of IT security	• Applications and protocols

Table 5.1: HOT attributes (adapted from Werlinger et al., 2008)

Table 5.2 lists the challenges identified by Werlinger et al. (2008) in the HOT aspects with regard to implementing security controls. This suggests that there are difficulties inherent in the use or implementation of technological controls by humans. In Figure 5.2, Werlinger et al. (2008) illustrate the HOT challenges and the interplay of the corresponding relationships in an organisation. In Figure 5.2, the two-sided arrows indicate the association between the HOT factors, while single-sided arrows indicate that one factor affects the other factor, but not vice versa. This figure illustrates that there are many links between the factors and the dimensions that may be overlooked.

Table 5.2: HOT challenges in the implementation of security controls (adapted from Werlinger et al., 2008)

ASPECT	CHALLENGES
HUMAN	• Lack of training or experience • Culture within the organisation • Communication of security issues
ORGANISATIONAL	• Risk estimation • Open environments and academic freedom • Lack of budget • Security as low priority • Tight schedules • Business relationships with other organisations • Distribution of IT responsibilities • Access control to sensitive data • Size of the organisation • Top management support
TECHNOLOGICAL	• Complexity of systems • Software vulnerabilities • Mobility and distributed access

In Figure 5.2, Werlinger et al. (2008) discuss the interplay between the various IT challenges. Although they consider human and organisational factors in the

development of security processes and technologies, they do not explain how these factors can be managed more effectively.

Werlinger et al. (2008) therefore acknowledge that more research is necessary to understand the interplay between security challenges, as these interactions affect the organisation's security levels and the extent to which they can be improved.

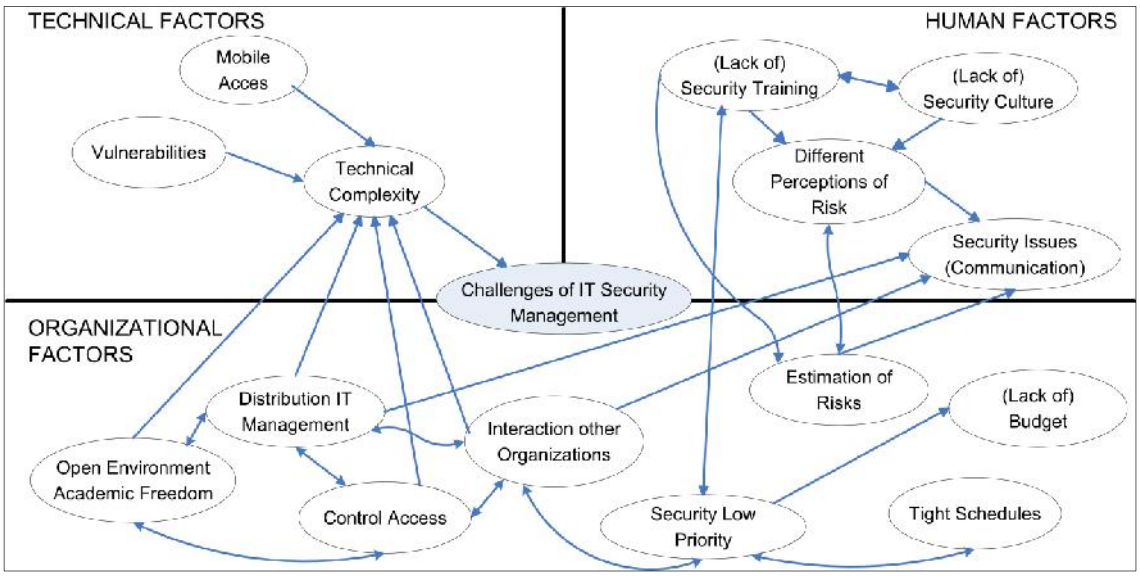


Figure 5.2: A holistic view of the challenges within the HOT factors and their interrelationships (extracted from Werlinger et al., 2008)

In their research, Cabrera et al. (2001) reveal that an integrative model will help both administrators and technology designers to understand and manage the interconnections between technology and the other human and organisational aspects of their business. Furthermore, they state that it is important to pay special attention to the factors that determine the behaviour of people in a particular organisation. Moreover, they maintain that organisational culture needs to be understood as it will describe factors that influence human behaviour. This would seem to underline the need to explore the factors that influence these relationships.

This section provided supporting evidence from the literature studied to describe an integrated approach that can be used to strengthen information security practice. However, this approach requires more understanding particularly in the integration

aspect. In this study, the ‘integrated approach’ consists of merging three main areas, namely, human factors, organisational aspects and technological controls. This approach will contribute to the creation of a HOT framework focusing on the prevention of phishing attacks.

To accomplish this integration, the main areas require more understanding, particularly in the way they influence relationships and in how they can be managed. This stems from the concern that an isolated single-layer defence approach is insufficient to mitigate phishing attacks comprehensively. More importantly, since each dimension has its own inherent weaknesses, even when a dimension is coupled with another dimension (e.g. H+T), the gap for phishers to exploit is not eliminated. As pointed out by Werlinger et al. (2008), these gaps become more apparent if dimensions are interrelated because of these very relationships. These interrelationships between dimensions have been demonstrated by relating information system elements in the context of the HOT dimensions.

The literature describes a need to suitably align the interdependencies or relationships that exist between HOT dimensions. As a result, some sources discuss adopting an approach whereby all HOT elements are included and, therefore, some studies have already partly integrated some of the dimensions. However, it would also seem from the literature studied that there are challenges with this integrated approach. Firstly, there needs to be an understanding of how to integrate these dimensions, as failure to achieve this could result in one relationship being compromised as result of it being loosely coupled and may have an undesired effect on other dimensions. Consequently, this could expose a gap in which phishing attacks could proliferate. To reduce this gap, the relationships that influence these dimensions need to be understood and addressed in more detail. The next section aims to achieve this. By describing problem-based scenarios, the following paragraphs shed more light on why victims fall prey to phishing attacks, putting into context the HOT dimensions and their role in the process. The section also establishes the main relationships between dimensions. The scenarios help to explain why ‘loosely coupled’ relationships are referred to as a ‘gap’.

5.3 A Need to Bridge the Phishing Gap

This section aims to further explore the loosely coupled link between HOT dimensions by using practical scenarios. These scenarios point out, in a phishing context, that there are relationships that exist between HOT dimensions. At the same time, this section also points out the gaps between each of these relationships. Understanding which relationships depend on one another will help establish which of the main HOT relationships require strengthening.

Scenario A: John receives an email from his banking institution. The email warns John that the bank's customers may be subject to fraudulent activities. Therefore, he is requested to verify his banking details to validate his account. The email provides a hyperlink which will direct him to the bank's website in order to complete this verification process.

In this scenario, John will have to know how to distinguish email scams or phishing emails from legitimate emails. Accordingly, this knowledge will determine his actions and behaviour in reaction to the email. In this scenario, the technological controls had failed, as the phishing email reached John, consequently exposing the human factor dimension, and making John vulnerable. Alternatively, if John had not received the phishing email, then the technological controls might have performed their role adequately by preventing the email from reaching him. In this case, the phishers used social engineering techniques combined with technological tools with the intention of tricking John into submitting confidential information (see section 4.2.2).

However, in this scenario, John could make effective use of technological tools such as an anti-virus program and/or features of the email client. If he can correctly identify the phishing email, then he can use the email client function to mark the email as spam, possibly preventing such emails from reaching him again in the future. Section 5.5.1 describes further activities that John can engage using technology. In these instances, only a single-layer defence is present, that is, either technological controls or human factors. Therefore, it can be established that in Scenario A **human** (H) and **technological** (T) dimensions are linked (H, T) and require further strengthening.

Scenario B: John manages to find time during working hours to communicate with his friends on his office computer terminal using social networking websites and other applications. From his computer terminal, he also manages to download software, games, movies, wallpapers and music, as he does not have an Internet connection at home.

In Scenario B, it would seem that John disregards any security risks he might pose to the organisation as he accesses social networking websites. Section 4.3 revealed that social networking websites have become a breeding ground for phishing attacks, as well as other information security threats. Should confidential information related to the organisation or its employees be leaked to phishers, this may put the organisation's reputation and its information at risk. John is abusing organisational resources by using the organisation's Internet service for his personal interests. He is also abusing organisational time, as he downloads files and is active on social networking websites instead of carrying out his work-related tasks. John is being paid to perform his duties at work and not for any personal activities. Some of his activities, such as downloading games, could potentially expose the organisation to viruses or Trojans, which may originate from phishers, consequently putting the organisation's information at risk. Excessive downloading may also affect the organisation's network connection speed or data capacity download limit. John should be made aware of the risks involved in falling victim to phishing emails. However, as pointed out in Chapter 4, phishers make use of a variety of modern and sophisticated technologies and techniques to trick their victims and John may not be aware that phishing is not limited to the use of emails. Through social networking websites, John may have clicked on hyperlinks, supposedly sent from his online friends, thereby downloading a virus or having his account hijacked. Consequently, he may not perceive any risk until an accident occurs, which is not ideal. Accidents themselves are not a viable policy tool for the improvement of information security. Organisations should not merely react spontaneously to security events as they occur, but should rather be proactive in their approach. This is supported by Gonzalez and Sawicka (2002), who state that "it is desirable that compliance with security measures is 'brought back' to a safe level long before the system enters the

accident zone, preferably before it enters the extinction of conditioned behaviour zone".

Background activities related to Scenario B could be organisational policies and procedures that strictly manage the use of technology by employees; for example, an Internet usage policy. On a user level (the human factor), John should be familiar with organisational policies and should adhere to them. Policies and procedures can also help ensure that he understands what encompasses acceptable and unacceptable behaviour in the workplace. However, even when aware of security policies, employees may choose not to adhere to them either because they have malicious intent or because they are inconvenient (Herath & Rao, 2009). Therefore, John should be aware of the risks that security threats pose to him personally, as well as technically knowledgeable about using websites, hyperlinks, email clients, software and so on. Even if John understands the risks of phishing emails, he may still fall victim to links on or originating from social networking websites.

In Scenario B, it is evident that there is a clear gap between John's needs and what the organisation expects and requires from John. In this instance, the main links that can be compromised by John's actions are the **human** (H) and **organisational** (O) dimensions. Section 5.5.2 discusses this link in more detail.

Scenario C: The organisation has very slow Internet connection and sometimes no Internet at all. As a result, staff often blame the organisation for not completing tasks on time. Moreover, the computer hardware and software are outdated and the organisation has no clearly defined policies or procedures describing the acceptable use of software or placing any restrictions on its use. In addition, individuals do not require authorisation to enter the work premises. Although staff training workshops are offered staff do not participate and generally absent themselves from such training.

In Scenario C, it is evident, that, from a technological perspective, the organisation is not providing a suitable service. It should ensure that technical staff apply technological controls such as network firewalls and anti-virus programs, and ensure that they updated regularly and managed correctly. The organisation could restrict

users (employees) from accessing social networking websites from their workstations during work time or even permanently. This could be achieved by implementing technological controls such as firewalls or authentication measures.

The organisation is not implementing good practice in that it does not use technology to carry out business functions correctly, accurately and efficiently and in a timely fashion. As a result, opportunities may be created for phishers to expose any weaknesses inherent in the systems. Weak policies can allow for employees to bring in their own technology from home, opening up new opportunities for phishers and other threats. As a result of outdated hardware and software, viruses (perhaps originating from phishers) can penetrate the organisation's weakened information system and compromise its information and data. Moreover, since this organisation has no access control measures in place, any unauthorised person may enter the premises posing as an employee or customer. This imposter could be a social engineer (i.e. phisher) intent on analysing any physical, technical and behavioural weaknesses in the system. Consequently this information could be used to plot a phishing attack on the organisation. From this scenario it is evident that there is a gap between the **organisational** (O) and **technological** (T) dimensions.

In all three of the scenarios described above, it is evident that a loosely coupled approach has affected the other dimensions involved, as the dimensions were not tightly linked to another. As such, these dimensions were treated as isolated single entities, thus forming only a *single-layer* defence. This is illustrated in Figure 5.3. In all three scenarios the human element was targeted most frequently, even though other controls played a role. Consequently, if one of the dimensions is weakened, phishing attacks may proliferate, thus compromising the other dimensions (Frauenstein & Von Solms, 2011). Unfortunately, users may therefore be of the view that, since phishing penetrates technological defences, technology requires the most improvement. However, phishers most frequently exploit human behaviour which is made easier by a lack of knowledge in using technology correctly. Furthermore, humans lack of compliance with organisational policies and procedures favours phishers. In order, therefore, to be adequately protected against phishing attacks, particularly in an organisational context, a framework a required consisting of all the HOT dimensions (Frauenstein & Von Solms, 2009).

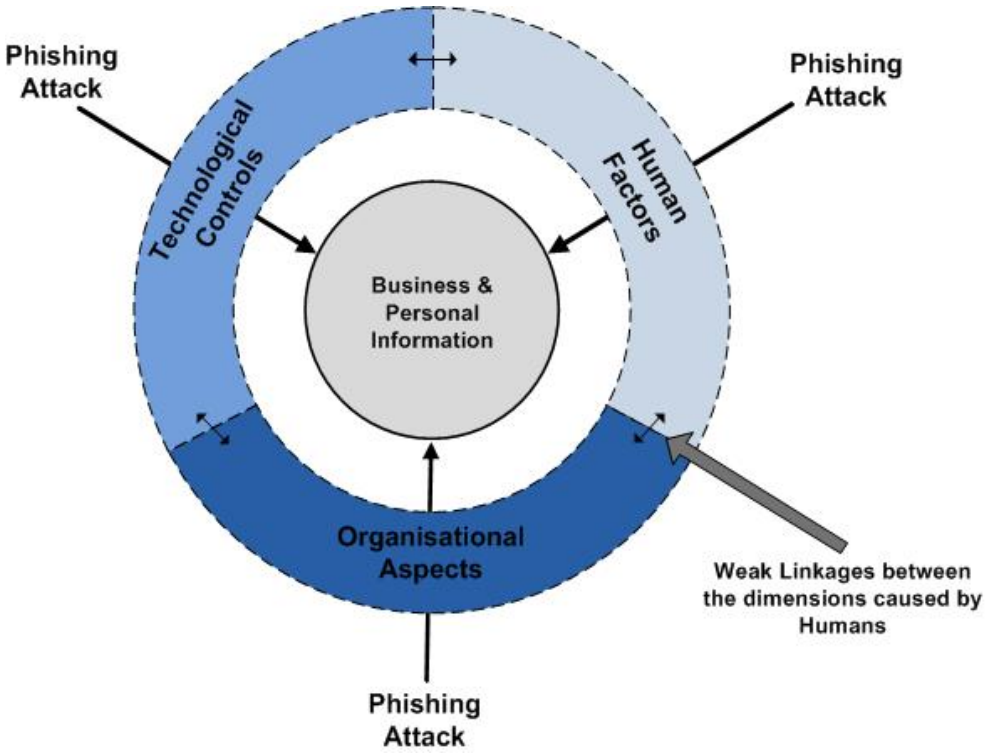


Figure 5.3: HOT dimensions targeted by phishers (adapted from Frauenstein & Von Solms, 2011)

This section revealed that there are indeed relationships that exist between each of the dimensions. However, these relationships are loosely coupled as a result of gaps in their protection. There is a need to close the gap between each dimension. If this is not done, any of the three HOT dimensions may be subsequently compromised to the detriment of the organisation. In the literature examined no approach could be found that describes ways to further integrate and improve the relationships between the HOT dimensions. In the next section, the introduction of the dominant relationships between each of the dimensions will be further examined. This is significant for determining how these relationships can be managed to form a tighter bond, thus reducing potential gaps in protection.

5.4 Relationships Established Between HOT Dimensions

Using scenarios in the context of phishing, section 5.3 demonstrated that there are indeed relationships between the HOT dimensions in an organisational environment. It also pointed out that these dimensions often depend on one another to achieve a function or process correctly. As can be seen in the above scenarios, the human (H), organisational (O) and technological (T) dimensions are loosely coupled to each other. This loosely-coupled approach provides the least amount of defence as it predominantly offers a single-layer defence. As mentioned before, the literature highlights cases where a dimension is paired with another dimension with the aim of forming a stronger layer of defence, for example (H+T). The aim of this study is to move towards a holistic framework which integrates all three elements of HOT. To accomplish this, important links or bonds need to be established between the following pairs of dimensions:

- **Human** and **Technology** (H,T);
- **Human** and **Organisation** (H,O);
- **Organisation** and **Technology** (O,T).

To identify the most suitable practices for binding these individual dimensions to one another, various theories and best practices will be studied. Hevner et al. (2004) support this approach, stating that the behavioural sciences approach this objective "through justifying theories explaining or predicting phenomena that occur". Using a design science approach would require the construction of innovative artefacts aimed at changing the phenomena that occur (Hevner et al., 2004). This process constitutes Hevner's second guideline, namely, problem relevance. In this regard, the phenomena are the loosely coupled links between the dimensions. Understanding theories and best practices can help strengthen the links between each of the dimensions in order to close the gap. The artefact is the anti-phishing model that results and which is revealed in the next chapter.

In section 5.3, three scenarios were used to describe the relationships between the dimensions and the consequences that could result should some of the relationships

be compromised. It is important that these relationships are strengthened to form a 'tighter' bond between each of the dimensions. In the next section theories and best practices are described that will assist in strengthening this 'binding' process.

5.5 Linking Dimensions towards a Holistic Framework

The previous section established and described the three main links that exist between the HOT dimensions. However, these links are still not tightly bound thus exposing a gap for phishers to exploit. As such, more understanding is necessary on how the links can be managed more appropriately. This section aims to achieve this by describing theories and best practices in conjunction with those links. An understanding of these theories and best practices will help point out specific areas that influence the respective dimensions, which will contribute to the establishment of an anti-phishing framework. The next subsection begins by introducing the popular Technology Acceptance Model, a theory that describes factors that influence the relationship between humans and technology.

5.5.1 The Technology Acceptance Model

Section 3.3 pointed out that technology has a useful role to play as it can be used in controlling and eradicating information security threats. It was also pointed out that organisations generally apply technological controls to combat general information security threats. However, one of the challenges in this regard is that technology must be accepted and understood in order to be used correctly by humans. For example, employees in an organisation are expected to be able to use Microsoft Office software applications correctly to create professional reports and presentations. If employees cannot use such basic application software technologies correctly, this would suggest that they cannot perform the duties expected of them. Security technologies can be even more challenging. In a study conducted by Furnell, Jusoh, and Katsabas (2006), the problems that end-users face when attempting to understand the security functions of common software applications were pointed out. In the case of specialised software, this may have even greater undesirable consequence. Specialised software comprises programs more narrowly focused on specific disciplines and occupations. For example, an automotive designer is expected to be able to design vehicles using specialised computer aided

design (CAD) software. If the automotive designer believes that merely using traditional tools to accomplish his tasks, such as paper, geometry tools and a pencil would suffice, potential faults may occur in his/her vehicle design that might perhaps have been overcome with the aid of technology. In the engineering fraternity it is accepted that using such software is common, advantageous and necessary, as it can help to reveal errors before a project is approved for manufacturing or development. Although it may be challenging to use the software at first, if the engineer undergoes proper training, he/she should be able to use it effectively. As a result, software developers place much emphasis on graphical user interface (GUI) design so that users are able to work with computer programs easily, productively and enjoyably (Galitz, 2007, p. 2). All of the examples mentioned relate to the human use of technology and the fact that technology is developed with the intention for being useful for humans. The next paragraph attempts to further explore this area.

Section 2.3.2 pointed out the dark side of technology, namely, use of technology by threat agents in order to commit crimes. However, there are many people who are not considered as a typical security threat agent to organisations. Such people misuse technology for unlawful activities. For example, cell phones are mainly used to communicate with others through voice and text messages. However, with the rapid development of the capabilities of such devices, they are often used unlawful purposes such as the pirate downloading of music, and games and so forth at no cost. Furthermore, involvement in pornographic activities, and sex chat (sexting). Using these devices, threat agents may also try to lure teenage girls into engaging in adult activity. In such instances, features of technology are exploited for the wrong reasons. In all these cases, it is human behaviour, and not technology, that needs to be addressed.

Many IT professionals consider that the key to the success of information security lies in the way humans use computers and technology. This brought to light the broad developmental area of human-computer interaction. Section 4.2 pointed out that phishers take advantage of aspects of human behaviour, specifically the way humans interact with computers (Schneier, 2000). Since it is apparent that humans are often unable to use technology optimally, developers are generally automating technology. Cranor (2008) substantiates this by stating that humans often fail in their security roles and therefore, to reduce human involvement where possible, it is

necessary for systems to be as automated as possible. For example, operating systems or anti-virus programs are usually set by default to be updated automatically from the Internet instead of requiring the manual involvement of the user (Ai Cheo Yeo et al., 2009). One of the factors that may cause humans not to use technology correctly is because it is technically complex; this one of the technological factors pointed out by Werlinger et al. (2008) in section 5.2.

The Technology Acceptance Model (TAM) is an information systems theory representing individuals' acceptance and usage of technology (Davis, 1989). For this reason, the TAM serves as a suitable model to understand the way in which the link between the human and technology dimensions can be further strengthened. According to Swanson (1988), one of the most challenging issues in information systems (IS) research is to understand why people accept or reject computers. If this can be understood, one would be able to predict, explain and increase user acceptance of technology (Davis, 1989). The TAM is an extension of Ajzen and Fishbein's (1980) study entitled "Theory of Reasoned Action (TRA)" and is used as a theoretical basis for specifying the causal linkages between two key beliefs. Accordingly, the TAM suggests that when users are presented with a new technology, a number of factors influence their decision about *how* and *when* they will use that technology. As discussed by Davis (1989), these two factors are

- perceived ease of use (PEOU)
- perceived usefulness (PU).

These two factors are regarded as important determinants of computer usage. Users' negative attitudes towards the use of technology may influence its perceived usefulness. To elaborate, users may feel technology is inadequate or that it always fails (breaks down) or is faulty. People who fear or do not like advanced technology and complex devices are said to have technophobia. A number of reasons may have contributed to this perception. For example, it may be caused by a lack of knowledge about technology and its potential benefits in that they may have experienced their computer starting up slowly or their anti-virus program not performing adequately in removing all the viruses on their system. There may be many other factors, other

than the technology itself, responsible for these challenges. As a result, users start developing negative attitudes and behaviour towards technology. Unfortunately, this is a result of users lacking knowledge about computer systems. For example, although humans tend to blame most computer-related problems on viruses, if they had knowledge of some of the technical and software related issues they might find that it is in fact a hardware related problem and not a virus.

According to Lee, Kozar, and Larsen (2003), TAM is a robust theory as it has been applied to many different software application technologies such as spreadsheets, graphics, word processors, email, v-mail, WWW, and hospital information systems. Adams, Nelson, and Todd (1992) found that, after examining the application of TAM to these technologies, it in general maintained its consistency and validity in explaining users' information systems acceptance behaviour. The TAM has also been applied to various situations (e.g. time and culture), with different control factors (e.g. gender, organisational type and size) and different subjects (e.g. undergraduate students, MBAs, and knowledge workers). This is an important issue, as phishers target different types of user under different conditions.

Since technology is one of the main dimensions in an anti-phishing framework, this theory will be used to understand the reasons why humans are susceptible to phishing attacks when they have technological controls at their disposal. Technology is frequently used by phishers as a tool to carry out their attacks. In response, users (the victims) should also be able to use technology as a tool to protect themselves against such attacks. However, the TAM's two factors of perceived ease of use (PEOU) and perceived usefulness (PU) of using technology can be used explain in more detail why humans find it difficult to identify the structure of spoofed websites and phishing emails. They may also help to explain why users ignore or pay little attention to technological warnings that appear on web browsers and suchlike. Consequently, education on and awareness of the use of technology and an understanding of its perceived benefits can help address the factors that influence perceived usefulness and ease of use.

According to Ai Cheo Yeo et al. (2009), substantive research highlights a strong relationship between attitude and behaviour (Ajzen & Fishbein, 1980). Accordingly, a change in attitude is likely to result in a modification of behaviour (Thomson & Von

Solms, 1998). The Theory of Reasoned Action (TRA) predicts that personal attitudes and societal norms are the two factors that guide behavioural intent. In this regard, attitude captures summary evaluations, such as good–bad, easy–difficult, harmful–beneficial, of a particular behaviour (Ajzen, 2001). For example, an organisation can have policies in place which restrict employees from visiting certain websites. This may make the employee develop a negative attitude to this, thus the employee may try to bypass this restriction as he/she feels it is a benefit for them to visit any website they wish.

Fogg (2002, as cited in Ai Cheo Yeo et al., 2009), states that, in recent years, research has been focused on using technology to intentionally persuade users to change their attitudes and behaviour in a predetermined way. To accomplish this, technologies such as computer systems, devices and software applications were used. According to Fogg (2002), this application of technology is defined as persuasive technology and is regarded as a major strategy for influencing people. Indeed, it has been applied in many disciplines such as marketing, health, environmental conservation and safety.

Using Scenario A in section 5.3 as an example, the involvement between the two dimensions of human (H) and technology (T) can be further described. In Scenario A, John represents the human (H) dimension and the use of technological controls (e.g. email client) represents the technological (T) dimension. There is no harm in John receiving a phishing email; the harm lies in his subsequent actions which may follow from his decision making. Accordingly, in the context of Scenario A, there are a number of actions or activities involving the use of technology that John could perform after receiving a phishing email.

- Use the email client functions: Open, Reply, Delete the phishing email, Mark the phishing email as junk or spam, Block from receiving further phishing emails from the source.
- Choose to ignore the phishing email.
- Click the hyperlink provided in the phishing email.
- Enter and submit personal particulars on the spoofed website.

- Download, run and save the attachment (if it is provided in the phishing email) to the local computer system or network drive.
- Scan the attachment (if it exists) using an anti-virus program.
- Report the phishing incident to other staff members (using email, organisational website, intranet, notice boards or directly).

In Scenario A, a number of technologies (mostly software) can be used. These technologies include the web browser, email client, anti-virus program and network firewalls. Other areas affected by the use of these technologies may require knowledge of websites, file management and so on. Firstly, it is important that John correctly identifies the email as a phishing email. Section 5.3 pointed out that a determining factor in John's choices mentioned above would be his knowledge and understanding of technology. John will also have to have knowledge on identifying phishing threats in order to make use of technology when needed. If John has a negative attitude towards technology and does not perceive any risk in visiting any website he wishes, this may pose a risk to both himself and the organisation. He may not perceive any risk in using an outdated anti-virus program. He may not take any of his computer system and web browser alerts and warnings seriously. Preferably, John should find the technology easy to use and useful for its intended purpose. If John finds technology useful, he would probably use the email client functions correctly (as described above) and mark phishing email as spam mail so that he no longer receives such emails from the source. Having these above-mentioned controls automated, does not guarantee that John will not in future fall victim to a phishing. However, in general if users do not accept technology, they may settle for alternatives to perform their tasks. These alternatives could result in the user performing inefficiently and consequently place the organisation at risk.

Ohaya (2006) points out in his study that most IT professionals continue to ask: "Why are many employees or users still susceptible to phishing?" Nevertheless, Ohaya (2006) feels that there are many reasons and lists the following as contributing factors:

- "lack of knowledge in computer systems;

- lack of security and security indicators;
- lack of attention to security indicators;
- lack of attention to the absence of security indicators;
- sophistication of spoofed websites."

These factors described by Ohaya reveal the gap between humans and technology. Ohaya (2006) explains that "many users do not have the underlying knowledge of how operating systems, emails and websites work. Many non-technical employees do not know what a domain name means and cannot tell the difference between a genuine website from a spoofed-website." Ohaya elaborates on the previous point with the following example, "[m]any users may think http://www.paypai.com is the same as http://www.paypal.com". Furthermore, the average employee does not know that a closed padlock icon displayed in the browser indicates that the web page is using Secured Socket Layer (SSL), which is a certificate verification process. Ohaya (2006) feels that to understand such topics employees should be part of the IT department or in the certificate verification business.

Another example added by Ohaya is that "technology-smart" phishers may use an image of a legitimate hyperlink but the image itself serves as a link to a spoofed site. This fools users in that they do not know that images can also contain links to websites. The result is that it is difficult for employees to keep up with the rapid technological advancements that phishers utilise in their attacks. In some cases, users ignore phishing warning messages from anti-phishing tools (Dhamija et al., 2006; Egelman et al., 2008; Florencio & Herley, 2005; Wu et al., 2006). This can be attributed to the fact that employees are too focused on their primary tasks to pay much attention to security indicators or the absence thereof.

Some phishers are very knowledgeable about web development and are able to develop websites that are almost perfect replicas of genuine websites (Jakobsson, 2007). This strongly suggests that individuals need to be educated, trained and made aware of phishing techniques and to be suspicious of well-designed spoofed websites. It also indicates that there are vulnerabilities in the way humans make use of technology. Accordingly, education is also necessary to train users of technology

to use it correctly. To strengthen the relationship between the human (H) and the technology (T) dimensions, education will have to ensure that employee behaviour is changed, as it will affect the actions mentioned above. Once education has successfully accomplished this change, the results will satisfy the TAM's objectives of

- technology (e.g. software) is **useful**
- technological controls are **easy** to use.

The literature studied has demonstrated that with any current or future technology development, key factors are necessary for making technology useful and easy for consumers to use. To successfully bridge the gap between humans and technology, it is imperative that users are educated about using technology correctly and seeing its usefulness.

As pointed out earlier in this context, it is necessary to understand why technology is not used by humans to mitigate phishing attacks, as the latter is a significant challenge. According to Adams et al. (1992), a subtle problem in examining the determinants of technology use is the notion of "captive use". They add that "[e]ven when usage is not strictly required as part of a job there may be no alternative but to use that system to effectively complete the job. Thus, the user's attitude might be, 'I don't like it but there's no alternative'". The latter statement can be linked to agency theory, which is described in the next paragraph.

The following paragraph describes agency theory, which will help explain the factors that influence the relationship between the human (H) and the organisational (O) dimensions.

5.5.2 Agency Theory

According to Eisenhardt (1989), agency theory is an important, yet controversial, theory because many authors have different interpretations of it. Eisenhardt (1989) states that scholars have applied agency theory in various disciplines, such as finance, economics, accounting, sociology, political science and marketing. Agency theory discusses the agency problem that arises when cooperating parties have

different goals and division of labour (Jensen & Meckling, 1976; Ross, 1973). This relationship is metaphorically described as a contract between two parties, namely, the *principal* who delegates work to the *agent* who performs that work (Jensen & Meckling, 1976). In this study, the research problem is addressed in an organisational context; as such, the principal is seen as the *organisation* and the agent is the *user* or *employee*. Agency theory is regarded here as being an appropriate theory to understand the significant role between human (employee) and organisational (management) dimensions.

The problem domain in agency theory is the relationship between the principal and the agent, who both have differing goals and risk preferences (e.g. compensation, regulation, leadership, impression management, whistle blowing, vertical integration, transfer pricing). According to Eisenhardt (1989), agency theory is concerned with resolving two problems:

- The conflicting desires or goals of the principal and agent
- The verification of the agent's activities, which is too difficult or expensive for the principal.

Conflict arises when the principal and the agent have different attitudes toward risk. These differing goals may explain why the agent (i.e. employees) disobeys or neglects organisational policies and procedures. The fact that organisations have policies and procedures in place means that there are no written disparities in what the employee should and should not do. However, even if an organisation has such policies and procedures in place, it should not necessarily be taken for granted that employees comply with and support them. Herath and Rao (2009) state that employee negligence and non-compliance with policies cost organisations millions of dollars every year. Accordingly, section 3.5.1 discussed the differences between policies and procedures and the related challenges.

To address the problems pointed out above, the principal aims to motivate the agent using incentives that recognise the agent's effort, as well as the environmental factors that have an effect on the outcomes (Herath & Rao, 2009). Bamberg and

Spremann (1987) illustrate this with an example: “the principal is assisted by the agent and the agent is deciding on level and kind of his effort. The principal is thus ready to pay some kind of reward to the agent in return for a certain decision, action or effort.”

As part of their research project, Schlienger and Teufel (2003) administered questionnaires at Orange Switzerland to determine whether employees knew and supported their organisation’s security policy. The results of their evaluation indicate that the security policy is known in general, but not supported by the employees or by management. According to Schlienger and Teufel (2003), this also indicates that the employees need extra security training and education.

For users to behave appropriately in the organisation they first need to be made aware of and given reasons why security policies and procedures are needed. Furthermore, they need to know and understand how to implement the procedures supporting such policies (Thomson & Von Solms, 1998). If this is not accomplished, users will put organisations’ information at risk. Organisational policies can ensure that employees cannot plead ignorance to the rules, as many insider problems stem from ignorance rather than malicious motivation (Cobb, 2010). However, in their study Schlienger and Teufel (2003) describe that even where employees know of security policies, they may still wilfully ignore such policies because they do not understand *why* they are needed. Educating employees on why such policies are in place not only increases understanding, but also increases motivation (Siponen, 2000). In terms of such policies, it is also important that employees understand their roles and responsibilities within the organisation. This is supported by ISO/IEC 27002 (2005, p. 23), which states that the organisation must ensure that its employees, contractors and third party users understand their roles and responsibilities in order to reduce the risks to the organisation.

Understanding why humans behave in a certain way in certain situations, or do not perform their duties according to the organisation’s procedures, requires a fundamental understanding of human behaviour. Establishing an organisational security culture is another element that cannot be ignored as it has great significance in agency theory. Organisational culture has two core elements, namely, *basic*

assumptions and *beliefs* (Schein, 1985). The organisational culture is consequently expressed in terms of the collective values, norms and knowledge of organisations (Schlienger & Teufel, 2003). In turn, those collective norms and values impact on the behaviour of the organisation's employees. If employees do not take the severity of risks posed by phishers seriously, they will affect other members of a particular organisation and thus put the organisation at risk. An information security culture, like an organisational culture, cannot be created once and then be used repeatedly (Schlienger & Teufel, 2003). To ensure that the organisational culture and the information security culture are aligned, culture has to be created and maintained or changed on an ongoing basis.

Herath and Rao (2009) point out that in the context of information security it is challenging to observe end-user behaviour. Similarly, Bamberg and Spremann (1987) add that "the principal cannot observe the agent's actions in full detail". Even when the principal is able to observe the agent's activities, it does not guarantee that the agent has done what is required of him/her in the interim to accomplish that outcome. This poses a problem – if the organisation does not fully observe its employees activities it may result in phishing threats entering the organisation through its employees. The information provided in this paragraph reveals that, generally, organisations may not completely trust their employees and therefore their employees have be monitored and supervised to ensure that the requirements of the organisation are met. This may create further conflict on the part of employees.

Using Scenario B in section 5.3 and considering all the variables that have an influence on agency theory to strengthen the relationship between the human (H) and the organisational (O) dimensions, the following factors should be taken into consideration. The next two paragraphs categorise **principal** and **agent** factors.

PRINCIPAL FACTORS

- Organisations should screen prospective employees carefully before employing them, preferably using trained employees for the task. This will allow organisations to trust and have confidence in their employees.

- Organisations should motivate employees. Organisations can introduce team-building workshops to encourage staff to work in teams. Furthermore, organisations can offer incentives to their staff.
- Organisations should have clear policies and should negotiate and draft related procedures. Government regulations and laws need to be understood by all parties concerned.
- Organisations can facilitate or organise information security training and anti-phishing campaigns. This can help to educate employees on the dangers of modern-day information security threats (specifically social engineering techniques and phishing).
- Organisations should educate their employees so as to understand their roles and responsibilities in information security (Van Niekerk & Von Solms, 2004a). More importantly, policies and procedures must be understood and followed.
- Organisations should have internal communication. There are two main forms: interpersonal and communication using media (Schlienger & Teufel, 2003).
- Organisations should perform monitoring and/or evaluation of its employees to determine whether they a performing according to organisational requirements and expectations.
- Organisations should ensure that employees can improve and further develop their career paths in the organisation. Further training and certification of such training can develop interests and skills.
- Organisations can reward staff if they go the 'extra mile' to meet the organisational targets set by their objectives. Rewards could include perks, incentives, verbal recognition, promotions and responsibilities. This will motivate employees.

AGENT FACTORS

- Employees should have knowledge of where to access organisational policies and procedures (e.g. intranet, organisation website, documentation).
- Employees should be made aware of organisational policies and procedures upon appointment through proper educational and awareness campaigns.

- Employees should understand their roles and responsibilities (i.e. daily tasks) and what is expected of them in the workplace.
- Employees should be cognisant of the organisation's mission, strategies, goals and objectives.
- Employees should understand that they are paid to perform a task or service to the organisation.
- Employees should be made aware of the severity of risks the organisation could face from security threats should policies be disregarded or neglected by them.
- Employees should understand the risk of noncompliance with organisational policies and procedures. Penalties or further disciplinary action may be taken against the employee.
- Employees should report all security-related incidents, for example to managers.

Addressing these factors requires both parties to understand their roles and responsibilities. In this regard, education is required to help change the behaviour of employees. Employees should have the best interests of the organisation at heart and should understand their role in protecting the organisation and not divert the responsibility to somebody else. If this could be achieved, this would satisfy the agency theory problems highlighted earlier, thus closing the gap between the human (H) and the organisational (O) dimensions. As such, this would also influence the agency problem alluded to earlier as follows:

- Principal's and agent's desires or goals **do not** conflict with each other
- Principal **can** verify what the agent is actually doing in the workplace.

The human-organisation (HO) link is an important hub from which other important processes between human-technology (HT) and organisation-technology (OT) flow. It would seem that there are some overlaps originating from the HO link that affects other relationships. For example, Posthumus (2009, p. 110) describes in his thesis that there is a close link between IT governance and agency theory relationships.

These overlaps can be explained and strengthened by education and will be discussed in the following chapter.

This subsection described the relationship between the employees as the agent and the agent's organisation (principal). It demonstrated that the relationship between these two parties is in conflict (based on differing goals), hence the term 'agency problem'. Agency theory has described many factors which influence the different objectives between these two parties. Most of these factors point out that employee behaviour needs changing, as employees do not comply with organisational policies and procedures. One of the factors that may have caused this relates to the limited knowledge of *why* such policies are needed. It is therefore important for the organisation to make its employees aware of this. This section further described factors that help to understand how to reduce the conflicting needs between employees and the organisation. An understanding of these factors pointed to the fact that an educational approach is necessary to solving these conflicting needs. Accordingly, education will help form a tighter bond between the human (H) and the organisational (O) dimensions. The following chapter will discuss further how education can be used to achieve this.

By examining an internationally recognised framework, the following paragraph attempts to understand factors that influence organisational (O) practice in terms of technology (T).

5.5.3 COBIT 4.1

Linking IT to business is not a new concept; it has previously been recognised as business-IT alignment. This alignment refers to "applying IT in an appropriate and timely way, in harmony with the business strategies, goals and needs" (Luftman, 2004). IT alignment specifically attempts to address the way the organisation should or could be harmonised with IT. For this reason, COBIT 4.1 serves as a suitable best practice to understand how the bonds between the organisational (O) and technology (T) dimensions can be strengthened. COBIT 4.1 (2007) is an organisational best practice and stands for Control Objectives for Information and related Technology. It is a framework and supporting tool set that allow managers to

bridge the gap between control requirements, technical issues and business risks, and communicate that level of control to stakeholders. COBIT 4.1 enables the development of clear policies and best practices for IT control throughout enterprises.

COBIT's objective is the following: "Specifying the decision rights and accountability framework to encourage desirable behaviour in the use of IT." It has been frequently pointed out in this study, human behaviour is a concern. COBIT is kept up to date and harmonised with other standards and guidelines that help in understanding and managing the risks and benefits associated with IT. The process structure of COBIT and its high-level, business-oriented approach provide an end-to-end view of IT and the decisions to be made about IT. Furthermore, COBIT provides good practices across a domain and process framework, and presents activities in a manageable and logical structure (COBIT 4.1, 2007, p. 4). IT governance implies a system in which all stakeholders, including the board, executive management, customers and staff, have clear accountability for their respective responsibilities in the decision-making processes affecting IT. These stakeholders form part of the organisational dimension.

The COBIT 4.1 framework covers five specific IT governance domains, namely, strategic alignment, value delivery, risk management, resource management and performance management. These domains are described in further detail in Figure 5.4 below.

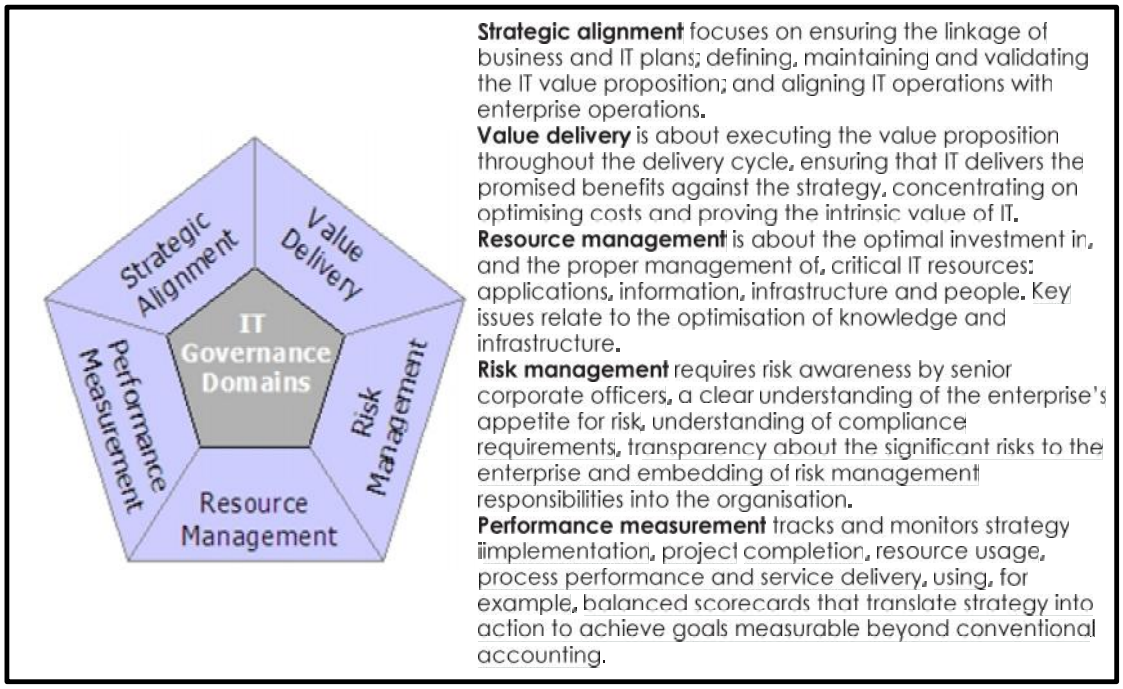


Figure 5.4: COBIT IT governance domains and their descriptions (adapted from COBIT 4.1, 2007)

Agency theory focuses specifically on organisational aspects (O) and the organisation's employees (H). COBIT, on the other hand, focuses on the organisation (O) and its use of IT (T). Extracted from COBIT 4.1, the benefits of implementing COBIT as an IT governance framework include the following:

- "Better alignment, based on a business focus;
- A view, understandable to management, of what IT does;
- Clear ownership and responsibilities, based on process orientation;
- General acceptability with third parties and regulators;
- Shared understanding amongst all stakeholders, based on a common language;
- Fulfilment of the COSO requirements for the IT control environment."

COBIT 4.1 can be used to prevent some of the challenges described in Scenario C. Elements of the COBIT 4.1 domains were selected specifically to deal with phishing

threats. The Delivery and Support domain of COBIT is concerned with the actual delivery of required services, which include service delivery, management of security and continuity, service support for users, and management of data and the operational facilities. This is important to ensure that phishing threats do not pose a risk to the organisation. The following box presents the controls extracted from COBIT's Delivery and Support domain of 'Ensure Systems Security' that are considered applicable in addressing the **organisational** and **technological** dimension specific to this study:

Delivery & Support 5: Ensure Systems Security

- DS5.1 Management of IT Security
- DS5.2 IT Security Plan
- DS5.3 Identity Management
- DS5.4 User Account Management
- DS5.5 Security Testing, Surveillance and Monitoring
- DS5.6 Security Incident Definition
- DS5.7 Protection of security technology
- DS5.9 Malicious Software Prevention, Detection and Correction
- DS5.10 Network Security
- DS5.11 Exchange of Sensitive Data

According to COBIT 4.1, **ensuring systems security (DS5)** would satisfy the requirements for IT by maintaining the integrity of information, processing infrastructure and minimising the impact of security vulnerabilities and incidents. This is applicable not only to phishing threats but also any security threat.

Within the COBIT 4.1 guideline of monitor and evaluate, **monitoring and evaluate internal controls (ME2)** and **ensure regulatory compliance (ME3)** were also selected as components that can improve the OT linkage. This monitoring and evaluating the effectiveness of controls is an important process given the ever-changing nature of technological controls and phishing attacks. As a result, controls may have to be improved accordingly.

This subsection points out that the responsibility shift in information security does not lie solely in the hands of users or employees. Management also has a vital role to play in ensuring that the organisational IT infrastructure provides a safe, reliable and secure environment in which its employees can perform their duties. As such, top-level management must support information security and ensure that employees are trained to exercise their information security responsibilities. If not, this will potentially create an opportunity for phishers to target weak IT infrastructure either by exploiting technological vulnerabilities, or through employee behaviour. This will consequently expose the organisation's vital information.

This section examined theories and best practices that are relevant to the main relationships that influence each of the dimensions. Theories and best practices provided guidance for understanding the variables that reveal gaps between each of the dimensions. As such, the section provided guidance on understanding *which* components within these links were in need of improvement. Figure 5.5 below brings the theories, best practices and their relationships with the dimensions into perspective.

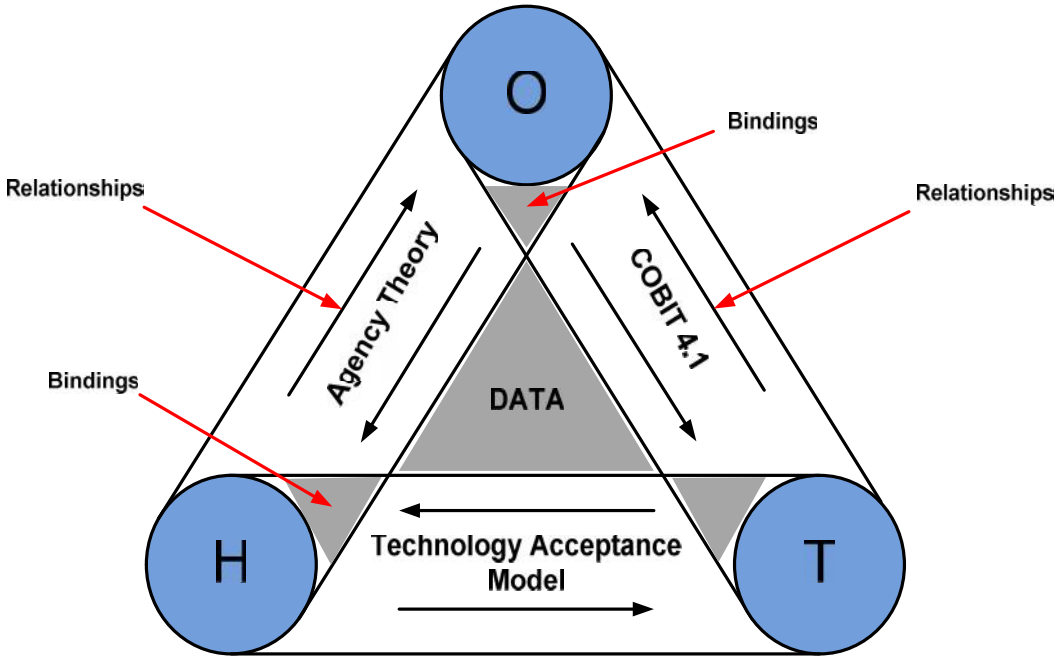


Figure 5.5: HOT linkages supported by theories and best practices

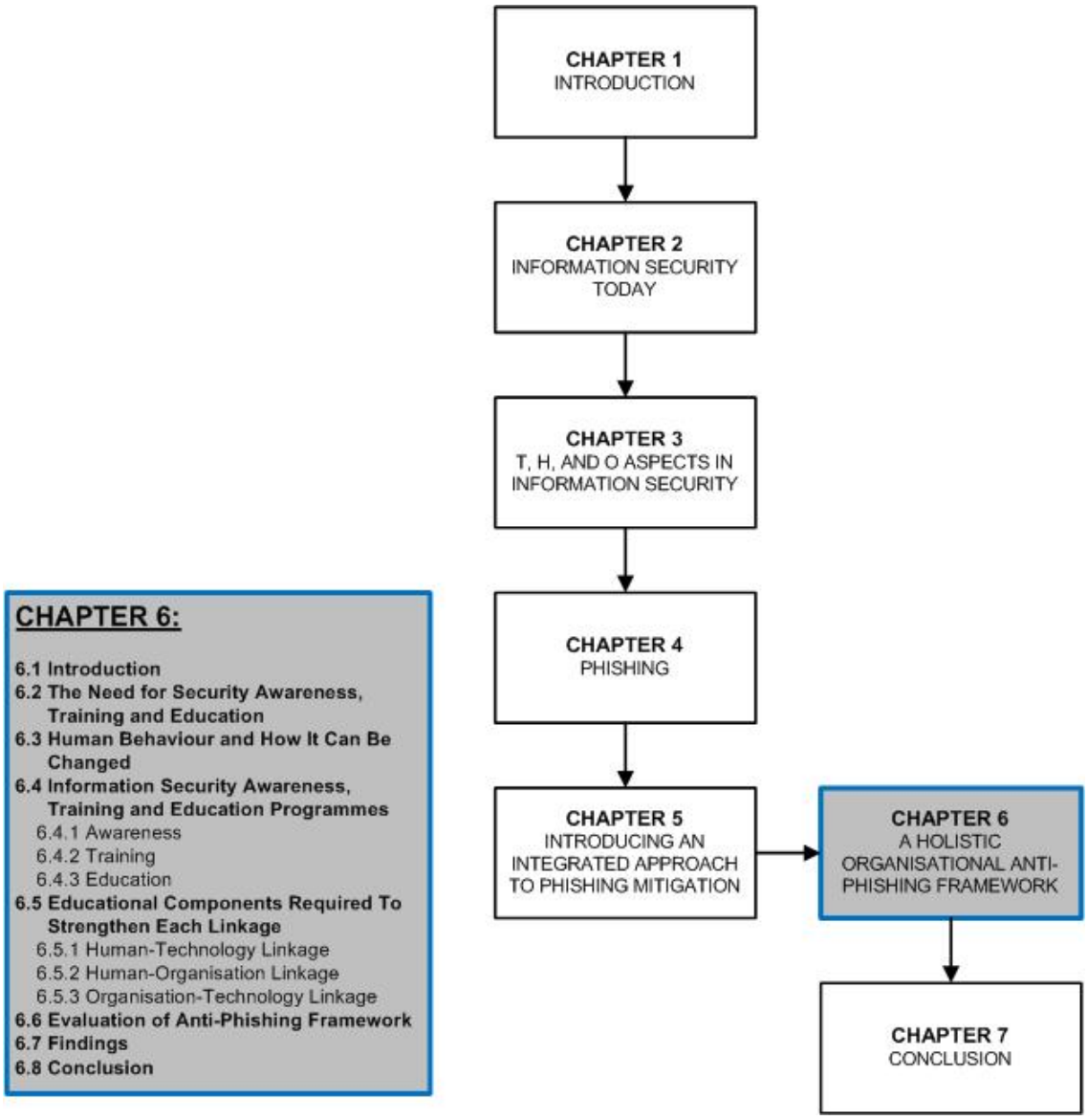
It is evident that in all three linkages (HT, HO, and OT), the attitudes and behaviour of users influence the functioning of these linkages. This is to be expected given that each link includes human involvement. Accordingly, education plays an essential role in ensuring that these linkages form a stronger bond with their respective dimension. From the understanding of the theories and best practices that has been created here, a number of gaps are highlighted between each of the links. Humans need to be properly educated to change their attitudes to technology and to see that it is easy to use and useful for its purpose. Moreover, humans need to be educated on security threats and their related risks. They also need to be educated in terms of carrying their roles and responsibilities safely in organisations; this is made possible by organisational policies and procedures. Finally, the organisation should ensure that its IT infrastructure and its associated processes are defined and managed correctly. Education will help facilitate communication between all three of the dimensions, and accordingly can be perceived as the catalyst that ignites the linkages between the dimensions. The relationships or linkages can be seen as the metaphoric glue that binds all dimensions together, thus forming a stronger layer of defence against phishing attacks**.**

5.6 Conclusion

This chapter introduced the concept of integrating human, organisational and technology (HOT) dimensions to help mitigate phishing attacks. It also established that there is currently no literature that can assist in describing *how* to integrate HOT aspects effectively. It is evident that a gap exists between the relationships and their respective dimensions, which created an opportunity to investigate ways in which this relationship can be further strengthened. Thus, the TAM, agency theory and COBIT 4.1 were used as suitable theories and best practices to help understand the components that influence each of the established links. Having understood the theories and their related components, it became evident that this gap was caused by human attitudes and behaviour in terms of the use of technology, security responsibility and compliance with policies and procedures. It emerged that education plays a vital role in strengthening this process and it can be seen as a catalyst for further bonding the relationships between the dimensions. This will allow for better communication between the linkages and their respective dimensions. As a

result, the current loosely coupled approach will form a tighter bond, subsequently closing the gaps that phishers try to exploit. The following chapter describes certain educational principles and develops an educational programme that can be used to strengthen the links between the dimensions.

CHAPTER 6
A HOLISTIC ORGANISATIONAL ANTI-PHISHING FRAMEWORK



6.1 Introduction

In the previous chapter, an approach to integrating human, organisational and technological (HOT) dimensions to address phishing threats was discussed. This approach was supported by the literature, which either encourages its use or integrates aspects relating to these dimensions. Three main linkages were established between the HOT dimensions. These linkages are, namely, human and technology (HT), human and organisation (HO) and, finally, organisation and technology (OT). Various theories and best practices were examined to determine the variables that influence each of these linkages. This achieved a number of objectives: firstly, to establish the gaps evident within each of these dimensions; and secondly, to provide guidance in identifying components that can be used to strengthen each of these linkages. It emerged that education is inevitably the solution when attempting to strengthen each of the linkages, as these dimensions all have some form of human involvement. Education in each of these linkages will result in a more cohesive bond between each of the dimensions, consequently resulting in a holistic anti-phishing framework.

The previous chapter identified the factors that are required to strengthen the linkages between the dimensions. The objective of this chapter is to discuss the *educational components* needed in each linkage to address such factors. The next section begins by discussing the need for security awareness, training and education. Human behaviour and some methods for changing it are briefly examined. Section 6.5 describes the educational components needed to address each of the respective linkages with the aim of safeguarding against phishing attacks. In section 6.6, the framework is evaluated by three organisations using an interview technique and the interview findings are discussed in section 6.7.

6.2 The Need for Security Awareness, Training and Education

Chapter 3 discussed the fact that human factors pose security risks to organisations. As mentioned, many of the problems experienced in the protection of information can be directly attributed to the involvement of humans in the process (Van Niekerk & Von Solms, 2008). Payne (2003) states that statistics have proven that the majority of security breaches affecting organisations are caused by insiders (i.e.

employees), as opposed to external threats such as hackers. A popular misconception is that these insider breaches are caused by disgruntled employees. Instead, Payne (2003) points out that individuals cause these breaches for the following reasons:

- Users are not aware of security threats.
- Users incorrectly rely on someone else to deal with security threats, for example IT personnel.
- Users are not adequately skilled in addressing threats.
- Users feel that they have more important things to do, for example their work tasks.

In the above list, the acts are not committed intentionally by insiders. However, phishers will exploit these opportunities without hesitation. Therefore, user education emerges as the solution to address these concerns. However, as pointed out by Payne (2003), this becomes more complicated when

- users do not acknowledge that it is their personal responsibility to ensure security
- users consider security too technically complex for them to understand
- top-level and middle management fail to comprehend the importance of information security and the threat that the related risks poses to the organisation
- security budgets and staff are not utilised correctly.

From the factors described above, a number of concerns emerge. Humans have a negative attitude towards accepting personal responsibility for ensuring information security. Furthermore, they are not adequately educated to deal with security threats. Consequently, they develop attitudes from the preconceived ideas that security is a technical concern and is thus the responsibility of technical staff, which then influences their behaviour. This is one of the reasons why in this study and in many others humans are referred to as the weakest link (Mitnick & Simon, 2002, p. 3). To address this concern, some organisations implement security awareness training

and education programmes aimed at changing employee behaviour. It has been proven that motivated and educated users are the best defence against any unwanted security threat (Thomson & Von Solms, 1998). Unfortunately, information security education is often neglected as a top priority by organisations in favour of the implementation of technological controls (Nosworthy, 2000). This is concerning, considering that one internationally accepted code of practice, namely, ISO/IEC 27002 (2005), emphasises the importance of information security education. NIST 800-16 (1998) emphasises that organisations cannot protect the confidentiality, integrity and availability of information without ensuring that employees understand their roles and responsibilities. Accordingly, the effectiveness of information security is becoming more dependent on the vigilance of its users. As such, it is important for every employee in the organisation who works on a computer to be educated about information security (ISO/IEC 27002, 2005, p. 25).

This section emphasised that human behaviour is a security risk to organisations. In this study, humans have either a direct or an indirect involvement with each of the processes in the HOT linkages. Thus, it is imperative that this behaviour is addressed through security awareness, training and education. This section also revealed that organisations do not treat information security as a high priority. The organisation, particularly management itself, should also receive education, as it must support information security and be made aware of the risks. The greatest influences stemming from human factors are the attitudes, behaviour, motivation, commitment, habits and norms of people. Unfortunately, very little is known about why users choose to engage in unsafe security behaviour (Aytes & Connolly, 2004). In this study, the human factor attributes that will receive the most attention are attitudes and behaviour. Therefore, the educational principles affecting attitudes and behaviour also need to be understood before an educational programme can be implemented. The following section aims to clarify and support this.

6.3 Human Behaviour and How It Can Be Changed

Earlier chapters pointed out that if human behaviour could be better understood, one could suitably address why humans fall victim to phishing emails (Beznosov & Beznosova, 2007; Downs et al., 2007). According to Lacey (2009, p. 252), changing behaviour is much harder than changing attitudes. The literature supports the view

that to improve human behaviour in information security requires security awareness, training and education. However, what if the education programme itself needs improving? Van Niekerk and Von Solms (2004a) point out that user education programmes do not focus enough attention on behavioural theories. Furthermore, they state that many educational programmes directed at users have been created by security professionals who do not necessarily have a background in education. As such, in their study Van Niekerk and Von Solms (2008) further deliberated on how the educational approach could be improved. They firmly believe that applying pedagogical principles, such as Bloom's taxonomy, can assist trainers in correctly measuring the needs and requirements of their target audience. In this regard, the concerning factor is that educational programmes are not designed properly.

On the other hand, Leach (2003) states that three key factors are necessary to improve user behaviour in information security. These factors are the following:

- The behaviour demonstrated by senior management and colleagues
- The user's security common sense and decision-making skills
- The strength of the user's psychological contract with the company.

The human factors described above have a great influence on the organisation itself. Furthermore, Lacey (2009) points out the social factors that also influence behaviour. To elaborate, Lacey (2009) uses the example of the way group norms can influence user password behaviour. When users share their passwords with their colleagues, it can be considered as a sign of trust, while refusing to share a password could be seen as a sign of mistrust. Lacey (2009, p. 253) further reveals the following ten factors that most influence people's attitudes and behaviour:

- "Stories that they read, and games that they play;
- Their perceived organisational role;
- The influence and authority of their management;
- Accepted corporate rules and procedures;
- The nature of the local office or cyberspace environment;
- The actions of their immediate colleagues;
- The cues and controls in the systems they use;

- The personal consequences of their actions;
- Things that are personal, immediate and certain;
- Their most recent experiences."

Thomson and Von Solms (1998) believe that, in order to change the ideas and behaviour of users in an organisation, the organisation would have to undertake an information security awareness programme that has aims to change the information security culture of its audience. They further suggest that the security awareness programme should apply different psychological principles in order to change the user behaviour (Thomson & Von Solms, 1998). They focus on three methods which aim to affect user's behaviour. These methods are the following:

- "Directly changing their behaviour (ignoring attitudes and knowledge);
- Using a change in behaviour to influence a person's attitude;
- Changing a person's attitude through persuasion."

To make the above-mentioned methods possible, the practice of information security has to be incorporated into the daily activities of employees. Thomson and Von Solms (1998) recommend that this should affect human behaviour to the extent that it becomes second nature or subconscious to users. Thomson et al. (2006) call this "unconscious competent"; this is a term used to describe the state where people start to perform tasks automatically without needing to think consciously about them.

Thomson and Von Solms (1998) discuss a variety of techniques that can be applied to accomplish the above-mentioned goals. To change the behaviour of users directly, Thomson and Von Solms (1998) recommend using the technique of operant learning. This refers to a situation where there is a relationship between a response and its consequence. They elaborate that if a person's behaviour is correct, then they are praised, and if their behaviour is incorrect they are reprimanded (Haber & Runyon, 1986, p. 73). In explaining how this technique can be applied, Thomson and Von Solms (1998) describe that in security awareness, training and education programmes, employees can be rewarded with small tokens for showing the desired behaviour. They add that these tokens should not be of any great monetary value, but rather the goal should be that they are earned. Thomson and Von Solms (1998)

also recommend that when employees are awarded these tokens, it should be clearly visible to the other employees so that they can be motivated to also earn such tokens. Motivation is a key concept when teaching learners about information security and it is often not taken seriously enough (Siponen, 2000). If employees identify the benefits of receiving security awareness training and education, they will be more willing to participate. The use of incentives is one of the factors considered by agency theory and is therefore recommended in this study.

This section highlighted the fact that educational programmes need to be understood in more detail before they are implemented. Accordingly, it is recommended that trainers have knowledge of effective educational principles before implementing educational programmes (Van Niekerk & Von Solms, 2008). It then further pointed out that user behaviour is also influenced by the behaviour demonstrated by management. This indicates that management also requires a change of behaviour as its influence has an effect on the entire organisation. If the educational programme does not consider behavioural aspects, it may not be effective enough in changing human attitudes and behaviour. Consequently, the section further explored the psychological methods suggested by Thomson and Von Solms (1998), which were used to change employee behaviour. In this study, these attitudes and behaviours are primarily focused on three main areas, using technology correctly, following organisational policies and procedures, and management's support of information security. As pointed out in section 3.4.1, Van Niekerk (2005) states that information security depends on both human knowledge and human cooperation.

According to Nosworthy (2000) a change in user's attitude automatically leads to a change in their behaviour (Nosworthy, 2000). In this regard, the human–organisation linkage will have the greatest influence in achieving this result. Changing an employee's attitude is important if the employee is expected to treat phishing threats seriously in an organisation. This can only be made possible through an information security educational programme that covers all content related to each of the linkages.

The next section will discuss security awareness, training and education programmes and their attributes. These programmes are used to deliver educational

content to members of organisations with the aim of educating them on each of the linkages. These educational programmes aim to change user attitudes and behaviour in terms of security in the organisation.

6.4 Information Security Awareness, Training and Education Programmes

Chapter 3 categorised and described various controls that organisations commonly apply to protect themselves against general information security threats. The literature points out that technological controls alone are inadequate to protect against security threats, especially phishing. This is largely due to the human behavioural aspects that affect technology use. Furthermore, organisational policies and procedures are another control measure that is affected by human attitudes and behaviour. As a result, a security awareness, training and education programme is one method that can be used to address the human aspect. Security awareness, training and education can help change users' mindsets and behaviour towards information security thereby making them a more effective security defence in an organisation (Johnson, 2006). In doing so, the number of security incidents can be reduced (Hight, 2005).

NIST 800-16 (1998) describes the process of information security education as a continuum. This continuum is fairly widely accepted and consists of awareness, training and education (Schlienger & Teufel, 2003; Van Niekerk & Von Solms, 2004b). This continuum is necessary for the successful implementation of any information security programme (NIST 800-50, 2003). Learning in the continuum begins with awareness, develops into training, and finally evolves into education (NIST 800-16, 1998, p. 14). Furthermore, the role each individual plays in an organisation determines and defines the IT security learning needed by that individual (NIST 800-16, 1998, p. 14). According to NIST 800-16 (1998), the purpose of information security awareness, training and education is to enhance security by

- improving awareness of the need to protect system resources
- developing skills and knowledge so computer users can perform their jobs more securely

- building in-depth knowledge, as needed, to design, implement or operate security programmes for organisations and systems.

The literature often conflates the terms ‘security education’, ‘training’ and ‘awareness’ into a single meaning. As a result, it is difficult to delineate the differences between them. However, some literature clarifies each of these areas. Accordingly, the following subsections aim to categorise and discuss these three levels of learning in more detail. They also attempt to point out how organisations deliver educational content to all their employees on each of these levels. The next subsection begins with the awareness level.

6.4.1 Awareness

NIST 800-16 (1998) states that awareness programmes are not training programmes. Accordingly, they are less formal and a presentation or briefing is often used to deliver content. Awareness programmes are an effective way of conveying education and the objective of such programmes is to make people pay attention to certain information (NIST 800-16, 1998, p. 15). Awareness programmes are made effective when media such as television advertisements and documentaries are used. Similarly, security awareness campaigns in organisations often make use of tools such as posters, websites, videos and promotional slogans.

According to Weippl and Klemen (2005), awareness is a much underappreciated step toward protecting IT systems. This is astounding, considering that it is regarded as the most cost-effective information security control an organisation can implement (Van Niekerk & Von Solms, 2002). According to Siponen (2000), security awareness is “a state where users in an organisation are aware, ideally committed to, of their security mission”. NIST 800-16 (1998, p. 5) considers awareness programmes as a prerequisite for information security training. Such programmes are usually short term, specific and immediate (NIST 800-16, 1998, p. 15). Furthermore, NIST 800-16 (1998) states that awareness programmes should be motivational, ongoing and creative, thus enhancing the learner’s attention so that learning will be incorporated into conscious decision making.

Awareness programmes are required for all employees and comprise a learning process focused on allowing individuals to recognise security concerns and to respond accordingly (NIST 800-16, 1998). Awareness programmes are intended to educate users on information security issues and also to continually remind users of the issues and any new pertinent issues involved (Thomson & Von Solms, 1998). In this study, the latter point is important especially as phishers constantly seek new technologies and techniques to lure their victims, for example social networking sites and mobile phones. Such programmes should instil a sense of responsibility and purpose in employees who handle and manage organisational information (Whitman & Mattord, 2004). They should also point out to users the role they play in the protection of the organisation's information and teach them to recognise the importance of information security (NIST). According to the Australian National Audit Office audit report (2009), security awareness programmes should be designed to

- promote the need for security and provide individuals with an understanding of their security responsibilities
- maximise individuals' contribution to the organisation's protective security practices, including increasing adherence to security policies and controls
- explain the potential implications of security breaches, including the costs of the compromise or loss of assets and information.

In meeting the above requirements, it must be ensured that individuals' attitudes and perceptions towards security are changed. If this is achieved, individuals will comply with organisational policies and procedures, security practices and so on. Johnson (2006) points out the benefits of security awareness programmes as follows:

- Improved protection of the confidentiality, reliability and correctness of the organisation's information
- Increased confidence of employees, suppliers, customers and shareholders in the organisation's security, thus improving employee morale and increasing productivity
- Earlier detection of security incidents; as a result, there will be fewer internal incidents, errors and omissions.

6.4.2 Training

Van Niekerk and Von Solms (2008) distinguish the differences between training and awareness in the following statement: “training seeks to teach a person skill’s in order to perform a specific function, while awareness seeks to focus an individual’s attention on an issue or set of issues.” Training is focused on providing relevant knowledge, security skills and abilities specific to individuals’ roles and responsibilities in the organisation. As such, training is more formal than awareness programmes (Van Niekerk & Von Solms, 2008). Training requires learners to take an active role when being taught (ISO/IEC 27002, 2005, p. 25). In terms of this approach, learners can be more equipped to deal practically with security threats. The aim of training is to improve employees’ job performance. Security training is typically technical in nature and, as such, is directed mostly at security staff and IT staff who have security-related responsibilities. Technology and systems are constantly changing and evolving in unanticipated ways (Bishop, 2000). As a result, the need to regularly educate end-users in technology has increased. Depending on the skill requirements needed by individuals, training content can be classified into different levels, such as beginner, intermediate and advanced.

In the context of information security training, the learner must be trained in how to behave securely in an organisation. Bishop (2000) points out training can be in the form of tutorials, which are hands-on and intensive. The benefit of tutorials is that learners can directly apply what they have learnt to their daily tasks. Another benefit of tutorials pointed out by Bishop is that learners will possess the material used in the training, for example, books and slides. This is useful, as learners may not be able to retain everything which is taught during their tutorials. They can then refer to the materials at any given stage, and remember some information (perhaps from the visuals) to refresh their memory. Training can also be done spontaneously at the workplace. For this to be possible, an employee would need a mentor in the workplace who is willing to answer any questions. For example, a trainee can be shown how the systems are configured and reconfigured (Bishop, 2000). Bishop adds that this technique is typically slow; however, it is effective because it educates the employee on problems that are specifically related to the organisation or the

system. Bishop (2000) further adds that this approach is also effective when combined with a general tutorial.

6.4.3 Education

In section 4.4.2.1, it was indicated that Van der Merwe et al. (2005a) state that there are five issues that have to be addressed in order to combat phishing, namely, education, preparation, avoidance, intervention and treatment. Robila and Ragucci (2006) believe that, within these groupings, education is given the least attention. Employees have unique backgrounds, age, strengths and skill sets. As such, they have different levels of understanding (NIST 800-16, 1998, p. 5). To address the latter, organisations usually provide further education to their staff through some training or awareness programmes. This is because education is often the only method to convince employees and managers of the need to do things differently (Schein, 1999, p. 120).

Education can be considered an advanced form of training as it integrates all the skills attained from training and awareness in a common body of knowledge (NIST 800-16, 1998, p. 16; Van Niekerk & Von Solms, 2008). Employees must understand, through knowledge, why information security is important for the organisation (Schlienger & Teufel, 2003). To accomplish this, educational material should ideally be tailored to the learning needs and styles of individual learners (NIST 800-16, 1998, p. 19; Van Niekerk & Von Solms, 2004a). It is important for the trainer to recognise the different methods by which individuals learn and memorise content (Danchev, 2003). Some people learn by reading material, while others might learn better by being presented with study material or other education approaches. Therefore, a variety of activities should be used in the education process (Danchev, 2003). Diagrams, pictures and even cartoons can be effective ways to gain the interest and participation of members. Cartoons, especially humorous ones, can be effective as members will remember a funny situation representing a more serious procedure (Danchev, 2003). However, caution should be exercised when using this approach, as one does not want members to treat the training as a comedy show. According to Danchev (2003), it has been proven that using this approach has a positive outcome in employees' understanding of content. As a result, this would

appeal to the diverse learning styles important for effective education involving adults (NIST 800-16, 1998, p. 20).

Literature describes many educational learning/teaching models that should be considered when developing an information security educational programme. Five well-known learning models include objectivism, constructivism, collaborativism, cognitive information processing and socio-culturalism and the consideration of these models can help to produce an effective educational programme. In Monk's (2011) study, he examined and discussed each of these learning models in the context of information security education. Monk (2011) concluded that each of these learning models presents problems when used to formulate an information security educational programme. Therefore these specific five learning models will not be considered although some of their principles have been integrated in the educational programme.

This section distinguished differences between levels of awareness, training and education, despite some researchers using these terms interchangeably. This section also helped establish how these educational programmes are operated and delivered. Education is the end-product of effective security awareness and training programmes. Ultimately, all employees need to be educated as 'education' is the entire process a learner undergoes to obtain the information they need to become knowledgeable of the concepts of information security (Monk, 2011). Educational principles influence the way awareness and training programmes are carried out and it is also important for security awareness and training programmes to be monitored and evaluated during and after their delivery.

Before implementing an educational programme, it is important for organisations to recognise their employees' background, specifically their strengths and weaknesses, as well as their learning styles. Learning styles that support visual learners, auditory learners and tactile learners can have an influence on how the educational content is received. For example, a computer technician can be taught verbally or can be taught while physically operating a computer terminal. If organisations understand their employees, problems or potential problems can be identified and remedied through some form of education, as such an understanding will determine the

training requirements. This includes identifying whether employees need to have their skills further improved or developed in order to perform their tasks or new tasks correctly. It is also important that learners are motivated during and after training.

By analysing the way information security educational programmes are delivered, a set of criteria can be created that could enhance the chances of a successful education programme (Monk, 2011). This is also necessary to define the knowledge and skills needed by various individual groups in the organisation. As such, the next section discusses components for each of the HT, HO and OT linkages.

6.5 Educational Components Required to Strengthen Each Linkage

This section will introduce the educational components (between HT, HO and OT) of a holistic anti-phishing framework. The previous section distinguished the principles of awareness, training and education. These principles will be integrated and used in delivering the educational content required to strengthen each of the subsequent linkages. Earlier chapters introduced the specific HOT controls needed to combat phishing threats. However, these controls were mostly used in isolation of one another. Therefore, theories and best practices studied in the previous chapter further helped to identify the major components needed to address possible gaps in phishing defences.

Furthermore, components from ISO/IEC 27002 (2005) were studied and taken into account. There are an overwhelming number of components that can generally address information security in each of these linkages; however, in this study components are limited to addressing phishing only. The National Institute of Standards and Technology (NIST) document specifies the way learners should be educated on information security (NIST 800-16, 1998). Many information security education programmes are designed in accordance with specifications taken from NIST 800-16. In line with this, the components in this document were studied to determine how content can be suitably delivered to the relevant audience. The educational components required for each of the linkages were evaluated by three organisations. The findings of the evaluations are later discussed in section 6.7.

It should be noted that, for the rest of this section, ‘users’ and ‘employees’ refer to any person who could benefit from gaining knowledge from education on each of the linkages. The term ‘users’ should not be confused specifically with end-users of computer systems, but rather refers to the staff involved at all levels of the organisation, including senior management, who are to receive training. It is noted that literature does indeed describe content that should be taught to users to help identify phishing attacks; however, in this regard it does not describe how to deliver the educational content effectively (Robila & Ragucci, 2006). This section aims to provide further guidance in this regard. The following subsections classify the educational components according to the three main linkages under discussion, which helps to structure the educational components more logically. Aligning these three linkages will help reduce the gap that allows phishing to proliferate through the other linkages. The next subsection begins by discussing the educational components needed to address the HT linkage in phishing.

6.5.1 Human-Technology Linkage

Previous chapters discussed the fact that organisations and end-users apply a great deal of attention to the implementation and use of technological controls to combat general information security threats. Predictably, this approach has been expanded to combat phishing attacks. Security-related educational programmes focus much attention on training users in the use (i.e. functions and features) of technology and neglecting, to some degree, whether users actually find the technology easy to use; for example using a web browser to help the user identify spoofed websites. Chapter 2 pointed out that people are misusing technology and information and that this trend is having a negative effect in that people are beginning to believe that this is acceptable. As a result, a change in user attitudes and behaviour is absolutely imperative and, to some extent, the goal of this study.

Despite the large number of technological tools available to fight phishing, it is clear that current practice in the use of these controls is inadequate because these technological controls are managed by individuals, who if not trained may leave the system open to attack. Furthermore, the technological controls themselves can also possess software vulnerabilities that phishers may exploit. To further add to this

complexity, technology is constantly changing and, as such, users need to be frequently educated on these changes. It may be argued that victims' lack of understanding in the use of such technologies is what exposes them to phishing attacks the most. Therefore, education should aim to enhance users' understanding of what the threat of phishing entails and also the most efficient ways in which technology can be used to combat this threat.

This subsection describes the components needed in this linkage to educate users with an emphasis on using these technologies correctly. The overall objective of this linkage is to ensure technology and its security controls are experienced by all users as being useful and as easy to use as possible. This supports the objectives of the TAM described earlier. This objective can be accomplished using a training programme.

PHASE	OBJECTIVES
Phase 1: Introduction to information security and security threats	• To give users knowledge of the dangers security threat agents present for organisational assets. • To distinguish between different types of security threat agents. • To identify phishing emails and spoofed websites.
Phase 2: Technological controls used to combat phishing attacks	• To give users the skills required to use technological tools correctly to combat phishing attacks.

Table 6.1: Using a phased approach for information security training

The content of such training programmes may differ, depending on the specific types of software (application and system software) organisations use. The training of individuals, especially in information security and supporting technologies can be a

complex task given their diverse backgrounds. If organisations have the time and resources, they can use a phased approach to their HT training. For example, they could classify their training programme into two phases. Table 6.1 gives an example of this approach. Phase 2 is of key importance here, as it specifically addresses phishing. Appendix A outlines the components of these two phases in more detail. To reduce costs and resources, the organisation can provide on-site training. In this particular training, the training environment should include sufficient computers, Internet availability and software relevant to the training. If an external facilitator or institution is conducting the training, trainees should be evaluated and possibly receive some certification or recognition on successful completion of the respective training modules. Although this will cost the organisation money it will nevertheless encourage employees to take the training more seriously as they stand to receive benefits for their efforts. This supports Thomson and Von Solms's (1998) technique of operant learning described earlier. It is important that members are practically assessed after their training. If members are not successful in their assessment, the organisation should ideally make it compulsory for them to complete the training within a suitable time frame. It should be noted that education in this linkage focuses on components related only to phishing, in addition to factors that have an impact on phishing education. As such, this section will elaborate more on such components and less on others. The next subsection will discuss the foundational user training component necessary before information security training takes place.

6.5.1.1 Information Security Training

Before users receive any training in information security aspects, they first need to be taught the necessary skills and competency regarding computer systems (NIST 800-16, 1998, p. 16). Section 2.2 established the important role of IT in organisations: Today, most organisations use computers to manage their business activities and processes and, accordingly, in this digital age, users are expected to possess the skills needed to operate a computer correctly.

Nosworthy (2000, as cited by Van Niekerk & Von Solms, 2002) states that each and every employee in the organisation, from the CEO to the cleaning staff, must be aware of and trained to exercise their responsibilities towards information security.

The NIST 800-16 (1998) document is a good starting point to guide the development of information security programmes. However, there are some prerequisites before information security training can begin.

The employee's role in the organisation shall determine the training requirements needed by that individual. Accordingly, employees can be classified into three major groupings, namely, **top management**, **end-user staff** and **IT/technical staff**. This will create a comfortable environment for learners to participate in, thus supporting Thomson and Von Solms's (1998) technique of "conformity". The training programme should be tailored to address these specific groupings (Thomson & Von Solms, 1998). End-user staff members should be able to use the technological control features and functions of the email client, web browser and anti-virus program correctly from the user-level. IT/technical staff, however, will receive specialised training in the implementation and configuration of security controls and technologies on an organisational level in order to help protect the organisation against phishing attacks. The next section describes the components needed to address the education of each of these groups.

Monk (2011) states that information security is viewed by many, as a boring topic to study. Accordingly, participants firstly need to be motivated to increase participation and, if possible, some rewards can even be given out after successful completion. Thomson and Von Solms (1998) state that these rewards could be in the form of coffee mugs, paper weights, mouse pads and so on. Secondly, information security is a very broad and detailed subject and can focus on many specific areas (e.g. network security, application security). Therefore it should focus on, or at least address, aspects related to phishing.

The trainer, in the case of course presentation, should ideally be a qualified expert in information security. If not, the audience may not accept or be convinced by the trainer's arguments (Thomson & Von Solms, 1998). The trainer should ideally possess certification, such as a Certified Information Systems Security Manager (CISSP) appropriate for this type of training. It should be conveyed to all trainees what the programme aims to accomplish and how vital education is for the survival of the organisation (Danchev, 2003). Since each employee has a different role to play

in the organisation, end-users may not be familiar with all the technical terms. The following paragraph begins with information security training for end-users.

End-user Training

According to Hight (2005), end-users have access to the most vital information an organisation possesses. Accordingly, depending on their knowledge and behaviour, they could potentially put the organisation at risk. Phishing is not limited to any type of user and targets any human behaviour regardless of status or position; thus, this type of training can include top management, depending on whether the organisation sees fit to do so. Training end-user staff can be challenging because such staff believe it is the responsibility of security personnel to protect the organisation against security threats. Therefore the training should consist of a number of short sessions designed to introduce the user to the various security aspects that need to be addressed in their daily routine (Thomson & Von Solms, 1998). Training of special security tools or features in applications should be offered by the organisation (NIST 800-16, 1998, p. 16; Schlienger & Teufel, 2003) and, to this end, end-users need to be trained in the following security features and applications which are specifically needed to combat phishing.

File Types

Users should be familiar with the different file types of computer systems, as well as their corresponding file extensions. In emails, there is a wide variety of attachments that contain different file types such as images, presentations, zip files, documents, pdf files and video. These different file types could cause confusion in users, potentially creating an opportunity for phishers. To elaborate, if users do not recognise these different file types then phishers could use this opportunity to attach a virus to an email. Viruses attached to emails can be created by phishers who aim to capture keyboard strokes and/or obtain screenshots of the victim's activities on the computer system. For example, it is common for executable programs attached to emails to contain viruses in a zip file. Users then identify the contents of the zip file only after it has been 'unzipped'. Microsoft Word documents can contain a special type of virus known as a macro virus. These viruses are sent by phishers with the intention of stealing passwords and monitoring keystrokes and online activity. The

passwords can then be used by the phisher to gain entry to any financial websites used by the victim. Another problem is that, by default, Microsoft Windows XP and Windows 7 operating systems do not have their file type extensions visible by default. Therefore, users cannot distinguish file types easily unless they are trained in how to view their properties. Thus users should be trained to uncheck the hidden file extension settings of the operating system.

Security Threats

Thomson and Von Solms (1998) and NIST 800-16 (1998) motivate the use of role-playing exercises. Since security threats are a technical subject, in helping members to understand security threats the trainer can act out the activities of threats in role-playing exercises. This can inspire humour among members, thus increasing participation. In the context of this study, particular attention and detail must be given to social engineers and phishers as the main security threat agent.

System Warning Alerts

In Chapter 4, the literature highlighted the fact that users often ignore or lack understanding of web browser warning alerts. These browser alerts warn users that they may be entering a website which has been identified as malicious, for example a spoofed website. Similarly, the operating system and application software generate alerts and require the involvement of users; for example, update now, submit, cancel, and continue. Therefore if users can understand *operating system alerts* they may be able to transfer this knowledge to understanding the alerts originating from other software applications such as the web browser as well.

Users should also understand that computer systems can request users to update the software, notably for the operating system and application software. Section 4.2.3 illustrated the fact that phishers can entice victims to update their software through hyperlinks in emails. As a result, if users have knowledge of software updates, they will recognise that this process is illegitimate; as such updates should not originate from these hyperlinks provided in emails.

Logging Off and Locking Computer Terminals

In times of absence users should be able to log off and lock their computer terminal using a password. This is to safeguard against social engineers who may be in the vicinity in the event of physical access control being compromised. If a computer terminal or information is stolen, it can be used by the social engineer for improper or illegal purposes. Users should also be taught to encrypt the information stored on their computer devices and need to practise this security behaviour until it becomes a habit. This specific best practice can be enhanced through ongoing awareness created by the organisation.

Anti-malware Software

Users must be educated in the correct use of anti-malware programs. It is important for users to understand that anti-malware programs must have their virus signatures/ definitions updated regularly (i.e. every day or hour) in order for it to be effective against the latest threats. Most anti-malware programs are packaged so as to be updated automatically. Chapter 4 established that phishers can disguise email attachments to contain a Trojan in order to capture passwords from their victims. As such, using the anti-virus program users can scan storage devices (e.g. flash disks) and attachments contained in emails. Users should practise saving email attachments to their local system directory so that the anti-malware program is given an opportunity to inspect the file for viruses or other malicious content (Ollmann, 2008). Modern anti-malware programs have built-in phishing detection which is able to detect phishing emails and spoofed websites.

Email Client

Wacaser and Mazzeo (2007) cite a 2005 survey conducted by the American Management Association. The results of the survey indicated that 26% of employers have terminated their employees for inappropriate use of email in the workplace. Lack of understanding in the use of the email client is an area that phishers tend to exploit. Section 4.2.2 described the characteristics of phishing attacks, specifically in the way that they are methodically carried out. Trainees therefore need to be educated in this regard. Special attention should be paid to technical details, such as email address structure, the hyperlink structure contained in the email, social

engineering techniques (the bait) used by the phisher and file attachment type. This will help users to correctly identify and distinguish phishing emails from legitimate emails.

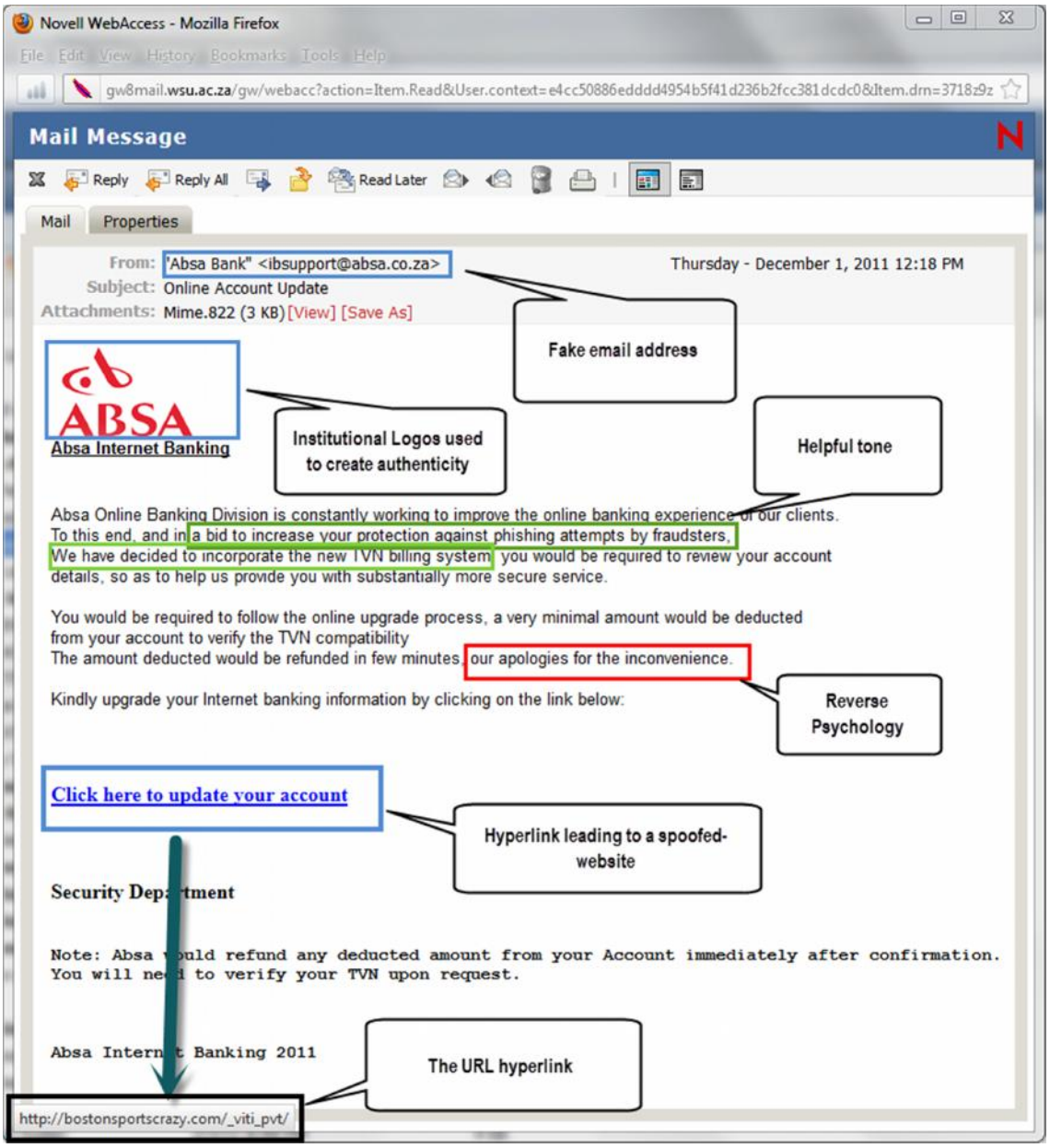


Figure 6.1: Educating users on the characteristics of a phishing email

Actual real-world examples of phishing emails must be made available to users instead of mere discussion. Figure 6.1 gives an example of how this can be carried

out. Sections to pay attention to in phishing emails can be highlighted for users in this manner. The email client's function of block/mark as spam can be used to prevent further phishing emails from the particular source. Users may also choose to select a number of other options such as trust sender, junk mail and block sender. Most importantly they should not respond to the email – just delete it.

Web Browsers

According to Ollmann (2008), web browsers may be the most technically sophisticated software applications that employees use. Wadlow and Gorelik (2009) believe that many security concerns relate to the user of the browser. This emphasises the importance of users being well trained in web browser use. Furthermore, using real-world examples users should be educated to distinguish between spoofed websites and legitimate websites. Training should therefore focus on the use of technical features and indicators on web browsers and web pages, such as SSL icon and URL structure. Users must understand that before submitting sensitive information on a web page, they should note the 'padlock' icon on the web browser's status bar and *not* on the web page area. The padlock icon indicates that the website is safe and secure (i.e. encrypted) in terms of transmitting confidential information.

Another indication that the website is in a secure state is if the web address begins with "https" instead of "http". Web browsers also alert users by displaying warnings indicating that they are either using an encrypted webpage or not. Most web browsers warn users if they are in an unsafe, malicious or suspicious website. Some spoofed websites may indicate that they are secure, using a phony padlock icon. Therefore, for added security, users should be trained to view the security certificate of that particular website in order to determine if it has been issued by a trusted certificate authority and that it is valid (Ollmann, 2008).

Ten Phishing Best Practices

Information security training for end-users can be concluded by highlighting the following ten phishing educational best practices. It is important for members to understand and remember these guidelines.

1. **Do not trust strangers**: This is one of the most important life rules one was taught as a child. To be safeguarded from threats we were educated from an early age not to talk to or trust strangers. The same rule applies when receiving emails, instant messages, text messages or phone calls from individuals you do not know. The argument that these technologies do not provide face-to-face communication does not excuse ignorance of this rule. Be more suspicious of anyone contacting you unexpectedly to request personal information. Even if this person may sound legitimate and trustworthy be wary as it may be a social engineer. Organisations and financial institutions do not operate in this manner. This includes a department within the victim's place of work.
2. **Scrutinise the contents of the email message:** Firstly, if you are not the customer of the organisation being imitated in the email, then delete it or block the sender. Legitimate emails should address one by their name not as a generic 'Dear Customer'. Typically, phishing emails do not refer directly to the person by name. Check for spelling mistakes or missing words. If any offer or story seems too good to be true, it most likely is. Users must also not be tempted by any cause or plea that preys on human emotions. For example, people who are suffering from an illness or dreaded disease requiring funding for assistance. These are email scams; use the email client features to report it as spam mail.
3. **Do not respond to emails that are in HTML format with embedded submission forms.** Any information submitted via email, even if it is legitimate, will be sent in clear text and may be observed (Ollmann, 2008). Images embedded in emails can contain a virus code and potentially be links to spoofed websites. This process is known as click jacking (Shelly & Vermaat, 2011, p. 405).

4. **Do not download email attachments from unknown sources.** This is similar to the first point. Pay attention to the type of file that is attached (e.g. document or zip file), as attachments can contain viruses.
5. **Do not reply to, or click on, hyperlinks or images contained in emails**. Delete the email especially if it warns you, with little or no notice, that an account will be terminated unless one complies with demands. In this instance, look out for the 'bait', as it is used to lure victims to comply with the request. Therefore, do not fear the threat or warning.
6. **Use the keypad to manually type URLs of website,** instead of clicking on hyperlinks. This is because some web page addresses are disguised to look like the legitimate websites. In some cases, phishers make use of obfuscation techniques to hide the source code of the website. Making use of the email clients feature to 'bookmark' legitimate websites can help, so that one does not have to type the URL again.
7. **Do not submit any personal information** such as passwords and PINs via email, or telephonically, or on websites to any authority no matter how enticing or credible the story may seem**.** Instead, confirm the authenticity of the request by contacting the institution cited in the email using a contact number or website address you know to be genuine (not the one provided in the email). If it is necessary, email sensitive information to an individual one knows, encrypting the email so that it is secure during transmission. Also look out for the padlock icon in the web browser which indicates that the website is protected with encryption technologies (SSL) to securely transfer personal information. Also check whether the URL in the web browser address bar begins with 'https://', which also indicates that it is a secure webpage. If one believes that a webpage could be spoofed, type in a fake password. Usually a spoofed website will accept it and redirect you to a webpage stating that the website is experiencing technical difficulties. A legitimate banking website will not provide such an opportunity.
8. **Do not use identical usernames and/or passwords** for different websites. If one password is compromised by a phisher, they can then use it for other websites. Think of this like having a universal key that will unlock the doors to one's house, office and vehicle. Instead, use different passwords for each

website. If one's password has been compromised, change it immediately. Some organisations require that users change passwords regularly. A password should consist of at least eight characters with a combination of uppercase and lowercase letters, numerical and special characters (Shelly & Vermaat, 2011, p. 278). Avoid using single word passwords and words that are easy for a phisher to guess. For example, one's first name. Phishers can also make use of software known as 'brute force password cracker'. End-users often complain that they cannot remember all their passwords; therefore, make sure that one uses a method to remember these passwords. One can make use of Password Manager software to handle one's passwords safely. Do not write usernames and passwords on pieces of paper that are readily available to people in the office;

9. **Validate credit card and bank account statements** as soon as one receives them. This is to detect problems of unauthorised charges early on. If a statement is late by more than a couple of days, contact the financial institution as soon as possible to confirm billing, account and address particulars (Ollmann, 2008).
10. **Do not leave an unoccupied computer terminal logged in** on websites, especially a banking website. When exiting a website, users should log out correctly and not merely close the window.

The above-mentioned educational guidelines, mostly involving the use of technology, are concise and understandable (i.e. not too technical) and, if adhered to, can have a significant impact in the battle against phishing. The ten phishing guidelines should be taught to employees using real phishing examples to demonstrate each case in point. These guidelines can also be used to form part of an organisational awareness campaign. In this regard, the organisation can create security orientated posters, screen savers, email reminders and mouse pads and display them in offices to remind employees of them. After the training, it is important to measure the level of impact of end-users' information security awareness. This will help to improve the quality for future implementation of these programmes, as common mistakes and misunderstandings on the part of both employee and trainer can be identified. This can typically be achieved by conducting a survey. It is important that employees are

informed that their responses to the survey will be treated as confidential, in order to maximise their candour and honesty.

An example of a proposed information security training programme for end-users is attached in Appendix A. This programme is described in more detail and is tailored to phishing. At this stage, the end-user staff training is complete. Should users experience any challenges in using these technological controls, they should be assisted by IT personnel in the ICT department, for example. This is supported by Bishop's (2000) approach to providing on-site training to employees through a mentor. The next paragraph discusses training for IT/technical staff.

IT/Technical Training

The second target group for information security training consists of the technical staff. This includes network administrators, IT technicians, software developers and information security administrators, among others. When technical staff are appointed, they are expected to possess the skills and experience relevant to their job description. However, owing to the ever-changing nature of IT, they may need further training. According to Payne (2003), there are many specialised training materials and web resources available to support IT staff members. For example, the SANS Institute provides IT professionals, including system administrators, network administrators and auditors, with resources such as research reports, best practices, trends, online training and certification programmes.

There are many other training institutes that provide training and support for technical staff and the organisation can make use of these resources. It is recommended that a trainer qualified in network security (e.g. Cisco certification) conduct this type of training for technical staff. In addition, to reduce costs the organisation could select individuals (based on some criteria) for specialised training, instead of training everyone. These individuals could then transfer the skills gained from the training to the other technical staff in the organisation. This can be regarded as on-site training. Training should focus on technological vulnerabilities and the techniques phishers use to gain unauthorised access to information. If members understand these weaknesses, they can implement the controls necessary to reduce risk. Members should be trained in technical details relating to the implementation

and operation of the technological security controls. Special attention should be paid to the technical details of phisher attack methods and how they are carried out. Ollmann (2008) lists some phishing attack methods below:

- URL obfuscation attacks
- Preset session attacks
- Man-in-the-middle attacks
- Client-side vulnerability exploitation
- Cross-site scripting attacks
- Observing customer data.

Technical staff should be trained in the controls used to combat these methods. They should also be willing to assist other employees (at all levels of organisation) in the use of these controls. Technology changes frequently; therefore it is recommended that a strategy be implemented in terms of which technical staff receive training when necessary.

Both user groups previously mentioned require support from management. The next paragraph describes the training required by top management.

Top Management Training

As mentioned earlier, top management should receive the same type of training as end-users. However, the organisation will determine whether they would be trained together with the operational staff. Firstly, it is important for top management to support the idea of ensuring that information assets are adequately protected on an ongoing basis. As such, training should take place in such a way that it convinces management to take information security and phishing very seriously. Payne (2003) states that when information security is explained to top management in familiar business terms, it sheds its stigma of technical complexity. It is imperative that management understand security threats to the organisation, the risks posed by these threats, and what can be done to mitigate unacceptable risks (Payne, 2003). This support and commitment will then filter down to other members of the

organisation. The following components should be highlighted to management in training.

Importance of Information Security

The importance of securing information and the reasons why such information is sought after by threat agents should be emphasised in management training. In the literature, information is often cited as being an organisational asset. Hence, management needs to understand the value of information and their responsibility towards ensuring it is protected. The training can furthermore explain how phishing threats have affected high-profile organisations and their customers financially. Actual case studies should be included. Management should appreciate that even reputable organisations can fall victim to phishing despite their financial wellbeing and large resources.

After training is complete, management should be committed to ensuring that the organisation's assets are protected and that information security behaviour is taken very seriously. This will then positively affect the development and implementation of the organisational policies and procedures, phishing training programmes and technological controls aimed at information security and phishing.

This section pointed out that security training in the HT linkage can positively influence attitudes towards the correct use of technology. They were also educated in identifying phishing emails and spoofed websites using technology. After completion of training in this linkage, it should be clear to all parties that information security is everyone's responsibility. According to Danchev (2003), a common problem in information security education programmes is that employees maintain that it is not their responsibility to improve the security of their organisation. They feel that security concerns are the responsibility of the IT department or the information security office (Danchev, 2003). Management and employees have a role to play and are only as strong as their weakest link. Employees should understand that lack of security systems for computers and networks, and a lack of concomitant knowledge in the use of these systems, gives phishers an opportunity to attack them. Employees must understand that these technological controls can be used as a shield to guard against phishing attacks. It is important that employees work correctly

and accurately at all times and to not overlook anything that looks suspicious. Users should be cognisant of the risks organisations face caused by their actions or lack of action if technology is not applied and used correctly and which should be documented in an information security policy. Identifying and safeguarding against threats is dependent on the knowledge and skills developed from training. Therefore users should see that the training they acquire benefits them personally as well as the organisation. It is challenging to have employees repeatedly attend information security training events especially if the same content is used in the training. Motivation and creativity will have a major influence in this regard. The latter relies on aspects described in the HO linkage. The organisation will have to determine a strategy to ensure its members participate and, most importantly, understand the training. The next section will focus on the educational components needed to strengthen the HO linkage.

6.5.2 Human-Organisation Linkage

The previous section discussed educating members of an organisation specifically on the use of technology associated with phishing, but also on the security of their computer system and information. Besides gaining knowledge in the use of these technologies, the aim was to influence attitudes technology in terms of being useful and easy to use, thus supporting the TAM objectives.

This section focuses on educational aspects of the organisation and how they govern information security in particular and its employees in general. This may seem to be irrelevant to phishing; however, it does have influence the prevention of phishing incidents. In section 5.5.1, agency theory posited that employees and the organisation often have conflicting needs. These conflicting needs may be a result of an employee's attitudes, behaviour or needs. As such, the link between the *human* and *organisational* (i.e. management) aspects requires strengthening and forms part of this linkage main objective. In this linkage, much attention is paid to the factors that affect user behaviour, specifically the changing of attitudes and behaviour to suit the organisation's needs. This is particularly important because phishers take advantage of ignorant or irresponsible human behaviour. For example, while at the organisation employees are supposed to be engaged in work-related activities, and not participating in social networking websites that create opportunities for phishers

to target them. If an employee's behaviour is not managed at the correct level, the organisation can be at risk of security threats, which most definitely include phishing.

ISO/IEC 27002 (2005, p. 23) classifies this linkage as human resources security. Similarly, COBIT 4.1 (2007, p. 55) describes it as IT human resources management. In comparing the principal and agent entities described in agency theory, the stakeholders affected in this linkage are the *organisation* and its *employees*. Top-level management and human resource management represent the organisational aspect and management is, typically, entrusted with formulating these policies. The 'employee' aspect consists of all other staff on whom organisational policies and procedures are imposed. The following paragraph describes what needs to be done to ensure that organisational policies and procedures are drafted and complied with.

6.5.2.1 Organisational Policies and Procedures (including Information Security Policy)

Chapter 3 described the importance of organisational policies and procedures and why they are used to manage employee behaviour. One method organisations use to enforce information security is through policies and procedures. The drafting of policies and procedures is vital to such an extent that COBIT 4.1 (2007) and ISO/IEC 27002 (2005) regard this as core to the relationship between the organisation and its employees. Policies and procedures define the relationship between the organisation (i.e. management) and its employees. More importantly, these policies and procedures dictate employee behaviour in the organisation (Mitnick & Simon, 2002; Ohaya, 2006). For a change in behaviour to take place, employees need to firstly be made thoroughly aware of policies and procedures. Merely signing that policies have been read does not change human behaviour. Contractors and third-party users should also receive appropriate security awareness training as well as regular updates in organisational policies and procedures, as are relevant for their job function (ISO/IEC 27002, p. 26, 2005). If this is done, there will be fewer opportunities for phishers to exploit human behaviour.

Herath and Rao (2009) point out that research and field surveys suggest that employees seldom conform to information security procedures. Unfortunately, information security policies are not taken seriously enough because they are seen

as mere guidelines or general directions to follow rather than actual rules (Herath & Rao, 2009). As a result, research in information security behaviour has started focusing on employees' intentions to conform to security policies. It has been revealed that even in cases where users have knowledge of a specific security policy, they may still deliberately ignore it because they do not understand *why* it is needed (Schlienger & Teufel, 2003). Furthermore, organisations do not put more resources into educating their employees in policies and procedures. Instead, the traditional approach used by organisations is to merely inform their employees that they have policies and that they should be obeyed or else they will face disciplinary action. According to Siponen (2000), this approach is not likely to increase employee motivation or improve attitudes. This will consequently put the organisation at risk as users will not necessarily behave securely in the organisation (Van Niekerk, 2005). This is highlighted by agency theory which describes the conflicting relationship between the organisation and its employees. Seen in the light of agency theory, it may be more sustainable to help employees understand how their actions in protecting information assets will empower them, instead of just making them follow orders (Du Plessis & Von Solms, 2002).

Awareness and training relating to the organisation's policies and procedures must be carried out before user access and services are granted (ISO/IEC 27002, p. 26, 2005). This can be done on appointment of employees, and then be continued on an ongoing basis. Furthermore, it should inform employees of known threats, who to contact for further security advice and the proper channels for reporting security incidents (ISO/IEC 27002, p. 26, 2005).

A security awareness programme must ensure that employees understand how their behaviour may endanger the information assets of the organisation and also how this can personally affect them. This requires employees to be educated in activities that are regarded acceptable and unacceptable by the organisation, details which can be outlined in organisations' security policy documents. Employees require training in the security threats and protection methods that were addressed in the information security training in the HT linkage. Once employees have been educated in this regard, they will understand the importance of policies and procedures and will therefore be positively influenced to abide by them.

To further enhance awareness of security policies and security threats, the organisation can place security posters conspicuously in offices and corridors. These posters will make employees aware of crucial points in policies, as well as well-known security threats. Thus, the opportunity is created for employees waiting for a meeting or having a tea break to read these posters. In this regard, awareness is used to continually remind people to comply with organisational policies. Employees should understand that it is their responsibility to acquire knowledge of the organisation's policies and procedures and they should not plead ignorance when accused of misconduct in this regard. Hence, employees should understand that the organisation can institute disciplinary proceedings if policies are not followed, regardless whether the misconduct was unintentional. This could be addressed by a general misconduct policy which further describes the procedures for the disciplinary process.

This subsection pointed out that, by educating employees on the purpose of security policies, employee attitudes, work ethic, knowledge and behaviour can be positively influenced. Motivation will play a vital role in ensuring that employees perform their tasks at an acceptable level. This statement is supported by ISO/IEC 27002, (2005, p. 26), which states that motivated personnel are likely to be more reliable and as a result will be less inclined to cause security incidents. However, there are other factors worth mentioning that also have an influence in strengthening the relationship between the organisation and its employees. ISO/IEC 27002 (2005, p. 23) terms these factors human resources security. These factors are generally targeted at recruiting trustworthy staff and shaping their behaviour towards the needs of the organisation. If these factors are not managed correctly, they can pose security risks to the organisation. These factors include the following:

- **Recruitment of new staff members –** interviews, background security checks/screening, employing suitable candidates that are qualified and/or experienced
- **Job descriptions –** integrating information security into job descriptions. Employees will then recognise that it is their responsibility to ensure

information security. Clearly defined roles can have a significant impact on people attitudes (Lacey, 2009);

- **Skilled staff –** it is important to have staff have the skills needed for their job responsibilities. If staff members are not adequately skilled for their tasks, they may pose security risks to the organisation. The Deloitte cyber security study revealed that a lack of skilled staff remains one of the top concerns for organisations (Deloitte, 2012)
- **Employment contract –** employees agree to binding organisational policies
- **Induction/orientation programmes –** extensive security briefings in policies, security procedures and access levels, training in the use of information systems
- **Fair compensation –** employees will feel that they are treated fairly if they receive adequate compensation (i.e. money) for their work (Lacey, 2009, p. 240). Incentives can also be used to reward employees for their work performance, as well as to motivate employees.
- **Monitoring and evaluation –** incorporating information security evaluation as part of job performance evaluation. Furthermore, monitoring Internet usage in order to protect the organisation's internal systems from threats (Danchev, 2003).
- **Termination or change of employment –** often referred to as an exit strategy, is the removal of employee access rights, including physical and logical access, keys, identification cards and information processing facilities. This includes the returning of assets supplied by the organisation. A formal disciplinary process for misconduct must be undertaken.

The manner in which these factors are implemented and managed can be described in organisational procedures. Poor management may result in employees feeling undervalued, thus having a negative impact on the organisation in terms of security (ISO/IEC 27002, 2005, p. 26,). For example, poor management may lead to security being neglected or the potential abuse of the organisation's assets. Ideally, if employees are motivated they will treat information security programmes differently, as they understand that the objective of having such programmes is to protect both them and the organisation. The survival of the organisation is dependent on its

employees support and vigilance toward organisation policies and procedures. If this does not happen, it can potentially put the organisation at risk. Employees should be mindful of the disciplinary action the organisation can take against them, should they fail to comply with policies. Accordingly, employees should also be educated in this regard.

COBIT 4.1 regards managing IT human resources as one of the factors necessary to ensure that the organisation has competent and trustworthy staff. As such, COBIT 4.1 points out that a motivated and competent staff complement should be acquired and maintained for the efficient creation and delivery of IT services to the organisation. This is achieved by following defined and agreed legal practices supporting recruitment and training, evaluating performance, and promoting and terminating service. Employee roles should correspond with skills by establishing a defined review process and creating job descriptions. Staff performance will have to be reviewed and the outcomes based on these reviews will determine whether staff requires further training to meet their job needs. Failure to achieve this can result in staff becoming demotivated, as a result of poorly defined roles and responsibilities. Furthermore, if staff is not trained they can pose security risks as they have not been made aware of security threats.

The next subsection discusses the components necessary to strengthen the organisational and technology (OT) linkage.

6.5.3 Organisation-Technology Linkage

In section 5.5.3, COBIT 4.1 was identified as a suitable best practice to manage aspects related to the organisation and technology. In this subsection, important components taken from COBIT 4.1 will be used to strengthen these two aspects.

COBIT 4.1 defines requirements for the control and security of sensitive data and therefore provides a reference framework. In addition, security awareness, training and education are needed to strengthen each of the linkages. In the COBIT 4.1 guidelines, there is no section explicitly dedicated to information security awareness and training; however, they do make specific reference to these in the following sections.

6.5.3.1 Communicate Management's Aims and Direction

Firstly, the organisation (i.e. management) should develop an organisational IT control framework and communicate policies. To accomplish this, management must approve and support an awareness programme to express its mission, service objectives and policies and procedures. Achieving this will ensure accurate and timely information on current and future IT services, the associated risks and the responsibilities of staff.

6.5.3.2 Ensuring Systems Security

The organisation's security should be managed at the highest appropriate organisational level. This is to ensure that security actions are aligned with business requirements (COBIT 4.1, 2007, p. 127). The IT security plan must be implemented in organisations' security policies and procedures, together with suitable investments in services, personnel, software and hardware.

The CEO should be informed of this process and the security policies and procedures should be communicated to all stakeholders. A management process is required to establish and maintain IT security roles and responsibilities, standards, policies and procedures. Therefore, management should ensure that technical staff is trained to implement up-to-date security patches and anti-virus solutions to protect the organisation's information systems and technology from malware (viruses, worms, spyware, spam, etc.) and phishing. The organisation should ensure that its security-related technology is protected from tampering and damage. Network security should be in place (e.g. firewalls, and intrusion detection systems) as this may be an entry point for phishing attacks. Security controls must be used to authorise access and control information that flows in and out of the organisational network. Furthermore, it should be assured that the organisation's data transactions are exchanged over trusted paths or media. Controls should be in place to provide authenticity of content, which is particularly important for customers who engage in online banking, which is a concern for phishing victims. The organisation should also ensure that it's critical information is withheld from unauthorised users (e.g. social engineers and phishers) and that measures are in place to protect and recover

information in the case of system failures, human error, disasters or deliberate attacks.

It should be noted that if employees are too restricted by security controls, employee productivity may be curtailed (Thomson, 2003). For the organisation to ensure that the requisite activities are carried out, the organisation should

- understand security requirements, vulnerabilities and phishing threats
- manage user identities and authorisations in a consistent manner
- assess its security levels regularly.

Section 4.3 pointed out that phishing has damaged the reputation of many reputable organisations. To prevent this, the organisation can measure its security levels by the number of security incidents affecting the public and themselves. This will include the monitoring and evaluation of internal controls.

6.5.3.3 Monitor and Evaluate Internal Controls

The organisation should ensure that the security controls it has in place to combat phishing attacks are monitored regularly by the relevant staff to ensure their effectiveness. The cyber security study by Deloitte (2012) revealed that only 8% of organisations (i.e. CISO) actually measure the value and effectiveness of their respective organisation's security activities. Any concerns should be reported to management for any further intervention.

6.5.3.4 Establish Regulatory Compliance

Compliance also plays a role in IT governance. This is supported by Brown and Yarberry Jnr (2009, p. 25), who state that "[r]egulatory compliance is one of the core governance disciplines". To ensure positive compliance and to reduce the risk of non-compliance with IT laws and regulations, an independent review process is necessary. Such as a process includes defining an audit charter, auditor independence, professional ethics and standards, planning, performance of audit work, and reporting of and following up on audit activities. To ensure compliance, the organisation should firstly identify IT-related legal and regulatory requirements, then

assess the impact of regulatory requirements and, finally, monitor and report on its compliance with regulatory requirements.

A popular compliance regulation is the Sarbanes-Oxley Act of 2002 (SOX). However, mere compliance with SOX regulations (i.e. passing section 404) does not imply that an organisation or IT department can now successfully manage its business correctly and that an optimal level of control exists (Brown & Yarberry Jnr, 2009, p. 25). Indeed, SOX compliance should be understood as a minimum standard only and not as the optimum (Brown & Yarberry Jnr, 2009, p. 25). An organisation will need to demonstrate its SOX compliance effectively and honestly. In this regard, COBIT 4.1 can be used as a starting point to meet this objective. A few typical steps towards SOX compliance, as identified by Brown and Yarberry Jnr (2009, p. 25), are listed below:

- **Identify an organisational framework**. Although legislation does not specifically require CobIT compliance, it is accepted by most organisations as a good starting point for objectives.
- **Develop a list of controls.** These controls are vital to the successful operation of IT and support the key requirements alluded to earlier.
- **Categorise the control list**. The controls can be divided into general controls, which are pervasive across all or most platforms and applications, and application controls.
- **Review control list with external auditor.** This is so as to avoid too many controls (some redundant) which can result in excessive costs. Controls should be tested and documented and, if found ineffective, remediated and then tested again.

This section discussed the components required to strengthen each of the respective linkages. To ensure that these components are understood by all users on different organisational levels, a security awareness, training and education programme is necessary. The HT linkage defined an information security training programme aimed at **training** end-user staff in the use of technological controls to combat phishing threats. It also presented ten important phishing guidelines that should be

followed by all users in the organisation. Technical staff training is necessary to ensure that the organisation has the appropriate tools to combat security threats. Moreover, top management requires training to understand their responsibility in the protection of the organisation's information. The aim of such training is to convince management that their responsibility towards security is not limited to technical staff or the IT department.

The HO linkage is concerned with the organisation's management of employee behaviour. The introduction of policies and procedures is one method used by organisations to ensure that their employees demonstrate the correct behaviour. However, employees are often unfamiliar with such policies, and therefore do not understand why it is needed. As such, policies and procedures should be communicated to employees through an **awareness** campaign. Such a campaign will ensure that employees understand the policies and procedures in place, know where to locate them and understand their importance in terms of the safety of the organisation. Whitman and Mattord (2010, p. 154) recommend that a set of tests or quizzes can be developed to determine if employees understand important points covered in the information security policy.

In the OT linkage, management has to ensure that it has the requisite staff and technological tools to support the organisation and protect it from phishing attacks. Technical staff will require training in this regard but raising awareness will also ensure that staff is aware of their roles and responsibilities. Ensuring enterprise security is even more important for organisations providing a service to their customers. In such cases if customers' information is compromised in any way, it would consequently affect the organisation's reputation.

The next section discusses the evaluation and findings from the interviews.

6.6 Evaluation of the Anti-Phishing Framework

The discussion on the anti-phishing framework in the previous section and the associated security awareness, training and education components has now been

concluded. This section will describe the process used to evaluate the anti-phishing framework.

As stated in section 1.5, Hevner et al.'s (2004) design science guidelines were used to assist in the design of the anti-phishing framework. Hevner et al. (2004) state that research in the field of information systems can typically be divided into two paradigms, namely, design science and behavioural science. The *design science* paradigm aims to extend the boundaries of human and organisational capabilities by creating new and innovative artefacts to solve an identified organisational problem (Hevner et al., 2004). This requires knowledge and understanding of a problem domain and the solution to the problem is achieved through the construction and application of the designed artefact. The artefacts are then evaluated in terms of the utility they provide in solving those problems (Hevner et al., 2004). In this study, the problem domain encompasses the fact that phishing penetrates organisational security controls by exploiting human behaviour. To address this problem, a *behavioural science* paradigm would seek to develop and verify theories that explain or predict human or organisational behaviour. In this study, the behavioural paradigm focused on identifying suitable theories and best practices, such as the TAM, agency theory and COBIT 4.1, to help understand human behaviour in each of the HT, HO and OT linkages. Hence, the intention was to help strengthen the organisation's security defences by focusing on educating humans in each of these areas.

This study has made use of both paradigms. This is supported by Hevner et al. (2004), who believe that both paradigms are fundamentally necessary for understanding people, organisations and technology. Indeed, the elements cited by Hevner et al. (2004) relate to the same foundations used in this study, namely, the HOT dimensions.

According to Hevner et al. (2004), evaluation is a vital component of the research process. The business environment establishes the requirements upon which the evaluation of the artefact is based. Hence, the anti-phishing framework was evaluated by personnel responsible for security in their respective organisations. This satisfies Hevner's third guideline for 'design evaluation'. In this respect, IT artefacts can be evaluated in terms of their functionality, completeness, consistency,

accuracy, performance, reliability and usability in the organisation environment. In this study, the aim is to establish the perceived usefulness (usability) of the IT artefact (i.e. anti-phishing framework) in the business environment. Accordingly, a design artefact is complete and effective when it satisfies the requirements and constraints of the problem it was meant to solve. In this study, the problem is to effectively educate humans to prevent them from falling victim to phishing attacks.

Hevner et al. (2004) categorise the evaluation methods that should be aligned appropriately to the designed artefact and the selected evaluation metrics. For this purpose a 'descriptive' evaluation method is used that includes 'informed argument' and 'scenarios' and both of these were applied to this study. Using the informed argument principle, information from relevant research was used to build a convincing argument for the need for an anti-phishing framework. In section 5.3, scenarios were also used to demonstrate the gaps in each of the linkages caused by human involvement. This contributed towards the development and utility of the anti-phishing framework (artefact).

As mentioned in section 6.5, senior staff members responsible for information security in three organisations were selected to evaluate the components of the anti-phishing framework during semi-structured interviews. The interviews were arranged beforehand with the participants who scheduled a time that was suitable for them. A semi-structured interview was chosen as the appropriate research method, as it is flexible and allows new questions to be asked during the interview process in response to what the interviewee says (Dawson, 2002). Semi-structured interviews require an interview guide containing prearranged questions. The interview guide for this research can be found in Appendix B. Participants gave permission for the conversations in the interview to be recorded. Note-taking was also used to record relevant key points during the interview (Dawson, 2002). The diagrams provided in the interview helped interviewees in terms of giving them a graphical representation of the anti-phishing framework. The diagrams illustrate the framework's beginnings as a single-layer defence model and it ultimate development into a multi-layer defence model.

6.7 Findings

All participants interviewed agreed that all three dimensions should be considered in an anti-phishing framework and they agreed that most of these dimensions operate in isolation from one another. However, Company C felt that the dimensions are not 'completely' isolated from each other, but certainly they need to be improved in terms of cooperation. As such, all participants stated that a holistic model is needed to address phishing instead of one comprising a single-layer defence. Company C stated that a multi-layered defence would have to focus in each of the HOT dimensions. All parties, without hesitation, felt that some form of education is necessary mostly on the part of humans to reduce this gap between each of the dimensions.

Company A pointed out that even if technology fails and users ignore policies, the human element is still the point where most security weaknesses occur. As such, Company A felt that the human element requires awareness raising and training to address these concerns. Company A maintained that the best way for an organisation to educate users on phishing is to carry out mock tests without the knowledge of its employees. The respondent added that induction programmes, brochures, flyers, emails, intranet, and posters on walls are all methods that make employees aware of pertinent security issues. However, Company A stated that, although people may read the information, they will only internalise it once they have suffered the consequences of a policy breach. Therefore, Company A's approach is to conduct external threat assessments of their employees by sending them phishing emails. Company A also believed that the organisation can implement firewalls and block certain websites to a certain extent; nevertheless, users will try to circumvent these controls. Company A felt that informing employees that the organisation has technological controls in place is even more risky. The respondent maintained that users should rather be informed about the technological controls the organisation has in place and the extent of the protection they offer and where the risks lie thereafter. The respondent further added that, today, phishing emails and spoofed websites are so sophisticated that even employees of Company A were unable to distinguish such emails as phishing attacks.

All participants agreed that there are linkages between each of the HOT dimensions. Most participants were not familiar with the TAM and agency theory. However, after having explained the theories, they accepted that they fit the context of each of the linkages appropriately. Company C, however, felt that it was necessary to understand how the TAM model could be applied backwards so as to be T and H instead of H and T. To elaborate, the respondent felt that the focus should be placed on increasing user involvement in technology in terms of combating phishing. They mentioned an example of an organisation having a policy where web browsers are configured to behave in such a way that users understand them more easily.

All participants agreed that training in the HT linkage should be classified into different user levels. The educational components in this linkage originally included basic computer literacy training offered by the organisation. However, all participants did not agree that end-users should be offered computer literacy training, as they felt strongly that employees are expected to possess such general, basic skills prior to appointment. Company A mentioned the following example: if an organisation is employing a software developer in Java, they would assume that the individual can perform the tasks using Java. All participants were adamant that in this digital age everyone should be computer competent. However, Company C stated that, should there be an instance where a new technology or feature is introduced, then employees would be trained accordingly. Moreover, members of top management who do not necessarily have the required security knowledge should be given basic information security training. One of the reasons for this is to lend management support for such programmes. The members of management who are responsible for information security should already have such knowledge and skills.

Company A was rather pessimistic about whether or not organisational policies and procedures would be able to change human behaviour. The respondent felt that human behaviour is so complex that for awareness of policies to be effective, they should be made more personal for employees; in other words, how the consequences of disobeying policies can affect them personally, for example, in terms of loss of income.

Company C believes that policies and procedures must exist as they set the boundary or scope of what employees are expected to do and how they do it.

However, Company C felt that this is still uncontrollable. Company C mentioned the following example: A working hours policy requires that one works from 8 to 5 every day. However, employees can choose to work slowly in their work environment. Accordingly, employees' ethics and behaviour become an issue. Thus, even though there may be boundaries created by the policies, people are still able to make decisions within those boundaries which consequently indirectly violate what the organisation expects from their employees.

Company C felt that employees are not likely to respond to policies unless there is a major consequence or reward. As such, Company C believes an awareness programme can inform users on these two aspects so that they can influence their behaviour. Company C felt that if employees behave in the best interests of the organisation, then they should be rewarded. Consequently, they can be used as an example to other users and therefore help to grow the culture.

Company C stated that comprehensive policy documents will not be read and, furthermore, that too much information given too quickly is not desirable. The respondent further stated that the amount of information people can internalise is limited. Therefore, they felt that it is beneficial to give less information to users more often. They also felt that awareness raising in terms of policies should not happen once, but should take place on a constant basis. They felt that actual training on policies will not be effective because the very nature of a training workshop may imply that training will take a few days and, as a result, will demotivate employees. Company C supports short work sessions during which employees are made aware of certain security aspects. This would mean that training takes less time and users know what to expect. In terms of policies, users should be made aware why they are in place and management should be able to justify the policies instead of taking an approach of "this is what you can or cannot do".

All participants have knowledge and experience in using COBIT. Participants were provided with the COBIT 4.1 guidelines. All participants believe that COBIT 4.1 is the appropriate linkage between O and T. Company A further maintained that they feel even more strongly about COBIT 5, in which risk and Val IT are combined and which has elements of ISO 27002. Companies A and B selected monitoring and evaluation guidelines ME2. Company C felt that merely ensuring systems security is an

operational item and can lose its importance over time if it is not regularly maintained. Company C therefore felt very strongly that monitoring and evaluation guidelines (ME2 and ME3) should be favoured above all other COBIT 4.1 guidelines. They felt that putting in place (i.e. delivering) technological controls is relatively simple, but if these controls are not monitored their effectiveness will decrease, especially since such technological controls are constantly evolving. Company C mentioned that there needs to be some level of feedback on the control levels and that if monitoring is performed, then the outcomes from monitoring will determine what areas need to be addressed through security awareness, training and education programmes.

Companies A, B and C did not feel that best practices, such as ISO 27002, should be a separate component of the linkages. Company C stated that such best practices “live” in each of the linkages.

On the question of whether this framework will help to protect an organisation against phishing attacks, Company A and B supported the notion that integrating the three main dimensions can help to address the phishing problem. Company C felt that putting these elements together would certainly be effective in improving the organisation’s current risk level. However, Company C felt that there would a need for an implementation strategy for the security awareness and training components to be put in place. Table 6.2 below summarises the finding of these interviews.

SUMMARY OF KEY FINDINGS
• All three HOT dimensions in an anti-phishing framework are required to combat phishing.
• Security awareness, training and education are necessary to strengthen each of the linkages.
• Ongoing awareness, using the requisite methods, of organisational policies and procedures must be made personal to employees.
• Computer literacy training offered by the organisation is not necessary in this Digital Age.
• All users should receive security training related to their roles and responsibilities.
• Monitoring and evaluation of the organisation's technological controls should be performed regularly.
• Management should openly demonstrate their support for information security.

Table 6.2: Summary of key findings

Taking the recommendations gleaned from the interviews into account, the implementation guidelines were adapted accordingly and therefore can be used in an anti-phishing framework. Applying a security awareness, training and education programme in each of the respective linkages would assist in forming a holistic anti-phishing framework. Figure 6.2 presents the anti-phishing framework together with its dimensions and attributes which function optimally in each of these linkages.

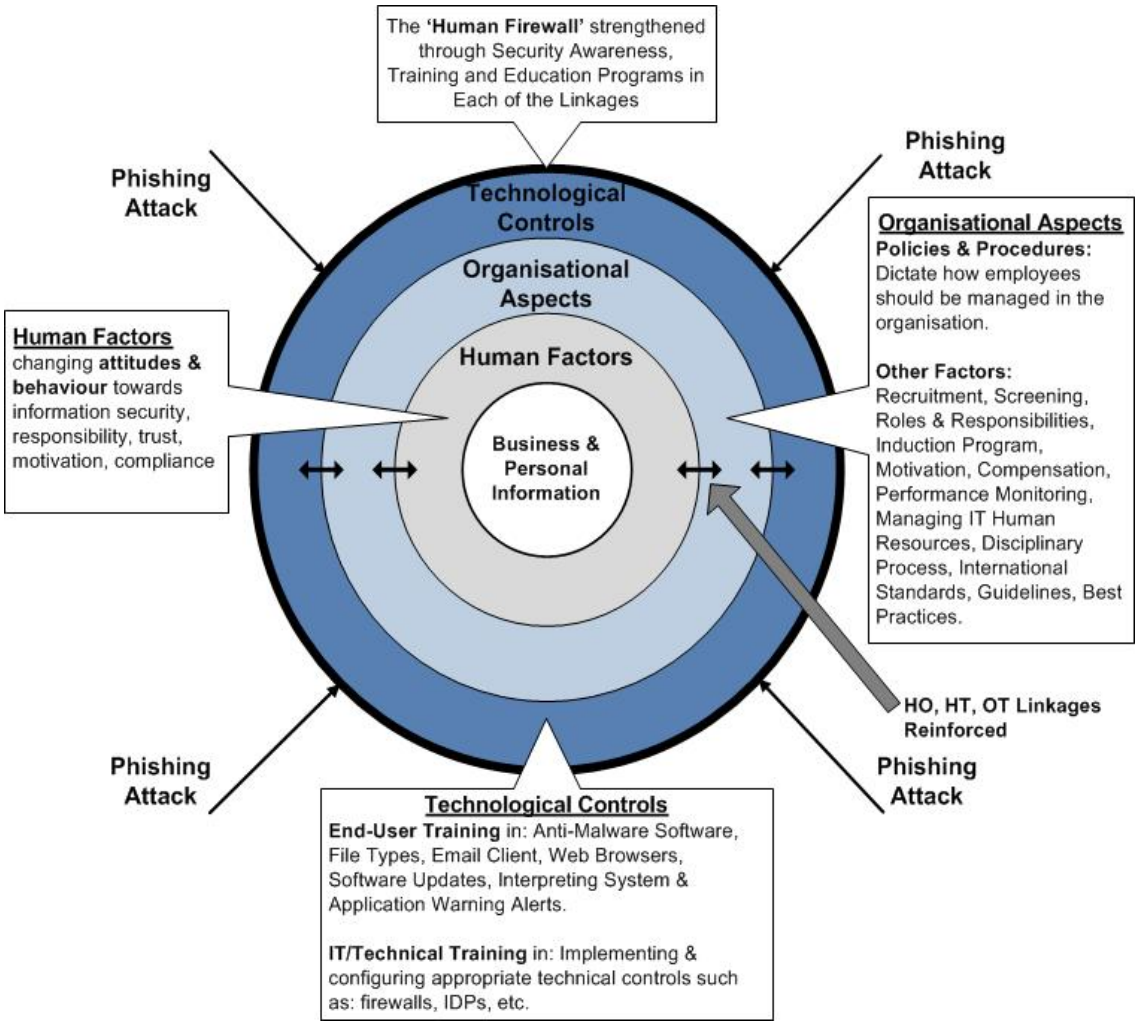


Figure 6.2: Aspects in an organisation related to an anti-phishing framework (adapted from Frauenstein & Von Solms, 2011)

In Figure 6.2, technological controls are typically the organisation's first line of defence against phishing attacks even though humans are involved in the process. Accordingly, humans should be regarded as the first and last line of defence. Constant communication *(concentric circles & arrows)* takes place between the HOT dimensions and, as illustrated, the linkages (arrows) are now reinforced. This serves as a multi-layer defence, as all the components are now operating in harmony with one another. The human dimension is an entry point (if technological controls failed) for phishing attacks and is the common link that influences all the other dimensions.

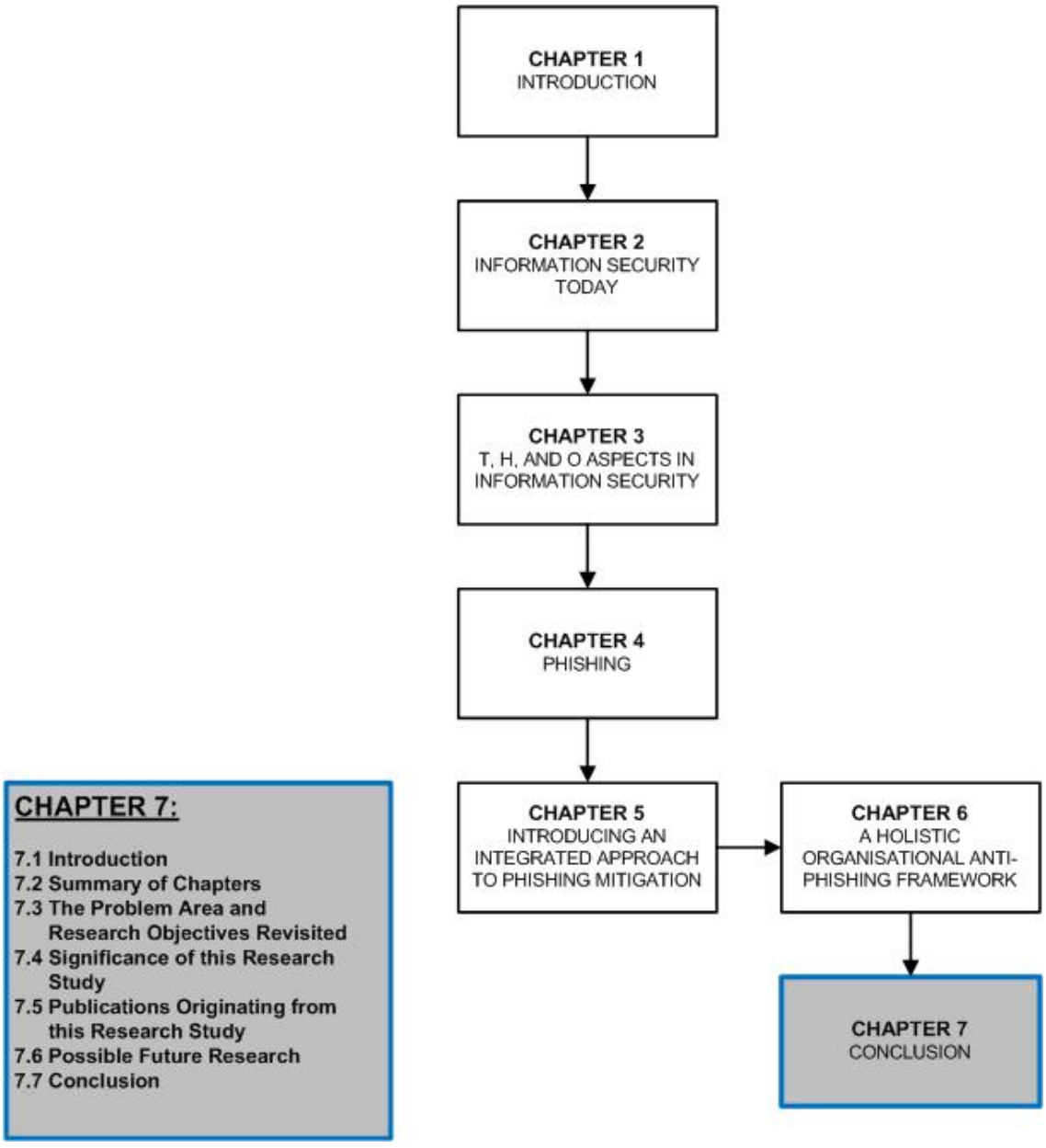
As such, security awareness, training and education aimed at addressing human attitudes and behaviour help to strengthen the interdependencies between each of these linkages**.**

6.8 Conclusion

When attempting to combat phishing in an organisation, more is needed than merely educating employees on how to identify phishing emails and spoofed websites. Despite the different backgrounds and learning styles of employees, the attitudes and behaviour of users still remain an influential factor in the way education is received. A great deal of influence stems from the human and organisational (HO) linkage, as it directly affects the other linkages. This is because most of the activities described in each of the HOT linkages are managed by organisational policies and procedures, which are the management's way of communicating acceptable behaviour and practice to the organisation. However, if these policies are ignored, the operations in each of the linkages will ultimately be affected. To a certain extent, such policies and procedures educate users on what they should and should not do in the organisation, which is the reason education in this regard is so important.

The next chapter concludes the study by briefly summarising the chapters of this dissertation and, further, presenting possible future research directions that have emanated from the work in this dissertation.

CHAPTER 7
CONCLUSION



7.1 Introduction

The objective of this chapter is to formally conclude the research study. The chapter begins by providing a brief summary of the important aspects and conclusions of the previous chapters leading up to the establishment of the anti-phishing framework. Furthermore, the research objectives, identified in section 1.4, will be examined to determine if they have been indeed met. Publications originating from this research will be then revealed. Finally, the chapter will conclude by discussing further conceivable enhancements and research in this field.

7.2 Summary of Chapters

Chapter 1 briefly introduced the problem area of the study. It revealed that humans are the target area for phishers, primarily because of their behaviour and their lack of knowledge concerning the dangers posed by phishing. Based on this problem, the research objectives were formulated. Furthermore, the chapter discussed the methodology used to meet these objectives.

Before phishing could be investigated, it was important to understand areas relating to information security. To start with a broad literature investigation into information security was undertaken in **Chapter 2.** Information is understood to be an asset to organisations and IT is understood to be the infrastructure supporting the storage and dissemination of information. As such, it is necessary for IT systems to be protected by various control measures, as the protection of IT systems will subsequently protect the information. This chapter briefly discussed the controls used to combat general security threats, with most of the controls stated in information security literature focusing on technology. In this study, controls were classified into three dimensions, technological, human and organisational. These three control dimensions are core to the study and, as such, were expanded on in more detail in Chapter 3.

Chapter 3 discussed a range of general information security controls that could be applied by an organisation. Once more, these controls were classified into technological, human and organisational dimensions. The chapter revealed that humans are an influential factor in operations in each of these dimensions. Human

factor issues were also discussed as being the main weakness that modern threat agents focus on.

Chapter 4 conducted an extensive literature study on phishing, the main research problem area of the study. It pointed out that phishers are making effective use of social engineering techniques in order to manipulate humans into giving up information willingly. This indicated that technological controls applied by organisations are inadequate as a defence against phishing attacks. Phishers are making use of technological tools to carry out their attacks. The chapter revealed a number of examples of phishing emails and showed how users can identify these emails if they are taught to identify certain features.

Phishing poses a great danger for organisations and users worldwide. As such, the core focus of this dissertation was to develop a holistic anti-phishing framework that considers human, organisational and technological dimensions. As far as could be determined, there are no frameworks, or models, in existence that combine these areas to combat phishing threats. The chapter pointed out that there are gaps between each of these linkages caused by limited interaction between them, hence resulting in a single-layer defence model. Therefore, there was a need to change this approach.

Chapter 5 proposed aligning each of the linkages. The chapter revealed, through the literature studied, that there is no solution to address the gaps in the linkages. In fact, some researchers state that further research is needed in this regard. To achieve this, scenarios were used to establish linkages between each of the dimensions. The linkages are, namely, HT, HO and OT. Furthermore, to understand the variables related to each of these linkages, theories and best practices were identified and examined. TAM was discussed to address the HT linkage, agency theory for the HO linkage and finally, COBIT 4.1 for the OT linkage. In each of these linkages problems concerning human attitudes and behaviour can be identified, thus creating a gap.

As a result, **Chapter 6** identified security awareness, training and education in each of the linkages as a solution in terms of strengthening these linkages. NIST 800-16 provided guidance in this regard. Components for each linkage were identified from best practices and guidelines such as ISO/IEC 27002 and COBIT 4.1. These components were used to establish the anti-phishing framework. Chapter 6 also

discussed the methodology used in conjunction with Hevner et al.'s design science guidelines. The effectiveness of the anti-phishing framework was verified by conducting semi-structured interviews with security individuals from three companies in Buffalo City. The responses from the interviews were used to validate the components of the anti-phishing framework. The final framework, or artefact, comprises a holistic defence model to strengthen the human, organisational and technological dimensions.

7.3 The Problem Area and Research Objectives Revisited

Protecting information is one of the most important activities an organisation can be involved in. Moreover, of the risks that general information security threats pose to organisations, phishing is certainly one of the most serious and can have severe financial implications for organisations and users. Moreover, it is difficult for organisations to protect themselves, because phishers are able to circumvent technological defences by targeting the human element. Technically minded phishers are also able to exploit software vulnerabilities in systems. Phishers also recognise that humans have psychological vulnerabilities in their knowledge, attitudes and behaviour and tend to exploit such vulnerabilities. Humans are vulnerable because they tend to trust people and want to be helpful, often trusting on sight. Humans, generally, lack knowledge relating to security risks and they also tend to disregard policies and procedures because of their attitudes. These factors all contribute to this security weakness and, as a result, humans are referred to in information security literature as being the weakest link.

Phishers make use of technologies, such as email and websites, in their attacks. Therefore, technological controls can also perform a role in combating phishing emails and preventing access to spoofed websites. However, there are a number of factors that can impede this process. Humans have to be equipped to use these technological controls correctly and phishers can potentially exploit software vulnerabilities if they exist.

Typically, organisations expect their employees to behave in a certain manner, which is managed by rules in the form of policies and procedures. However, if employees do not obey such policies they may also be exposed to phishing attacks. As such,

there is a need for a holistic anti-phishing framework that considers all of these variables.

In this study, an anti-phishing framework classified these different areas as the dimensions of human factors, organisational aspects and technological controls (HOT). Between these dimennions, three linkages were established. Each of these three linkages has human involvement and as such there would predictably be gaps in the form of educational vulnerabilities between them, vulnerabilities that phishers would exploit. This reveals that an anti-phishing solution would have to consider educating humans as a means of aligning each of these areas to reduce the gap. The primary objective of this study was to develop a framework to assist in effectively combatting phishing in an organisational context. The primary objective was accomplished through the following secondary objectives:

- Identify, through literature, those areas that phishing threat agents exploit.
- Identify current protection measures that have been put in place by organisations to guard against phishing attacks.
- Identify the major elements that should play a role in protecting organisations against phishing attacks.
- Identify any weakness in these major elements.
- Identify, through a literature review, how to integrate these elements into a single holistic approach.

The first three of the secondary objectives were achieved in Chapter 4. However, Chapters 2 and 3 did play a role in this process as they introduced the background leading up to Chapter 4. To achieve each of these objectives, an extensive literature review was conducted and reported on in all three chapters. The fourth secondary objective was achieved by means of Chapter 5. Chapter 5 revealed that each of the HOT dimensions operates in isolation as a result of the human involvement or a lack thereof. The final secondary objective was achieved in Chapter 6. The elements were integrated through a security awareness, training and education programme. By achieving each of these objectives, it can be argued that the primary research objective has been met.

7.4 Significance of this Research Study

This study can be considered significant because as far as it could be determined in the literature studied, no research has classified an anti-phishing solution by considering the HOT dimensions. When the literature did identify these dimensions, it was in the context of addressing general information security threats only. Moreover, these dimensions were also not holistically addressed. Although researchers admittedly pointed out that more research is required to understand the relationships between each of these dimensions (Werlinger et al. 2008), most of the literature studied addressed phishing by focusing on educating users in identifying phishing emails and interpreting web browser warnings.

Other research focused on improving technology mostly in terms of web browser plug-ins to protect users on a personal level against phishing attacks. To a certain extent, both of these areas have been proven unsuccessful. This study considered all of these areas in a holistic manner in order to create an anti-phishing framework. One of the respondents commented that the anti-phishing framework could be adapted to any security threat. This creates an opportunity for future researchers to make use of the model and further enhance it.

7.5 Publications Originating from this Research Study

The following peer-reviewed papers have been accepted and presented at conferences during the course of the study:

- Frauenstein, E. D. & Von Solms, R. (2009). Phishing: How an organisation can protect itself. *Information Security South Africa (ISSA).* Johannesburg, South Africa.
- Frauenstein, E. D. & Von Solms, R. (2011). An Enterprise Anti-Phishing Framework. *Proceedings of the 7th World Conference on Information Security Education (IFIP WISE7 TC11.8).* Lucerne, Switzerland: Springer.

These research papers can be located in Appendix C.

7.6 Possible Future Research

This study did not consider investigating organisations targeted by phishing attacks because there is much evidence in the literature that demonstrates the impact phishing has on most users and organisations. Moreover, the study did not test the effectiveness of organisations implementing the components of the anti-phishing framework. It would be fascinating to measure an organisation affected by phishing with a 'before and after implementation' analysis. Only three organisations were used to evaluate the components of the anti-phishing framework, therefore is would be ideal to expand the scope to include organisations outside the Buffalo City region.

7.7 Conclusion

Phishing attacks pose a significant threat to both organisations and users. In order to combat phishing attacks, this study presented a holistic, anti-phishing framework that takes into account the human, technological and organisational (HOT) dimensions. Each of the HOT elements has human involvement. The current phishing defence model, described in literature, is treated as a single-layer defence. Therefore, phishers can exploit the human element. In each of these areas, the implementation of security awareness, training and education strategies in an organisation is necessary and should be treated as an ongoing process. This will help reduce the 'gap'. All stakeholders will have to be made aware of phishing through a specific education intervention programme which should ensure that all users in the organisation understand the risks of phishing, know how to use technology to combat phishing attacks, and understand organisational policies and procedures as well as the risks of not complying with them. Moreover, it is imperative that management demonstrates its support and commitment to these security education programmes.

REFERENCES

AARON, G. (2010). The state of phishing. *Computer Fraud & Security***,** 5–8.

ABURROUS, M., HOSSAIN, M., DAHAL, K., & THABTAH, F. (2010). Experimental case studies for investigating e-banking phishing techniques and attack strategies. *Cognitive Computation, 2*, 242–253.

ACCUVANT LABS. (2011). Browser security comparison: A quantitative approach. Available: http://www.accuvant.com/sites/default/files/AccuvantBrowserSecCompar_FINAL.pdf. [Accessed 05 July 2012].

ADAMS, D. A., NELSON, R. R., & TODD, P. A. (1992). Perceived usefulness, ease of use, and usage of information technology: A replication. *MIS Quarterly, 16*, 227–247.

AGARWAL, N., RENFRO, S., & BEJAR, A. (2007). Phishing forbidden. *Queue, 5*, 28–32.

AI CHEO YEO, M., RAHIM, M., & REN, Y. Y. (2009). Use of persuasive technology to change end-users' IT security aware behaviour: A pilot study. *International Journal of Human and Social Sciences*.

AJZEN, I. (2001). Nature and operation of attitudes. *Annual Review of Psychology, 52*, 27–58.

AJZEN, I., & FISHBEIN, M. (1980). *Understanding attitudes and predicting social behavior.* Englewood Cliffs, NJ, Prentice Hall.

ALFREDS, D. (2012). Hackers hit SA Web users [Online]. Available: http://www.news24.com/SciTech/News/Hackers-hit-SA-web-users-20120702 [Accessed 04 July 2012].

ALSAID, A. & MICHILL, C.J. (2006). Preventing Phishing Attacks using Trusted Computing Technology. Sixth International Network Conference, Citeseer.

AUSTRALIAN NATIONAL AUDIT OFFICE. (2009). Security awareness and training: Audit Report No. 25. Available: http://www.anao.gov.au/uploads/documents/2009-10_Audit_Report_25.pdf. [Accessed 12 September 2012].

AYTES, K., & CONNOLLY, T. (2004). Computer security and risky computing practices: A rational choice perspective. *Journal of Organizational and End User Computing, 16*(3), 22–40.

BAMBERG, G., & SPREMANN, K. (1987). Agency theory, information, and incentives. Berlin, Germany: Springer. 3–38.

BARMAN, S. (2001). Writing Information Security Policies. Available: http://safari.informit.com/?xmlid=1-57870-264-X/ch02#ch02.

BERGHOLZ, A. (2009). AntiPhish: lessons learnt. *Proceedings of the ACM SIGKDD Workshop on CyberSecurity and Intelligence Informatics.* Paris, France: ACM.

BERGLUND, M., & KARLTUN, J. (2007). Human, technological and organizational aspects influencing the production scheduling process. *International Journal of Production Economics, 110*, 160–174.

BERR. (2008). Department for Business Enterprise and Regulatory Reform (BERR) Information Security Breaches Survey. (2008) Available: http://66.102.9.132/search?q=cache:LK4aPYKu4gcJ:www.berr.gov.uk/files/file45714.pdfþberrþ2008þbreaches&;cd=2&hl=en&ct=clnk&gl=uk [Accessed 4 May 2010].

BERTI, J., & ROGERS, M. (2004). *Social engineering: The forgotten risk.* Boca Raton, FL: Auerbach.

BEZNOSOV, K., & BEZNOSOVA, O. (2007). On the imbalance of the security problem space and its expected consequences. *Information Management & Computer Security, 15*, 420–431.

BILGE, L., STRUFE, T., BALZAROTTI, D., & KIRDA, E. (2009). All your contacts are belong to us: Automated identity theft attacks on social networks. *Proceedings of the 18th International Conference on World Wide Web.* Madrid, Spain: ACM. 551–560.

BINARYCSE. (2010). Information Security [Online]. Available: http://www.binarycse.com/information-security?format=pdf. [Accessed 14 May 2011].

BISHOP, M. (2000). Education in information security. *IEEE Concurrency, 8*, 4–8.

BROWN, E. J., & YARBERRY JNR, W. A. (2009). *The effective CIO: How to achieve outstanding success through strategic alignment financial management & IT governance.* New York: Auerbach.

BROWN, G., HOWE, T., IHBE, M., PRAKASH, A., & BORDERS, K. (2008). Social networks and context-aware spam. *Proceedings of the 2008 ACM conference on Computer supported cooperative work.* San Diego, CA, USA: ACM.403–412

BUTLER, R. (2007). A framework of anti-phishing measures aimed at protecting the online consumer's identity. *Framework of Anti-Phishing Measures, 25***,** 517–533.

CABRERA, Á., CABRERA, E. F., & BARAJAS, S. (2001). The key role of organizational culture in a multi-system view of technology-driven change. *International Journal of Information Management, 21*, 245–261.

CENTREFORCONFIDENCE.CO.UK. (n.d.) *6 ways to create a more positive atmosphere at work.* Available: http://www.centreforconfidence.co.uk/pp/techniques.php?p=c2lkPTEwJnRpZD0zJmlkPTI3OA== [Accessed 04 July 2012].

COBB, M. (2010). *Preventing phishing attacks: Enterprise best practices* [Online]. SearchSecurity.co.uk. Available: http://searchsecurity.techtarget.co.uk/tip/0,289483,sid180_gci1381209,00.html?Offer=mn_eh030910UKSCWELC_phishing&asrc=EM_EVM_2-11390344&uid=8019187 [Accessed 23 May 2010].

COBIT 4.1. (2007). *COBIT 4.1 Executive Summary*. Illinois, USA: IT Governance Institute.

COLWILL, C. (2010). Human factors in information security: The insider threat – Who can you trust these days? *Information Security Technical Report, 30***,** 1–11.

CRANOR, L. F. (2008). *A framework for reasoning about the human in the loop*. Proceedings of the 1st Conference on Usability, Psychology, and Security. San Francisco, California: USENIX Association.

CRAWFORD, M. (2006). *Whoops, human error does it again* [Online]. CSO Online. Available: http://www.csoonline.com.au/index.php/id;255830211;fp;32768;fpid;20026681 [Accessed 10 February 2010].

DACS. (2008). Enhancing the development life cycle to produce secure software. Available: http://www.thedacs.com/techs/enhanced_life_cycles [Accessed 28 May 2009].

DANCHEV, D. (2003). Building and implementing a successful information security policy, WindowsSecurity.com. Available: http://www.windowsecurity.com/pages/security-policy.pdf [Accessed 20 September 2012].

DAVIS, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*, 319–340.

DAWSON, C. (2002). *Practical research methods: A user-friendly guide to mastering research.* United Kingdom. HowtoBooks.

DEFINO, S., KAUFMAN, B., VALENTEEN, N. J., & GREENBLATT, L. (2010). *Official certified ethical hacker review guide.* Boston, MA: Course Technology/Cengage Learning.

DELOITTE. (2009). *Protecting what matters: The 6th Annual Global Security Survey*. Available: http://www.deloitte.com/assets/Dcom-shared%20Assets/Documents/dtt_fsi_GlobalSecuritySurvey_0901.pdf [Accessed 15 August 2011].

DELOITTE. (2012). *Deloitte-NASCIO Cybersecurity Study: State governments at risk: a call for collaboration and compliance*. Available: http://www.nascio.org/events/2012Annual/documents/State-Governments-at-Risk.pdf [Accessed 20 November 2012].

DHAMIJA, R., TYGAR, J. D., & HEARST, M. (2006). *Why phishing works*. Proceedings of the SIGCHI conference on Human Factors in computing systems, Montreal, Quebec, Canada: ACM. 581–590.

DHILLON, G. (1997). *Managing information system security*. Houndmills, Basingstoke, Hampshire: Macmillan Press.

DHILLON, G. (2001). Violation of safeguards by trusted personnel and understanding related information security concerns. *Computers & Security*, *20*(2), 165–172.

DHILLON, G., & BACKHOUSE, J. (2001). Current directions in IS security research: Towards socio-organizational perspectives. *Information Systems Journal, 11*, 127–153.

DODGE JR., R. C., CARVER, C., & FERGUSON, A. J. (2007). Phishing for user security awareness. *Computers & Security, 26*, 73–80.

DOWNS, J. S., HOLBROOK, M. B., & CRANOR, L. F. (2006). *Decision strategies and susceptibility to phishing.* Proceedings of the second symposium on Usable privacy and security. Pittsburgh, Pennsylvania: ACM. 79-90.

DOWNS, J. S., HOLBROOK, M. B., & CRANOR, L. F. (2007). *Behavioral response to phishing risk.* Proceedings of the Anti-Phishing Working Group's 2nd Annual eCrime Researchers Summit, 2007 Pittsburgh, Pennsylvania. 1299019: ACM, 37-44.

DRAKE, C. E., OLIVER, J. J., & KOONTZ, E. J. (2004). *Anatomy of a phishing email.* Conference on Email and Anti-Spam (CEAS). Citeseer.

DU PLESSIS, L., & VON SOLMS, R. (2002). *Information security awareness: Baseline education and certification.* Proceedings of ISSA 2002, Muldersdrift, South Africa.

DYE, M., MCDONALD, R., & RUFI, A. (2008). *Network fundamentals: CCNA exploration companion guide.* Indianapolis, IN: Cisco Press.

EGELMAN, S., CRANOR, L. F., & HONG, J. (2008). *You've been warned: An empirical study of the effectiveness of web browser phishing warnings*. Proceedings of the

twenty-sixth annual SIGCHI conference on Human factors in computing systems. Florence, Italy: ACM.1065-1074.

EISENHARDT, K. M. (1989). Agency theory: An assessment and review. *Academy of Management Review, 14*, 57–74.

EKLUND, J. (2003). *An extended framework for humans, technology and organization in interaction.* In K. J. ZINK & H. LUZCAK (Eds.), Proceedings of human factors in organizational design and management. Wissenschaftsverlag, Aachen.

ERNST & YOUNG. (2010). *Borderless security: Global Information Security Survey 2010.* Available: http://www.ey.com/Publication/vwLUAssets/Global_information_security_survey_2010_advisory/$FILE/GISS%20report_final.pdf [Accessed 13 August 2011].

EVERETT, C. (2011). Is ISO 27001 worth it? *Computer Fraud & Security***,** 5–7.

EXPERIAN. (2009). *Information security controls: Briefing for clients on Experian information security controls*. [Accessed 01 May 2011].

EXPERTRON. (2009). *Standard Bank warns of phishing scam* [Online]. Available: http://www.expertron.co.za/index.php?module=newsmodule&src=@random41940a897e943&int=&action=view&id=24 [Accessed 01 October 2009].

FERUZA, Y. S., & TAO-HOON, K. (2007). IT security review: Privacy, protection, access control, assurance and system security. *International Journal of Multimedia and Ubiquitous Engineering* [Online], 2. Available: http://www.sersc.org/journals/IJMUE/vol2_no2_2007/2.pdf. [Accessed 12 January 2012].

FETTE, I., SADEH, N., & TOMASIC, A. (2007). Learning to detect phishing emails. *Proceedings of the 16th international conference on World Wide Web.* Banff, Alberta, Canada: ACM.

FIN24.COM. (2009). *Sars issues scam warning* [Online]. Available: http://www.fin24.com/articles/default/display_article.aspx?ArticleId=1518-1786_2466825 [Accessed 05 October 2009].

FLORENCIO, D., & HERLEY, C. (2005). *Stopping a phishing attack, even when the victims ignore warnings*. Available: ftp://ftp.research.microsoft.com/pub/tr/TR-2005-142.pdf. [Accessed 21 April 2009].

FLOWERDAY, S., & VON SOLMS, R. (2005). Real-time information integrity system integrity data integrity continuous assurances. *Computers and Security***,** 604–613.

FOGG, B. J. (2002). Persuasive technology: Using computers to change what we think and do. *Ubiquity, 2*.

FRAUENSTEIN, E. D., & VON SOLMS, R. (2009). Phishing: How an organisation can protect itself. *Information Security South Africa (ISSA).* Johannesburg, South Africa. 253–268.

FRAUENSTEIN, E. D., & VON SOLMS, R. (2010). The wild wide west of social networking sites. In N. CLARKE, S. FURNELL, & R. VON SOLMS (Eds), *South African Information Security Multi-Conference* (pp. 74–88). Port Elizabeth, South Africa.

FRAUENSTEIN, E. D., & VON SOLMS, R. (2011). An enterprise anti-phishing framework. *Proceedings of the 7th World Conference on Information Security Education (IFIP WISE7 TC11.8),* (pp. 80–88). Lucerne, Switzerland.

FULKS, B. (2010). Whaling: Going phishing for a bigger fish. Available: http://www.brighthub.com/computing/smb-security/articles/14193.aspx [Accessed 26 December 2010].

FURNELL, S. M., & CLARKE, N. L. (2005). Organisational security culture: Embedding security awareness, education and training. *Proceedings of the 4th World Conference on Information Security Education (WISE 2005)*, Moscow, 67–74.

FURNELL, S. M., JUSOH, A., & KATSABAS, D. (2006). The challenges of understanding and using security: A survey of end-users. *Computers & Security*, *25*, 27–35.

GALITZ, W. O. (2007). *The essential guide to user interface design: An introduction to GUI design principles and techniques.* Indianapolis, IN: Wiley.

GARERA, S., PROVOS, N., CHEW, M., & RUBIN, A. D. (2007). A framework for detection and measurement of phishing attacks. *Proceedings of the 2007 ACM workshop on Recurring malcode* (pp. 1–8). Alexandria, VA: ACM.

GARTNER. (2005). Wetware's Intrusion Prevention Systems: Defending Against Social engineering [Online]. Gartner IT Security Summit 2005. Available: http://gabiam.com/software/users/kfc/pdf/sec11_a5.pdf [Accessed 10 September 2010].

GEER, D. (2005). Security technologies go phishing. *IEEE Xplore, 38***,** 18–21.

GEER, D., SOO HOO, K., & JAQUITH, A. (2003). Information security: Why the future belongs to the quants. *IEEE Security & Privacy***,** 24–32.

GIBSON, R. (2007). Who's really in your top 8: network security in the age of social networking. *Proceedings of the 35th annual ACM SIGUCCS conference on User services* (pp. 131–134). Orlando, FL: ACM.

GOERTZEL, K. M. (2008). *Insider threat in the SDLC*. Available: https://buildsecurityin.us-cert.gov/swa/downloads/Tutorial_Goertzel_Insider_Threat.pdf [Accessed 26 December 2010].

GONZALEZ, J. J., & SAWICKA, A. (2002). A framework for human factors in information security. *WSEAS International Conference on Information Security*. Rio de Janeiro, Brazil.

GORGE, M. (2007). Cyberterrorism: Hype or reality? *Computer Fraud & Security***,** 9–11.

GRAGG, D. (2002). A multi-level defense against social engineering. *InfoSec Reading Room.* SANS Institute.

GROSS, R., & ACQUISTI, A. (2005). Information revelation and privacy in online social networks. *WPES* (pp. 71–80). Alexandria, Virginia, USA: ACM.

HABER, A., & RUNYON, R. P. (1986). *Fundamentals of psychology* (4th ed.). New York, NY: Random House.

HARRISON, D. A., NEWMAN, D. A., & ROTH, P. L. (2006). How important are job attitudes? Mata-Analytic comparisons of integrative behavioural outcomes and time sequences. *Academy of Management Journal*, *49*, 305–325.

HAWKEY, K., BOTTA, D., WERLINGER, R., MULDNER, K., GAGNE, A. & BEZNOSOV, K. (2008). Human, organizational, and technological factors of IT security. *CHI '08 extended abstracts on Human factors in computing systems*, 2008 Florence, Italy. 1358905: ACM, 3639-3644.

HELOKUNNAS, T. & IIVONEN, I. (2003). *Information security culture in small and medium size enterprises*. Business Research Forum. Tampere University of Technology, Tampere. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.101.8320&rep=rep1&type=pdf. [Accessed 15 July 2009].

HERATH, T., & RAO, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47***,** 154–165.

HEVNER, A., MARCH, S. T., PARK, J., & RAM, S. (2004). Design science in information systems research. *MIS Quarterly, 28*, 75–105.

HIGHT, S. D. (2005). *The importance of a security, education, training and awareness program.* Available: http://www.infosecwriters.com/text_resources/pdf/SETA_SHight.pdf. [Accessed 02 September 2012].

HINSON, G. (2003). *Human factors in information security*. Available: http://www.infosecwriters.com/text_resources/pdf/human_factors.pdf. [Accessed 10 October 2012].

HOFSTEE, E. (2006). *Constructing a good dissertation: A practical guide to finishing a masters, MBA or PhD on schedule*. Johannesburg: EPE.

HTCIA. (2010). *Report on cybercrime investigation* [Online]. Roseville, CA: High Tech Crime Investigation Association. Available: http://www.htcia.org/pdfs/2010survey_report.pdf. [Accessed 20 August 2011].

HUBPAGES. (2012). *Top 10 light antivirus softwares* [Online]. Available: http://nainoo1.hubpages.com/hub/Top-10-Free-Antivirus-Software-Of-Year-2010. [Accessed 24 October 2012].

ISACA. (2009). *An introduction to the business model for information security*. Available: http://www.isaca.org/Knowledge-Center/BMIS/Documents/IntrotoBMIS.pdf. [Accessed 10 July 2009].

ISO/IEC 27002. (2005). Information Technology: Security techniques – Code of practice for information security management. *ISO/IEC 27002:2005.* Standards South Africa.

JAKOBSSON, M. (2007). The human factor in phishing. *Privacy & Security of Consumer Information*.

JAKOBSSON, M., & RATKIEWICZ, J. (2006). Designing ethical phishing experiments: a study of (ROT13) rOnl query features. *Proceedings of the 15th International Conference on World Wide Web.* Edinburgh, Scotland: ACM.

JAKOBSSON, M., TSOW, A., SHAH, A., BLEVIS, E., & LIM, Y. K. (2007). What instills trust? A qualitative study of phishing. *Proceedings of the 11th International Conference on Financial cryptography and 1st International conference on Usable Security.* Scarborough, Trinidad and Tobago: Springer-Verlag.

JANCZEWSKI, L. J., & COLARIK, A. M. (2007). *Cyber warfare and cyber terrorism.* New York, NY: Information Science Reference.

JENSEN, M., & MECKLING, W. (1976). Theory of the firm: Managerial behavior, agency costs, and ownership structure. *Journal of Financial Economics, 3*, 305–360.

JOHNSON, E. C. (2006). Security awareness: Switch to a better programme. *Network Security*, 15–18.

KANKANHALLI, A. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management*.

KING REPORT. (2001). *The King Report on Corporate Governance for South Africa*. Johannesburg: Institute of Directors of Southern Africa.

KING III REPORT. (2009). *The King III Report on Corporate Governance for South Africa*. Johannesburg: Institute of Directors of Southern Africa.

KIRDA, E., & KRUEGEL, C. (2006). Protecting users against phishing attacks. *The Computer Journal*, 49.

KIRSTEN, H. W. (2001). *Personnel management for N5 students: A practical approach for technical colleges in South Africa*. Johannesburg: Future Managers.

KRAEMER, S., CARAYON, P., & CLEM, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computers & Security, 28*, 509–520.

KRAMMER, V. (2006). Phishing defense against IDN address spoofing attacks. *Proceedings of the 2006 International Conference on Privacy, Security and Trust: Bridge the Gap Between PST Technologies and Business Services.* Markham, Ontario, Canada: ACM.

KUMARAGURU, P., CRANSHAW, J., ACQUISTI, A., CRANOR, L., HONG, J., BLAIR, M. A., & PHAM, T. (2009). School of phish: A real-world evaluation of anti-phishing training. *Proceedings of the 5th Symposium on Usable Privacy and Security.* Mountain View, California: ACM.

KUMARAGURU, P., RHEE, Y., SHENG, S., HASAN, S., ACQUISTI, A., CRANOR, L. F., & HONG, J. (2007). Getting users to pay attention to anti-phishing education: Evaluation of retention and transfer. *Proceedings of the Anti-Phishing Working Group's 2nd Annual eCrime Researchers Summit.* Pittsburgh, Pennsylvania: ACM.

LACEY, D. (2009). *Managing the human factor in information security: - How to win over staff and influence business managers*. West Sussex, England: Wiley.

LEACH, J. (2003). Improving user security behaviour. *Computers & Security, 22*, 685–692.

LEAVITT, N. (2005). Instant messaging: A new target for hackers. *IEEE Computer Society Press*, 20–33.

LEE, Y., KOZAR, K. A., & LARSEN, K. R. T. (2003). The Technology Acceptance Model: Past, present, and future. *Communications of the Association for Information Systems, 12*, 752–780.

LEGRISA, P., INGHAMB, J., & COLLERETTE, P. (2001). Why do people use information technology? A critical review of the technology acceptance model. *Information & Management, 40*, 191–204.

LEVY, E., & ARCE, I. (2004). Criminals become tech savvy. *IEEE Security & Privacy, 2*, 65–68.

LEWIS, M. (2012). *Lucrative incentives for SA Olympic athletes* [Online]. EyeWitness News. Available: http://ewn.co.za/en/2012/07/11/Lucrative%20Olympic%20incentives%20for%20athletes.aspx. [Accessed 13 July 2012].

LIM, J. S., AHMAD, A., CHANG, S., & MAYNARD, S. (2010). Embedding information security culture: Emerging concerns and challenges. *PACIS,* 463–474.

LIM, J. S., CHANG, S., MAYNARD, S. B., & AHMAD, A. (2009). *Exploring the relationship between organizational culture and information security culture. Proceedings of 7th Australian Information Security Management Conference*, SECAU Security Congress 2009, Perth, Western Australia.

LITAN, A. (2004). *Phishing attack victims likely targets for identity theft*. Gartner, Available: http://www.gartner.com/resources/120800/120804/phishing_attack.pdf [Accessed 05 December 2010].

LITAN, A. (2005). *Increased phishing and online attacks cause dip in consumer confidence.* Gartner. Available: http://leetupload.com/database/Misc/Papers/Web%20Papers/Gartner_IncreasedPhishingAffectConsumerconfidence_22Jun2005.pdf. [Accessed 05 December 2010].

LITAN, A. (2006). Phishing attacks leapfrog despite attempts to stop them. *Proceedings Of the 12th Annual Conference on World Wide Web Applications.* Gartner.

LUFTMAN, J. (2004). *Strategies for information technology governance.* Pennsylvania, USA: Idea Group (IGI Global).

MANN, I. (2008). *Hacking the human.* Hampshire: Gower.

MICROSOFT. (1999). *Security threats: Best practices for enterprise security* [Online]. Available: http://technet.microsoft.com/en-us/library/cc723507.aspx. [Accessed 20 October 2012].

MICROSOFT. (2008). *Protecting your business and brand from online threats (White Paper)* [Online]. Available: http://download.microsoft.com/download/c/2/3/c2371de6-2ea0-455d-b6eb-b8a21fc9a14e/domain_protect.pdf [Accessed 10 January 2012].

MICROSOFT. (2009). *Protect yourself from social engineering attacks* [Online]. Microsoft. Available: http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Virus%3aWin32%2fSality.AT#summary_link [Accessed 10 July 2010].

MITNICK, K. D., & SIMON, W. L. (2002). *The art of deception: Controlling the human element of security.* New York, NY: Wiley.

MITTNER, M. (2007). *New e-scam hits Absa* [Online]. Fin24.com. Available: http://www.fin24.com/articles/default/display_article.aspx?ArticleId=1518-24_2229521 [Accessed 03 October 2009].

MONK, T. P. (2011). *Educating users about information security by means of game play.* Magister Technologiae: Information Technology, Nelson Mandela Metropolitan University.

MYDEBT.CO.ZA. (2011). *Q&A identity theft in South Africa* [Online]. Available: http://www.mydebt.co.za/index.php?option=com_content&view=article&id=112:qaa-identity-theft-in-south-africa&catid=47:identity-theft&Itemid=157 [Accessed 10 August 2011].

NATIONAL CHAMBER FOUNDATION. (2005). What are counterfeiting and piracy costing the American economy? Available:

http://www.fnal.gov/directorate/OQBP/sci/sci_reference_docs/SCI%20Costs%20to%20Economy%20uschamber.pdf. [Accessed 10 June 2012].

NELSON, A. D. (2011). *Patching the wetware: Addressing the human factor in information security.* Degree of Master of Cyberwarfare: Air Force Institute of Technology.

NIST 800-16. (1998). *Information technology security training requirements: A role-and performance-based model.* Gaithersburg, MD: National Institute of Standards and Technology.

NIST 800-50. (2003). *Building an information technology security awareness and training program*. Gaithersburg, MD: National Institute of Standards and Technology.

NIST 800-53. (2009). *Recommended security controls for federal information systems and organizations.* Gaithersburg, MD: National Institute of Standards and Technology.

NIST 800-37. (2010). *Guide for applying the risk management framework to federal information systems: A security life cycle approach*. Gaithersburg, MD: National Institute of Standards and Technology.

NOSWORTHY, J. D. (2000). Implementing information security in the 21st century: Do you have the balancing factors? *Computer & Security, 19*, 337–347.

OGREN, E. (2009). *Phishing protection begins with training, antiphishing evangelist*. Available: http://searchsecurity.techtarget.co.uk/news/column/0,294698,sid180_gci1371629,00.html [Accessed 20 December 2010].

OHAYA, C. (2006). Managing phishing threats in an organization. *Proceedings of the 3rd annual conference on Information security curriculum development*, 2006 Kennesaw, Georgia. 1231083: ACM. 159–161.

O'LEARY, T. J., & O'LEARY, L. I. (2010). *Computing essentials 2011.* New York, NY: McGraw-Hill/Irwin.

OLLMANN, G. (2008). *The phishing guide (white paper).* Available: http://www.ngssoftware.com/papers/NISR-WP-Phishing.pdf [Accessed 16 April 2009].

ORGILL, G. L., ROMNEY, G. W., BAILEY, M. G., & ORGILL, P. M. (2004). The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems. *Proceedings of the 5th conference on Information technology education.* Salt Lake City, UT, USA: ACM.

PAHNILA, S., SIPONEN, M., & MAHMOOD, A. (2007). Employees' behavior towards is security policy compliance. *Proceedings of the 40th Hawaii International Conference on System Sciences*, Hawaii.

PARSONS, K., MCCORMAC, A., BUTAVICIUS, M., & FERGUSON, L. (2010). *Human factors and information security: Individual, culture and security environment.* Edinburgh, South Australia: Defence Science and Technology Organisation. Available: http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA535944. [Accessed 10 October 2012].

PATEL, D. & LUO, X. (2007). Take a close look at phishing, *Information Security Curriculum Development Conference '07*, *Proceedings of the 4th annual conference on Information security curriculum development*, Kennesaw, Georgia, USA: ACM. 1-4.

PATRICK, A. S., BRIGGS, P., & MARSH, S. (2005). *Security and usability: Designing secure systems that people can use.* Canada: National Research Council.

PATTERSON, M. G., WEST, M. A., LAWTHOM, R., & NICKELL, S. (1998). *Impact of people management practices on business performance.* London: Institute of Personnel and Development. Available:http://www.cipd.co.uk/NR/rdonlyres/75D39FB0-061E-4983-B681-FB1E0C43CB96/0/ImpactofPeoplMgmntinBusPerf.pdf [Accessed 10 July 2012].

PAYNE, S. (2003). Developing security education and awareness programs. *Educause Quarterly, 4*, 49–53.

PICKWORTH, E. (2009). *Phishing scams persist* [Online]. Available: http://www.news24.com/Content/SciTech/News/1132/85d65418408c4cc1920b78b8aaa930de/21-07-2009-10-32/Phishing_scams_persist [Accessed 06 April 2009].

PIPLINE, M. (2005). *WiPhishing' said to threaten wi-fi users* [Online]. Information Week. Available: http://www.informationweek.com/story/showArticle.jhtml?articleID=59301241 [Accessed 10 June 2010].

POSTHUMUS, S. (2009). *A model for aligning information technology strategic and tactical management.* Philisophiae Doctor: Information Technology, Nelson Mandela Metropolitan University.

POSTHUMUS, S., & VON SOLMS, R. (2004). A framework for the governance of information security. *Computers & Security, 23*, 638–646.

PRICEWATERHOUSE COOPERS. (2008). Safeguarding the new currency of business. Findings from the 2008 Global State of Information Security Study. Available: http://www.pwc.com/gx/en/information-security-survey/pdf/safeguarding_the_new_currency.pdf. [Accessed 12 September 2009].

RAGHU, T. S., JAYARAMAN, B. & RAO, H. R. 2004. Toward an integration of an agent and activity centric approaches in organizational process modelling: incorporating incentive mechanisms. *Information Systems Research,* 15.

RASMUSSEN, J. 1994. *Risk management, adaption, and design for safety,* Dordrecht: Kluwer Academic Publishers.

ROBILA, S. A., & RAGUCCI, J. W. (2006). Don't be a phish: Steps in user education. *Proceedings of the 11th Annual SIGCSE Conference on Innovation and Technology in Computer Science Education.* Bologna, Italy: ACM.

ROSS, S. (1973). The economic theory of agency: The principal's problem. *American Economic Review, 63*, 134–139.

RUSSELL, C. (2002). *Security awareness: Implementing an effective strategy*. Available: http://www.sans.org/reading_room/whitepapers/awareness/security-awareness-implementing-effective-strategy_418 [Accessed 10 May 2011].

SAFECODE. (2008). *Software assurance: An overview of current industry best practices*. Available: http://www.safecode.org/publications/SAFECode_BestPractices0208.pdf [Accessed 14 April 2009].

SARS. (2009). *SARS phishing attack.* Available: http://www.sars.gov.za/home.asp?pid=42736 [Accessed 14 April 2009].

SCHEIN, E. H. (1985). *Organizational culture and leadership: A dynamic view.* San Francisco, CA: Jossey-Bass.

SCHEIN, E. H. (1999). *The corporate culture survival guide.* San Francisco, CA: Jossey-Bass.

SCHLIENGER, T., & TEUFEL, S. (2003). Information security culture: From analysis to change. *Proceedings of the 3rd Annual Information Security South Africa Conference (ISSA).* Johannesburg, South Africa, 183–196.

SCHNEIER, B. (2000). *Semantic attacks: The third wave of network attacks*. Available: http://www.schneier.com/crypto-gram-0010.html#1. [Accessed 14 April 2009].

SCHNEIER, B. (2003). *Beyond fear: Thinking sensibly about security in an uncertain world.* New York*:* Springer-Verlag.

SCHNEIER, B. (2008). The psychology of security. *Proceedings of the Cryptology in Africa 1st international conference on Progress in cryptology.* Casablanca, Morocco: Springer-Verlag.

SHELLY, G. B. & VERMAAT, M. E. (2011). *Discovering Computers 2011-Living in a Digital World, Complete*, Cengage Learning.

SHENG, S., HOLBROOK, M., KUMARAGURU, P., CRANOR, L. F., & DOWNS, J. (2010). Who falls for phish?: A demographic analysis of phishing susceptibility and effectiveness of interventions. *Proceedings of the 28th international conference on Human factors in computing systems.* Atlanta, Georgia, USA: ACM.

SHENG, S., MAGNIEN, B., KUMARAGURU, P., ACQUISTI, A., CRANOR, L. F., HONG, J., & NUNGE, E. (2007). Anti-Phishing Phil: The design and evaluation of a game that

teaches people not to fall for phish. *Proceedings of the 3rd symposium on Usable privacy and security.* Pittsburgh, Pennsylvania: ACM.

SHING, M.-L., SHING, C.-C., CHEN, K. L., & LEE, H. (2010). A game theory approach in information security risk study. *International Conference on E-business, Management and Economics.* Hong Kong: IACSIT Press.

SIPONEN, M. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8*(1), 31–41.

SOPHOS. (2005). *Phishing and the threat to corporate networks (White Paper).* Available: http://www.sophos.com/whitepapers/sophos-phishing-wpuk.pdf. [Accessed 16 May 2010].

STEPHANOU, A. T., & DAGADA, R. (2008). The impact of information security awareness training on information security behaviour: The case for further research. *Proceedings of Information Security South Africa (ISSA).*

SWANSON, E. B. (1988). *Information system implementation: Bridging the gap between design and utilization.* Homewood, IL: Irwin.

THOMSON, K.-L. (2003). *Integrating information security into corporate culture.* Magister Technologiae: Information Technology, Port Elizabeth Technikon.

THOMSON, K.-L., VON SOLMS, R., & LOUW, L. (2006). Cultivating an organizational information security culture. *Computer Fraud & Security.*

THOMSON, M. (1998). *The development of an effective information security awareness program for use in an organization.* Magister Technologiae: Information Technology, Port Elizabeth Technikon.

THOMSON, M. E., & VON SOLMS, R. (1998). Information security awareness: Educating your users effectively. *Information Management & Computer Security*, *6*, 167–173.

THREAT INSIGHT QUARTERLY (2005). Phishing and other significant threats of 2004. Internet Security Systems, Avaliable: http://documents.iss.net/ThreatIQ/ISS_XFIQ0205.pdf [Accessed 14 April 2009].

TUE. (2012). *Human-technology interaction* [Online]. Available: http://www.tue.nl/en/education/tue-graduate-school/masters-programs/human-technology-interaction/ [Accessed 20 October 2012].

UNISYS. (2008). *Unisys identifies five security issues likely to emerge across multiple industries in 2008* [Online]. BusinessWire. Available: http://www.businesswire.com/portal/site/google/?ndmViewId=news_view&newsId=20080115005324&newsLang=en [Accessed 14 April 2009].

VAN DER MERWE, A., LOOCK, M., & DABROWSKI, M. (2005a). Characteristics and responsibilities involved in a phishing attack. *Proceedings of the 4th International Symposium on Information and Communication Technologies.* Cape Town, South Africa: Trinity College Dublin.

VAN DER MERWE, A., SEKER, R., & GERBER, A. (2005b). Phishing in the system of systems settings: Mobile technology. *Systems, Man and Cybernetics IEEE International Conference 10–12 October, 1*, 492–498.

VAN DYKE, J. (2004). *Online account management as the antidote to fraud: Financial institutions and billers must revamp their web features and messages* [Online]. Javelin Strategy & Research. Available: http://www.javelinstrategy.com/rp.html 2010.

VAN NIEKERK, J. F. (2005). *Establishing an information security culture in organizations: An outcomes based approach.* Magister Technologiae: Information Technology, Nelson Mandela Metropolitan University.

VAN NIEKERK, J., & VON SOLMS, R. (2002). A web-based portal for information security education. *Information Security South Africa (ISSA).* Muldersdrift, South Africa.

VAN NIEKERK, J., & VON SOLMS, R. (2004a). Organisational learning models for information security. *Information Security South Africa (ISSA).* Johannesburg, South Africa.

VAN NIEKERK, J., & VON SOLMS, R. (2004b). Corporate information security education: Is outcomes based education the solution? *10th IFIP WG11.1 Annual Working Conference on Information Security Management, World Computer Congress (WCC),* Toulouse, France.

VAN NIEKERK, J., & VON SOLMS, R. (2008). Bloom's taxonomy for information security education. *Information Security South Africa (ISSA).* Johannesburg, South Africa.

VEGTER, I. (2005). Plugging the 'phishing' hole. *iWeek, 5*, 16–18.

VON SOLMS, B. (2000). Information security: The third wave? *Computers & Security, 19*, 615–620.

VON SOLMS, B. (2006). Information security: The fourth wave. *Computers & Security, 25*, 165–168.

VON SOLMS, B., & VON SOLMS, R. (2005). From information security to business security? *Computers & Security, 24*, 271–273.

VON SOLMS, B., & VON SOLMS, R. (2006). Information security governance: Due care. *Computers & Security, 25*, 494–497.

VON SOLMS, R. (1998). Information security management: The code of practice for information security management (BS 7799). *Management & Computer Security, 6*, 224–225.

VON SOLMS, R., & VON SOLMS, B. (2004). From policies to culture. *Computers & Security, 23*, 275–279.

VON SOLMS, R., & VON SOLMS, S. H. (2006). Information security governance: A model based on the direct–control cycle. *Computers and Security, 25*, 408–412.

VON SOLMS, S. H., & VON SOLMS, R. (2009). *Information security governance.* New York, NY: Springer.

WACASER, A. J., & MAZZEO, J. C. (2007). *Can your business survive email? 21st Century Solutions for Today's Companies (whitepaper)*. StratAssemble.

WADLOW, T., & GORELIK, V. 2009. Security in the browser. *Queue, 7*, 40–41.

WEBSTER, J., & WATSON, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly, 26*, xiii-xxiii.

WEIPPL, E. R., & KLEMEN, M. (2005). Implementing IT security for small and medium enterprises. *Enterprise Information Systems Assurance and Systems Security: Managerial and Technical Issues*, 112–130.

WERLINGER, R., HAWKEY, K., & BEZNOSOV, K. (2008). Human, organizational and technological challenges of implementing it security in organizations. *Human Aspects of Information Security and Assurance (HAISA) 2008* (pp. 1–10). Plymouth, England.

WEST, R. (2008). The psychology of security. *Commun. ACM, 51*, 34–40.

WHITEHOUSE. (n.d). *Transnational Organized Crime: A Growing Threat to National and International Security* [Online]. Available: http://www.whitehouse.gov/administration/eop/nsc/transnational-crime/threat. [Accessed 10 June 2012].

WHITMAN, M. E., & MATTORD, H. J. (2004). Making users mindful of IT security; awareness training is vital to keeping the idea of IT security uppermost in employees' minds, *Security Management*, *48*(11), 32–34.

WHITMAN, M. E., & MATTORD, H. J. (2003). *Principles of information security*. Canada: Course Technology.

WHITMAN, M. E., & MATTORD, H. J. (2010). *Management of information security.* Canada: Course Technology/Cengage Learning.

WHITMAN, M. E., & MATTORD, H. J. (2012). *Principles of information security*. Canada: Course Technology/Cengage Learning.

WHITMAN, M. E., MATTORD, H. J., & GREEN, A. (2012). *Guide to firewalls & VPNs*, Canada, Course Technology/Cengage Learning.

WIPAWAYANGKOOL, K. (2009). Security awareness and security training: An attitudinal perspective. *SWDSI*, 266–273.

WORKMAN, M., BOMMER, W., & STRAUB, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*.

WU, M., MILLER, R. C., & GARFINKEL, S. L. (2006). Do security toolbars actually prevent phishing attacks? *Proceedings of the SIGCHI conference on Human Factors in computing systems.* Montreal, Quebec, Canada: ACM.

YUE, C., & WANG, H. (2008). Anti-phishing in offense and defense. *2008 Annual Computer Security Applications Conference.* IEEE Computer Society.

YUE, C., & WANG, H. (2010). BogusBiter: A transparent protection against phishing attacks. *ACM Trans. Internet Technol., 10*, 1–31.

APPENDICES

Appendix A: Example of Information Security Training Programme

This appendix provides an example of an information security training programme overview aimed at addressing phishing. This programme is divided into two phases: the first phase is theoretical, focusing on explaining information security terms and threats, while the second focuses on giving employees the skills needed to use technology correctly to combat phishing attacks. The contents indicated in bold are the training components necessary to educate users on phishing.

Appendix B: Semi-structured Interview Guide

This appendix contains the interview guide that was used in the interview process. Individuals responsible for information security at three organisations were interviewed.

Appendix C: Published and Presented Conference Papers

Peer-reviewed conference papers related to the study that were published and presented are provided in this appendix and is described further below:

Published Paper 1

Frauenstein, E.D. & Von Solms, R. 2009. **Phishing: How an organization can protect itself.** In: *Proceedings of Information Security South Africa (ISSA)* conference held at University of Johannesburg (UJ), South Africa from 06-08 July 2009, pp. 253-268 (ISBN: 978-1-86854-740-1).

Published Paper 2

Frauenstein, E.D. & Von Solms, R. 2011. **An Enterprise Anti-Phishing Framework.** In: *Proceedings of the 7th World Conference on Information Security Education (IFIP WISE7 TC11.8),* conference held at Lucerne, Switzerland, 09–10 June 2011, pp. 80-88 (ISBN: 1-933510-94-3).

Phase 1: Information Security & Security Threats Training

1. Importance of information

Types of information (information assets: personal records, organisational records)

The purposes for which information can be used by threat agents

2. Information security

What is information security?

Confidentiality, integrity and availability (CIA)

How can information be protected? (human factors, organisational aspects, technological controls)

Examples of organisations that have fallen victim to threats

3. Types of security threats

Humans

Cyber criminals (spammers, fraudsters, crackers, hackers)

Outsiders

Employees/insiders

Terrorists

Social engineers (phishers)

Environmental hazards

Fires, floods, earthquakes

Technological failures (hard drive crash, voltage surge)

4. Activities carried out by threat agents

Spyware, malware and worms

Cybercrime (Web forgery, identity theft, fraud)

Denial of service attacks (DoS)

Website defacing

Unauthorised system intrusions (hacking)

Social engineering techniques

Email attacks

Malicious programs (viruses, spyware, key loggers, Trojans)

Unsolicited mail (spam)

Phishing

5. Phishing education

APPENDIX A: EXAMPLE OF INFORMATION SECURITY TRAINING PROGRAM

Identifying a phishing email

Email address structure

Message contents (fabricated story, attachments, HTML images, and hyperlinks)

Identifying a spoofed website

Security indicators: padlock icon, URL structure, browser warnings

Ten Phishing Best Practices

Phase 2: Technological Controls Used To Combat Phishing Attacks

1. The role technology plays in our lives today
2. Can technology be useful and easy to use?
3. **Technological controls used to combat phishing threats**
    - **3.1 Email client**
        - Terms and concepts
        - Blocking phishing emails
        - Encrypting email messages
    - **3.2 Web browser**
        - Choosing a web browser
        - Terms and concepts: filters, ActiveX, cookies, add-ons/ plug-ins, cache memory, advertisements etc.
        - Browser plug-ins
            - Pop-up blocker
            - Phishing filters
        - Responding to phishing warnings, pop-up blocking
        - Deleting browser history, temporary Internet files, cookies, cache memory
        - Encryption (SSL)
    - **3.3 Anti-virus programs**
        - Scanning files, folders, web links and storage devices
        - Shield types
        - Program and virus definition updates
        - Responding to virus warning alerts
    - **3.4 Software updates**
        - Application software and operating system updates
    - 3.5 Password managers

INTERVIEW GUIDE

The objective of this interview is to evaluate the components of the anti-phishing framework created as a result of the literature studied. The purpose of the interview is not to analyse the phishing experiences in terms of your current organisation, but rather to obtain your opinions and recommendations based on your work experience and knowledge.

Phishing is the act of attempting to acquire personal information, such as usernames, passwords, and credit card details, by means of deception by disguising the phishing attacker as a trustworthy entity in email. These emails contain links that direct the user to a website which looks identical to the original website. The user unsuspectingly enters their credentials which are captured by the phisher. Phishing emails are effective because they make use of social engineering techniques to target weak human behaviour and emotions.

1. After explaining human factors, organisational aspects and technological controls in the context of phishing, do you agree that these HOT dimensions should be considered as the three **main** areas in an anti-phishing framework?

2. Do you agree, from the diagram provided, that each of these three dimensions is evidently operating in isolation, thus forming only a single-layer defence against phishing?

3. Do you agree that each of these three dimensions have the common element of human involvement?

4. From this human involvement, three linkages can be established between the dimensions namely: HT, OT and HO. In this regard, do you agree that security awareness, training and education programmes are core to strengthening **each** of these linkages in order to form a holistic model?

5. Having established these linkages, theories and best practices were identified relating to each of these linkages. These theories and best practices helped in understanding the variables involved in each of these linkages. The Technology Acceptance Model (TAM) is concerned with two factors related to the way humans perceive technology:

- **easy** to use
- **useful** in its purpose.

As such, do you agree that the TAM would serve as the most appropriate linkage between humans and technology?

6. Having understood the brief description of the TAM, do you agree with the following training requirements for the HT linkage:

- End-users should be competent and be trained by the organisation in using a computer system correctly, i.e. computer literacy training.
- End-users should be given information security training focusing particularly how to use technology, such as the email client, web browser and anti-virus programs, to combat phishing threats.
- Technical staff should receive specialised training in configuring and managing the relevant technological controls for the organisation
- Top management should receive the same training as end-users.

7. Do you feel that, after such training, all users will perceive technology as being easy to use and useful for accomplishing their task?

8. Agency theory is concerned with the variables affecting the relationship between management and employees. Agency theory is concerned with resolving two problems:

- The **conflicting** desires or goals of the principal and agent

- **Verification** of the agent's activities is too difficult or expensive for the principal.

As such, do you agree that agency theory would serve as the most appropriate linkage between the organisation and the human dimension?

9. Do you agree that organisational policies and procedures comprise the main component needed to addresses the H and O linkage?

10. How do you think organisational policies and procedures should be communicated to employees? Through awareness and/or actual training?

11. Do you think this would be sufficient to change their behaviour? If not, what would you suggest to improve this?

12. Looking at the CobiT guidelines (provided), which of the following do you feel is the most appropriate linkage for the O and T dimension, also considering phishing?

13. Do you agree that the CobiT guideline of **'ensuring systems security'** is the most appropriate linkage between the O and T dimension?

14. How do you feel this guideline could be addressed through a security awareness, training and education programme?

15. Where do you think organisations' application of best practices (e.g. ISO 27002) should be featured in the anti-phishing framework?

16. Can you identify any other components that should be considered in the anti-phishing framework?

PHISHING: HOW AN ORGANISATION CAN PROTECT ITSELF

Edwin Donald Frauenstein[1] and Rossouw von Solms[2]

[1,2]Nelson Mandela Metropolitan University, South Africa

efrauenstein@wsu.ac.za[1], rossouw@nmmu.ac.za[2]

ABSTRACT

The objective of this paper is to report on research to construct a model, which should provide guidance to an organization on how to address all dimensions associated with phishing and assist in solving the problem holistically. The emphasis will be placed on the human and organizational dimensions. Most research in this area has shown that only certain dimensions used to combat phishing attacks, in an organization, are addressed in isolation and not holistically. Anti-phishing research literature studied has either focused on algorithms for detecting phishing attacks in web browsers (Egelman, 2008; Fette, 2007; Garera, 2007; Patel, 2007) or on evaluating the user interfaces of anti-phishing web browser toolbars (Wu, 2006). From research studied, there has been little work conducted on preventing users from falling for phishing email messages. It has been proven that phishing does indeed pose an ongoing threat to an organization through its employees. Therefore, a suitable solution to this problem should be devised. This paper attempts to present such a holistic solution in the form of a model.

KEY WORDS

Phishing, social engineering, information security model, e-mail scams, spoof-websites

PHISHING: HOW AN ORGANIZATION CAN PROTECT ITSELF

1. INTRODUCTION

Information in the modern electronic world can be viewed as the most important asset in a global market. Individuals, businesses, organizations and governments depend on information to be embedded in secure, private and trustworthy IT infrastructures (http://www.thedacs.com/techs/enhanced_life_cycles/). Individuals within an organizational environment often tend to rely on an organization to take responsibility and have these well defined controls to protect the integrity and availability (ICT Standards Board, 2007) of their personal data from unauthorized access, use, disclosure, disruption, modification or destruction (IBM Business Consulting Services, 2006). However, these controls alone cannot avert information security threats. An alternative technique of gaining unauthorized access of information, apart from the common procedure of hacking, is *Phishing*.

The objective of this paper is to report on research to construct a model, which should provide guidance to an organization on how to include all dimensions associated with phishing and assist in solving the problem holistically. The emphasis will be placed on the human and organizational dimensions. This paper also addresses, from research studied, the problems that phishing poses to individuals and organizations (Orgill, 2004).

2. BACKGROUND TO THE PROBLEM OF PHISHING

There is much evidence in literature that proves that phishing is a growing problem in the current global industry and poses an ongoing threat that may affect every individual in an organization (Ohaya, 2006; Orgill, 2004; Safecode, 2008; Threat Insight Quarterly, 2005). Phishing is a social engineering technique through which an individual attempts to solicit and steal confidential information from a user or employee by masquerading as a legitimate entity (Kumaraguru, 2007). Today, phishing has become much more sophisticated in techniques using technology, advantageously, as a tool through a combination of spoofed emails, Internet Relay Chat (IRC) and instant messages to lure individuals (Ohaya, 2006).

Since most organizations are conducting business transactions through the Internet, IT is rapidly changing the world through information and communication technology (Alkadi, 2004). Today most communication occurs through electronic mail. According to Badra (2007), there are many various forms of phishing attacks however, common phishing schemes mostly use spoofed e-mails to lure users to fake websites designed to capture the sensitive information (Ohaya, 2006). The spoofed- email normally tends to have a slightly threatening message or tone to increase the effectiveness of luring the victim to avoid any further consequence. An example of this could be that the user's bank account details would be terminated if failing to respond. Phishing is not only based on obtaining user account details, but includes access to all personal and financial data. When individuals respond to such messages, they are putting themselves and their respective organizations at risk. This is caused primarily due to a lack of knowledge in information security protocols and carelessness regarding the consequences which may follow.

Recently, social attraction networks (e.g. MySpace, Facebook and Friendster) have gained popularity in phishing attacks (Brown, 2008; Unisys, 2008) and are being used as sources to lure individuals to give out their personal information. The latter substantiates the point that

threats are constantly finding new weaknesses in technology and using more sophisticated techniques to gain entry through this modern, technological age (Orgill, 2004). Since people can be considered to be the weakest link in a very technologically secure computing environment (according to current standards), they are consequently targeted by social engineering attacks (Orgill, 2004). Much emphasis is placed on making computer systems more secure (technology aspect) and thus, the human element is often forgotten, ignored or neglected. Each new threat adds to the difficulty of securing an information system. The attacker does not have to have any prior knowledge into hacking systems to understand and use social engineering techniques. Human emotion and manipulation are used to trick victims into giving up personal information. The social engineer attempts to exploit the natural desires of humans to trust others and strangers, to assist in other's labours and to gain favor in their eyes (Orgill, 2004). PayPal, eBay, American Online and the South African Revenue Services (SARS) are well known examples of organizations that have all claimed victim to having been financially affected by phishing attacks (http://www.sars.gov.za/home.asp?pid=42736).

People and organizations, especially in a South African context, may not be aware of the dangers that phishing presents or how to detect these threats. This is indeed the case, even though much literary sources educate users on how to effectively identify these threats (Fette, 2007; Garera, 2007; Patel, 2007). People seem too dependant on IT systems to manage security concerns. This lack in responsibility exposes this weakest link, the human factor (Orgill, 2004; Patrick, 2005; Robila, 2006).

3. CURRENT PROTECTION MEASURES IN ORGANIZATIONS

Organizations can effectively manage and protect their information from unauthorized access, by following the internationally accepted and recognized Code of Practice for Information Security Management i.e. ISO 27002 (http://www.iso27001security.com/html/27002.html). This international standard is but one 'best practice' that provides recommendations in terms of what companies should implement to protect their information assets. The standard also addresses many issues and concerns relating to information security. Applying only an international standard may not be adequate as even these generally accepted Information Security (IS) standards and best practices do not effectively address the Social Engineering aspect of Information Security defences and may leave gaps for phishing attacks. The document does not particularly focus on the term "phishing" attacks but does indeed mention that it is a problem. However, it merely gives general guidelines that one shouldn't exchange information with unknown parties or open emails from unknown sources etc. The fact that emails appear to be from a legitimate source is what allows phishing attacks to be so effective. The email seems relevant in context and seems legitimate, in design, to the individual (Egelman, 2008). The latter is regarded as a spear phishing attack (Microsoft, 2005). Therefore, spear phishing attacks have the potential to pass through strong company regulations and seemingly secure technology controls, relying mostly on the human element for protection (Orgill, 2004).

There are many reasons why individuals fall susceptible to phishing attacks. According to Ohaya (2006) some of the reasons include a lack of knowledge of computer systems, lack of security and security indicators, lack of attention to the security indicators, lack of attention to the absence of security indicators, and the sophistication of spoofed sites seem to be the greatest threat. If the site looks authentic, users have confidence in it as they could not tell the difference between a genuine or spoofed web-site. Ohaya (2006) states further that security

managers should take the following steps to protect the organization and employees from phishing attacks:

> 1. "Ensure privacy and security are perceived at a macro level in the organization.
> 2. Create security policies, standards, and procedures that are part of an ongoing overall security management framework
> 3. Ensure that all employees in the organization have security education, training and awareness about phishing and other threats in addition to following security policies and procedures."

Orgill (2004) substantiates this in stating that employee education should cover the company's strong policy statements, including penalties for non-compliance. In fact, researchers (Ohaya, 2006; Orgill, 2004; Robila, 2006) have shown that user education is the most important aspect of preventing phishing attacks. Kumaraguru (2007) designed and evaluated an embedded training email system that teaches people the dangers of phishing during their normal use of email as he feels that people simply ignore security notices and warnings. Sheng (2007) developed a game that teaches people not to fall for phishing, thus getting them more interested in the fun educational aspect. According to Badra (2007), reducing the phishing threat can be achieved if a given solution could meet the following functions: monitoring potentially malicious activity, authenticating email messages, detecting unauthorized use of trademarks or logos or other proprietary imagery, improving the security patching infrastructure to increase resistance to malware, using personalized information to authenticate an email directly to a user and detecting a fraudulent web site and alerting the user.

According to O'Brien (2000) there are 3 major types of controls that must be developed to ensure the quality and security of information systems

- **Information System controls** (input, processing, output and storage controls)
- **Procedural Controls** (standard procedures, documentation, authorization requirements, auditing)
- **Facility Controls** (physical protection, computer failure controls, network security and biometric controls).

These above-mentioned controls merely focus on the management aspect of the information system in relation to normal everyday conditions of business transactions, specifically the input, processing, output and storage activities in an information system. This approach focuses more on the technological and organizational measures in place rather than an unforeseen human error. It does not encompass provisions for the idiosyncratic nature of the human element, especially within a social context. Phishing has few technical boundaries. Its strength lies in its ability to trick any individual irrespective of experience, knowledge or position in the organization. This method of acquiring sensitive information from the individual could then lead to the entire organization's confidentiality or individual's personal information being put at risk.

While technology is important, organizational and human factors also play a crucial role in achieving information security (Dutta, 2008). These dimensions should play a role in constructing a holistic approach to protect information assets against phishing attacks. The ***technological*** dimensions would typically involve anti-phishing software, spam filters, firewall etc. The ***human*** dimension calls for effective awareness and education to assist in strengthening the 'human firewall' and to ideally cultivate a culture of information security

behavior. On the other hand, sound ***organizational*** measures, e.g. policies and procedures, need to be in place to put everything into perspective. Of these dimensions, the human factor is probably the most important since this is the area that phishing exposes the most. Research suggests that if human behavioral response can be understood, then one may have a solution to the issue of why people fall susceptible to phishing attacks (Downs, 2007). Information Security should not be regarded as a technical issue but rather a multi-dimensional issue. Therefore is a need for all of these dimensions to be considered. In doing so, this should provide for adequate overall risk mitigation against phishing attacks.

Below are main components that will be addressed in the anti-phishing model and recommendations for each of these components:

International Standards, Guidelines and Best Practices: As mentioned**,** numerous international standards, best practices and guidelines refer to the effective protection of information assets, e.g. ISO 27002 (http://www.iso27001security.com/html/27002.html), COBIT (COBIT, 2000), the King II Report (King Report, 2001), etc. Such standards, best practices and guidelines should play an integral role in the eventual plan to protect organizational information assets against phishing attacks.

Technology Controls: As earlier discussed in this paper, threats are finding new weaknesses in technology. Therefore it is considered a dimension that compromises the integrity of an organization's information security. It is important to address its role in the model. Phishing attacks can breach a weak technological barrier. The "phisher" may rely on the individual or organization to have an outdated or ineffective web browser, outdated anti-virus program due to poor organization policies. The phisher may lure individuals through websites like Facebook, Twitter etc. The use of IRC and Instant messengers are a new breeding ground for phishing attacks. Most organizations should have anti-virus programs installed. However, an effective anti-virus program is only as good as the currency of its virus definition updates that it receives. Besides its primary function of scanning for virus signatures, some anti-virus programs can also detect most phishing websites (http://anti-virus-tools.software.informer.com/). The anti-virus program can also remove key-logger Trojans- a virus designed by 'phishers' to monitor keystrokes from the keyboard.

Organizations use firewalls, in a network environment, to filter incoming emails as well as to block unauthorized entry from outsiders. If properly defined through procedures, the firewall also prevents employees from accessing illegal or unwanted websites, in this regard phishing websites.
(http://www.security-forums.com/viewtopic.php?p=5787&id=db1bca5dcddd4bff0
5dd056501b7e922).

The internet web browser also forms an important role, in security, in having the built-in capacity to identify spoofed websites. Common web browsers such as Microsoft Internet Explorer 7, Opera 9.5, Firefox 3, and Safari 3.2 etc. can detect most phishing websites. However, each reacts differently to suspicious spoofed-websites in the manner it displays active phishing warnings to the user (Egelman, 2008). This presents a problem in the sense that it may confuse the individual when presented with such a warning. An organizational standard should be set as to identify which browser would best be suited in such a case of an individual falling susceptible to a phishing website.

The operating system (e.g. Windows XP, Windows Vista, etc.) should be regularly updated for software enhancements (updates, patches, hot-fixes etc.) either automatically or by relevant staff. Failure to do so creates an opportunity for viruses to either pose as an application or as a warning notification thus luring the victim to submit confidential information. The latter is another technique of phishing that acquires personal information(http://computing.vassar.edu/safecomputing/security/ospatch.html). Phishing attacks can also be in the form of malicious code-based or Trojan-based attacks, in which malicious software causes data compromises (Badra, 2007)

Technological aspects form an imperative part in the eventual anti-phishing model. Clear guidelines need to be provided as to which controls should be implemented in this regard.

Organizational Aspects: Human Resource related aspects play a major role in the recruitment of skilled and trustworthy staff. This can be done through effective screening etc. Newly appointed staff must be made aware of company policies and procedures. This can be defined in a policy document by the organization requiring employees to sign upon appointment. Failure to comply with these procedures should result in penalties by the staff member. Some of these policies may have a relationship with technology aspects e.g. do not install pirated software, individuals must encrypt sensitive files when emailing clients, software updates must be done regularly by IT staff, downloading of files not relative to organization needs is not permitted etc. The organization needs to adopt an information security culture. The organization needs to realize the importance of strengthening and securing their information, and lead the way in ensuring that future security threats are prevented and controlled. This can be done through effective physical and software procedures. It is critically important that the organization should ensure that proper policies, regarding protection against phishing attacks, are defined and that sound procedures are put in place. Once in place, this will then have an effect on the technological aspects and human aspects.

Human Factors: As mentioned throughout this paper, the weakest target phishing attacks focus on is through the human aspect. Through education, employees can be made more aware of the activities involved in a phishing attack (van der Merwe, 2005) and how it may affect them and the organization. This can be done through regular training workshops. The training needs to have some incentive or humour in gaining effective participation from its employees. The training should also give relevant examples in context of daily issues that plague employees in the organization, specifically in emails from unknown sources. The latter should address how to identify these threats and what procedures to follow. An added benefit, through training, allows employees to also learn of other current and future threats of information security aspects instead of phishing attacks alone. According to van der Merwe (2005), there are five issues that a company or individual should be aware of in phishing: education, preparation, avoidance, intervention and treatment. All of the latter issues have been considered and addressed in the proposed model.

As previously mentioned, three very important dimensions should form part of the protection model against phishing attacks. These are; technological, organizational and human related dimensions. These dimensions should be governed by applicable international standards, guidelines and best practices. Below, figure 1, graphically represents the anti-phishing model with the above-mentioned dimensions to be considered in protecting company information assets from phishing attacks.

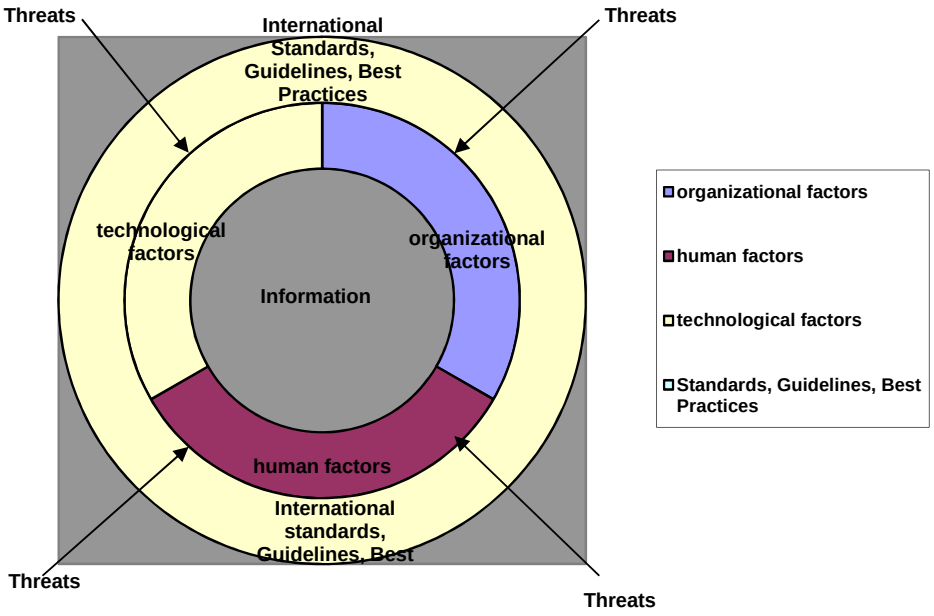


Figure 1: The anti-phishing model highlights major aspects, in an organization, that must be considered to form a complete barrier of defense against phishing attacks

4. CONTRIBUTION OF THE STUDY AND FURTHER RESEARCH

The proposed solution will be refined and tested, using design science, through further literature studies as well as a case study in an organization to determine its effectiveness. Sound methodologies will also be utilized to ensure that the model is developed with rigor to result in a trustworthy artifact. Of the three dimensions, through research studied, the human dimension has been established to be the weakest aspect in which phishing threats breach information security.

The detailed, eventual, model will help make an organization more aware of the dangers of phishing and educate them to prevent phishing attacks by addressing all dimensions required.

5. CONCLUSION

As more organizations provide greater online access for their customers, phishers are successfully using more social engineering techniques to steal personal information and conduct identity theft at a global scale. By understanding the tools and technologies that phishers use, organizations and their customers can take a proactive approach in defending themselves against future phishing attacks. To make this possible, it is imperative that organizations and its employees, across the entire organization, be properly educated about the dangers of phishing thus addressing the human dimension. It must be understood that all dimensions, as a whole, should be considered in the model and not just one in isolation. This will form a complete barrier against phishing attacks. Although an organisation may have well defined policies and procedures that employees could read and sign every year, it has proven to be insufficient (Gragg, 2002). The latter can be due to large amounts of policy documentation that employees aren't keen to read and consequently merely signing it. Given a predicted increase in tools available to fight phishing, it is expected that future attacks will

continue to be more refined in terms of targeting the user and even specificity (Robila, 2006). The latter such case of an employee within the organization attempting to acquire information illegally through another employee is known as spear phishing. Therefore, the proposed solution to this problem needs to be designed through an effective, rigorous model.

6. REFERENCES

Alkadi, I and Alkadi, G, (2004). '*Information technology in the business world through the years and beyond!'*, Journal of Academy of Business and Economics

Badra, M., E-L Sawda, S., Hajjeh, I, (2007). '*Phishing Attacks and Solutions'*, ACM International conference proceedings of the 3rd International conference on mobile multimedia communications, vol. 329, ICST (Institute for Computer sciences, social-informatics and telecommunications engineering, Nafpaktos, Greece

Brown, G., Howe, T., Ihbe, M., Prakash, A. and Borders, K. (2008). ' *Social Networks and context-aware spam*', Proceedings of the ACM 2008 conference on computer supported cooperative work, ACM, San Diego, CA, USA, pp. 403-412
COBIT (2000), '*Control Objectives for information and related technologies'* (COBIT), 3rd Edition, IT Governance Institute, USA, 2000

Downs, J.S., Holbrook, M. and Cranor, L.F (2007). '*Behavioral response to phishing risk*,' ACM International Conference Proceeding series, vol. 269, ACM, Pittsburgh, Pennsylvania, pp. 37-44

Dutta, A., Roy, R. (2008). '*Dynamics of organizational information security'*, System Dynamics Review, vol.24, Issue 3.,Wiley Interscience, Accessed 14 April 2009, http://www3.interscience.wiley.com/journal/121518999/abstract?CRETRY=1&SRETRY=0

Egelman, S., Cranor, L.F. and Hong, J. (2008). '*You've Been Warned: An Empirical study of the effectiveness of web browser phishing warnings'*, Conference on Human Factors in computing systems-Proceedings of the 26th annual SIGCHI conference on Human factors in computer systems, ACM, Florence, Italy, pp. 1065-1074

Enhancing the development life cycle to produce secure software (2008), Retrieved 28 May 2009 from http://www.thedacs.com/techs/enhanced_life_cycles/

Fette, I., Sadeh, N. and Tomasic, A. (2007). ' *Learning to detect phishing emails'*, Proceedings of the 16th International conference on World Wide Web, ACM, Banff, Alberta, Canada, pp 649-656

Garera, S., Provos, N., Chew, M. and Rubin, A.D (2007). ' *A framework for detection and measurement of phishing attacks*', Proceedings of the ACM workshop on recurring malcode, ACM, Alexandria, Virginia, USA, pp. 1-8

Gragg, D. (2002). '*A multi-level defense against social engineering'*, SANS Institute InfoSec Reading Room, Accessed on 3 April 2009, http://www.sans.org/rr/papers/51/920.pdf

How to keep your computer's operating system and programs up-to-date. Retrieved 17 April 2009 from http://computing.vassar.edu/safecomputing/security/ospatch.html

IBM Business Consulting Services (2006). '*Federal Information Security Management Act (FISMA) Compliance Solution- Improving management, operational, and technical controls over information, personnel, and physical security and privacy*', USA, Accessed on 14th April 2009, http://www-03.ibm.com/industries/global/files/FISMA_Cutsheet_PS_0306.pdf

ICT Standards Board (2007). '*Network and Information Security Standards Report'*, Issue 6.2, Accessed on 17th April 2009, http://www.cen.eu/CENORM/BusinessDomains/businessdomains/isss/activity/nisfinalreport.pdf

ISO/IEC 27002:2005 Information technology -- Security techniques -- Code of Practice for Information Security Management. Retrieved 14 April 2009 from http://www.iso27001security.com/html/27002.html

King Report (2001). '*King Report on Corporate Governance for South Africa 2001'*, Accessed on 17 April 2009, http://general.uj.ac.za/infosci/scipsa/king-report-on-corp-gov.pdf

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L.F., Hong, J. and Nunge, E. (2007). *'Protecting people from phishing: The design and evaluation of an embedded training email system'*, Proceedings of the SIGCHI conference on human factors in computing systems, ACM, San Jose, California, USA, pp. 905-914

Microsoft (2008). '*What is spear phishing?-Help prevent identity theft from new targeted phishing scams'*, Accessed on 10 April 2009, http://www.microsoft.com/canada/athome/security/email/spear_phishing.mspx

O' Brien, J. (2000). *'Introduction to Information Systems-Essentials for the internetworked Enterprise*, ninth international edition, Irwin/McGraw Hill, United States

Ohaya, C. (2006). '*Managing Phishing threats in an organization*', Information Security Curriculum Development Conference, Proceedings of the 3rd annual conference on Information security curriculum development, ACM, Kennesaw, Georgia, pp 159-161

Orgill, G.L., Romney, G.W., Bailey, M.G and Orgill, P.M (2004). '*The Urgency for Effective User Privacy-education to Counter Social Engineering Attacks on Secure Computer Systems*', Information Technology Education (Formerly CITC), ACM, New York, USA, Salt Lake City, UT, USA, pp. 177-181

Patel, D. and Luo, X. (2007). ' *Take a close look at phishing'*, Information Security Curriculum Development Conference'07, Proceedings of the 4th annual conference on Information security curriculum development, ACM, Kennesaw, Georgia, USA

Patrick, A., Marsh, S. and Briggs, P. (2005). '*Designing systems that people will trust'*, National Research Council Canada, Accessed on 14th April 2009, http://www.iit-iti.nrc-cnrc.gc.ca/publications/nrc-47438_e.html

Robila, S.A and Ragucci, J.W. (2006). *'Don't be a phish: Steps in user education'*, Annual Joint Conference Integrating Technology into Computer Science Education, Proceedings of the 11th annual SIGCSE conference on Innovation and technology in computer science education, ACM, Bologna, Italy, pp. 237-241

Safecode (2008). '*Software Assurance: An Overview of Current Industry Best Practices'*, Accessed on 14th April 2009, http://www.safecode.org/publications/SAFECode_BestPractices0208.pdf

Security and Privacy / Anti-virus Tools at Software Informer. Retrieved 17 April 2009 from http://anti-virus-tools.software.informer.com

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L.F., Hong, J. and Nunge, E. (2007). '*Anti-phishing Phil: The design and evaluation of a game that teaches people not to fall for phish'*, Proceedings of the 3rd symposium on usable privacy and security, vol.229, ACM, Pittsburgh, Pennsylvania, pp. 88-99

South African Revenue Services – SARS Phishing Attack. Retrieved 14 April 2009 from http://www.sars.gov.za/home.asp?pid=42736

Threat Insight Quarterly (2005). '*Phishing and other significant threats of 2004'*, Internet Security Systems, Accessed 14 April 2009, http://documents.iss.net/ThreatIQ/ISS_XFIQ0205.pdf

Unisys (2008). '*Unisys Identifies Five Security Issues Likely to Emerge Across Multiple Industries in 2008*', BusinessWire, Accessed on 14th April 2009, http://www.businesswire.com/portal/site/google/?ndmViewId=news_view&newsId=20080115005324&newsLang=en

van der Merwe, A., Loock, M. and Dabrowski, M. (2005). '*Characteristics and Responsibilities involved in a Phishing attack'*, ACM International Conference Proceeding Series; Vol. 92, ACM, Cape Town, South Africa, pp.249-254

Wang, A.J.A. (2005). *' Information Security Models and metrics'*, Proceedings of the 43rd annual south east regional ACM conference, vol.2, ACM, Kennesaw, Georgia, pp. 178-184

WindowSecurity.com Beyond the Firewall (White Paper). Retrieved 17 April 2009 from
http://www.security-forums.com/viewtopic.php?p=5787&sid=db1bca5dcddd4bff05dd056501b7e922

Wu, M., Miller, R.C. and Garfinkel, S.L. (2006). *'Do security toolbars actually prevent phishing attacks?'*, Proceedings of the SIGCHI conference on human factors in computing systems, ACM, Montreal, Quebec, Canada, pp. 601-610

An Enterprise Anti-Phishing Framework

Edwin Donald Frauenstein[1] and Rossouw von Solms[2]

[1]Walter Sisulu University, School of Computing, East London, South Africa
[2]Nelson Mandela Metropolitan University, School of ICT, Port Elizabeth, South Africa
{efrauenstein@wsu.ac.za[1], rossouw@nmmu.ac.za[2]}

Abstract. The objective of this paper is to report back on an organizational framework, which consisted of human, organization and technology (HOT) dimensions in holistically addressing aspects associated with phishing. Most anti-phishing literature studied either focused on technical controls or education in isolation however; education is core to all aspects in the above-mentioned framework. It is evident, from literature, that little work has been conducted on anti-phishing preventative measures in the context of organizations but rather from a personal user-level. In the framework, the emphasis is placed on the human factors in addressing phishing attacks.
Keywords: Information Security, social engineering, human factors, phishing, email scams, spam, spoofed-websites

Introduction

It is evident that as more organizations provide greater online access to their customers, phishers are successfully using social engineering techniques and technology advantageously to steal personal information and conduct identity theft on a global scale [20]. Organizations financial information is at risk, because most information-workers are vulnerable to social engineering techniques as the organizations possess financial information [29]. Fraudulent emails, such as phishing, can harm their victims as well as organizations resulting in financial losses, damaged reputation [27] and identity theft. Given a predicted increase in the tools available to fight phishing, it is expected that future attacks will continue to be more refined in targeting users i.e. spear phishing [24] incorporating greater elements of context to become more effective and thus more dangerous for society. Hence, by understanding the tools and technologies that phishers use, organizations, users and their customers can take a proactive approach in defending themselves against future phishing attacks [20]. Although this paper presents a holistic framework which requires all dimensions to be of key importance however, education is indeed a major component of protection against phishing. Thus, the objective of this paper is to emphasis how education, awareness and training are required to effectively strengthen the dependencies between the dimensions in the framework. The rest of the paper is structured as follows: In Section 2, we give a background of phishing and explain its effectiveness. In Section 3, we illustrate the need for a holistic framework. In Section 4, we demonstrate the anti-phishing framework focusing on human factors. Finally, conclusions are drawn in Section 5.

Phishing Explained

"Phishing" is a hacker's term that originated from fraudsters whom are "fishing" for confidential information, mostly conducted through using fake emails and spoofed websites acting as the "bait", and the victim's accounts as the netted "phish" [27]. Phishing is a component of social engineering through which an individual attempts to solicit and steal confidential information from a user or employee by masquerading as a legitimate entity, usually from well-known financial or e-commerce institutions [27] as the primary of objective is to fraudulently obtain money. PayPal™, eBay™, American Online™, ABSA™, Standard Bank™, Google™, Microsoft and the South African Revenue Services are a few popular cases of organizations, and its clients, that have financially been affected through phishing attacks. Although most cases are financial related, phishing includes unauthorized access to all types of data e.g. social security number. Besides email, there are a number of other phishing variations such as spear phishing, wi-phishing, vishing, baiting, whaling and pharming. Phishing techniques have become more sophisticated [27], making use of a range of modern technologies such as: Internet Relay Chat (IRC), instant messengers (IM's), social networking sites (e.g. Facebook, MySpace) [10],[17],[19] and Trojan horse [6],[27]. The effectiveness of using social engineering techniques do not require much prior technical knowledge or education into hacking information systems; instead human emotion, deceit and manipulation are tools used to trick victims into giving up their personal information.

From the description of phishing above, typically five main processes are used to carry out a phishing attack:

Planning: Phisher determines who and how to attack and the information to be obtained from the victim. According to Orgill [21], social engineering attacks usually entail two facets namely: the physical aspect (e.g. workplace, online) and the psychological aspect or a combination using both aspects to gain desired information.

Email Design: The illusion based by email appearance (e.g. email address structure, subject header and content), is made to appear more legitimate by using institution logos, terminology etc. to create authenticity in the mind of the victim.

Fabricated Story: Is used to gain the victims attention, supposedly in their best interest, that a problem exists e.g. customer accounts has been hijacked. The email can also perceive to have a friendly tone e.g. thanking you for your co-operation. Using reverse social engineering, before the problem is resolved, the target feels indebted to the attacker.

Threatening Tone or Consequence: The user is lured by the fake warning and enticed to click on a hyperlink which is usually disguised as text or an image e.g. Click here for verification. The tone, together with reverse psychology, is used e.g. the user fears that if they choose not to verify, consequently result in their account being automatically deleted. Ironically, it is "human nature" not to want any further undesired consequences or hassles e.g. renewing accounts etc.

Spoofed-Website: After the user selects/clicks the hyperlink embedded within the email message, they are directed to a spoofed-website which also appears authentic and legitimate in design, and subsequently the victims personal details are captured unsuspectingly.

The Need for a Holistic Anti-Phishing Framework

Organizations are at risk caused through their employees' actions and behavior [28]. If human behavior could be understood, one may suitably address why humans fall for victim to phishing emails [1],[5]. According to Hinson [13], it can be argued that technical flaws themselves are the product of human errors. Even so, companies concerned with information and data security are increasingly dedicating more *technological* resources to evaluate and protect their information systems [13] thus ignoring employees as the source of their most prevalent exposure. It is often easier for attackers to exploit human and social weaknesses of the defences than to defeat the technological countermeasures [18]. This is also evident in anti-phishing literature as most research focused on technical solutions such as: developing browser toolbars/plug-ins [23] preventative measures, characteristics and email structure [6],[20],[22], algorithms for detecting, identifying and measuring phishing emails and sites [8],[11],[32] and evaluating the effectiveness of web browser toolbar warnings/indicators [4],[7],[12],[31]. Many employees cannot identify the difference between a genuine and a spoofed website [4],[21]. Furthermore, many users are too preoccupied with their primary work duties that they hardly remember to pay attention for web browser security indicators [19]. Information security is far more than applying a range of physical and technical controls [13] and technically knowledgeable specialists often make the mistake of believing that technical measures succeed in protecting them and average consumers [14]. Social engineering attacks and lack of compliance of organizational security policies are increasingly cited as security concerns. Technical solutions are only as good as the people that use and operate them because information security is a multi-dimensional issue and only be achieved if a holistic approach is taken [3].

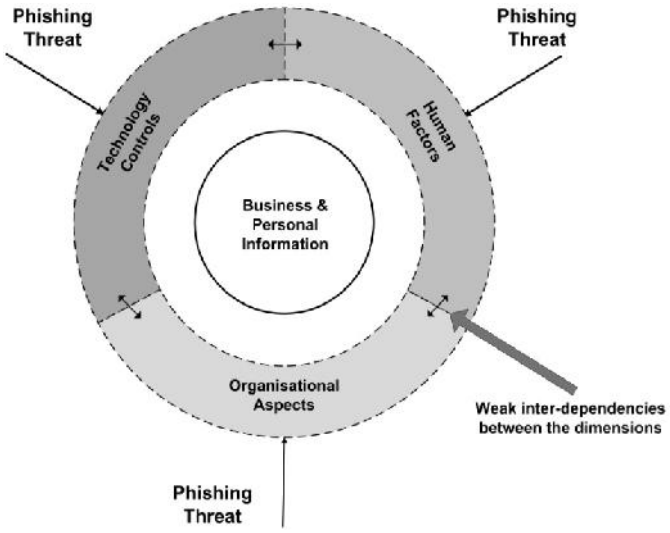


Fig. 1. Organizational dimensions targeted by phishing

Generally information security threats exploit human behavior and thus, in an organizational context, require a framework consisting of human, organizational and technological dimensions (HOT) to address against such threats [9]. Illustrated in Fig 1, HOT dimensions are operating in isolation of one another *(dotted lines)*, caused from limited communication and interaction between each of them thus forming only a 'single layer' oriented defense. As a result, if one of the dimensions is weakened, phishing attacks may proliferate compromising the other dimensions respectively. Ideally, it is suitable to move towards an 'in-depth' defense oriented model (see Fig. 2), thus allowing several barriers to serve a defense.

Anti-Phishing Framework: Phishing for a Solution

Technology controls have proven to be inadequate in protecting against phishing especially when applied in isolation of other organizational aspects. While technology is important, organizational and human factors also form a crucial role in achieving information security [1]. Understanding of how different human, organizational, and technological elements interplay could explain how different factors lead to sources of security breaches and vulnerabilities within organizations [15],[30]. Since each dimension has human involvement, even if the organizational dimension is added, protection may not be sufficient as both the organizational and technology dimensions depend on the H dimension. In the organizational dimension, best practices, policies, procedures and international standards (e.g. ISO 27002, King III, COBIT 4.0); fully depend on humans obeying them. Furthermore, they need to be in place to guide the other dimensions. Technology dimensions would typically involve any technical controls such as: anti-phishing browser plug-ins, anti-virus software, spam filters, web browsers, network firewalls, etc. and is dependent on humans to follow the procedures to ensure the technical controls are functioning and applied correctly. The human dimension calls for effective *awareness*, *education* and *training* to assist in strengthening the 'human firewall' and to ideally cultivate information security behavior in the organization. Of these dimensions, the human dimension is the area that phishing exposes the most and as a result, compromises the technology and organizational dimensions. Thus, there is a need for the education element to be present in *all* of the above-mentioned dimensions to ensure that all HOT dimensions are functioning optimally. In doing so, this should provide for adequate overall risk mitigation against phishing attacks (see Fig.2). Further research will validate these findings through an expert review.

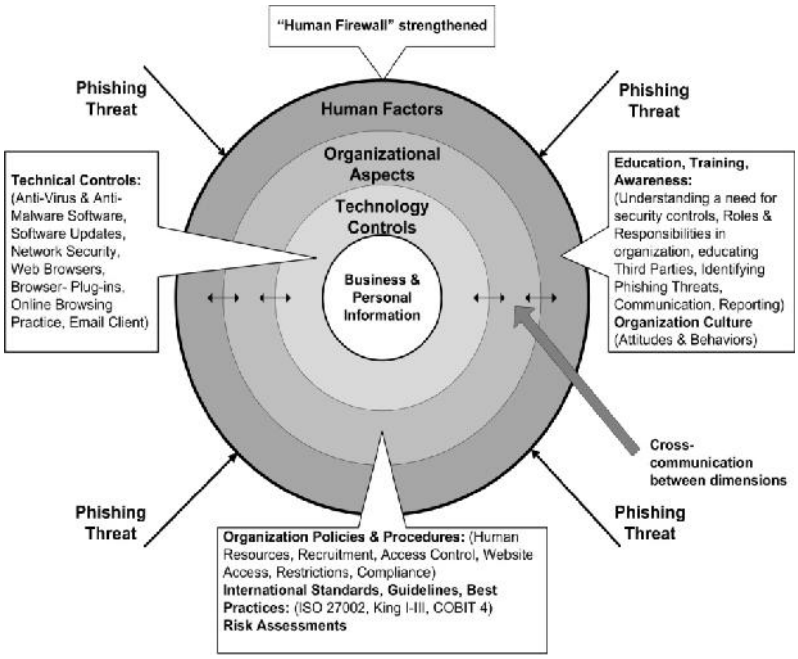


Fig. 2. Aspects in an organization, holistically related to an anti-phishing framework

Illustrated in Fig 2, continual communication *(concentric circles & arrows)* between the HOT dimensions serves a stronger defense. The human dimension is the entry point for phishing attacks and the common link (the glue) which influences all the other dimensions. It requires education to strengthen the interdependencies between the other areas e.g. staff must be knowledgeable enough of policies and technical aspects to ensure that operational procedures are obeyed and implemented correctly. The following section focuses on the components required to address the human factor dimension.

Information Security Management & Culture: Information security management requires, as a minimum, participation by all employees, shareholders, suppliers, third parties, customers or other external parties [25]. It is the responsibility of all employees to protect information thus defending the reputation and financial well-being of the business [2]. Effective interactions and communications are required to reach a mutual understanding about security risks among different stakeholders [30]. An information security culture needs to be adopted to ensure that information security becomes a natural aspect in the daily practice of every employee.

Educate Staff in Recognizing Phishing Emails and other Online Threats: Staff security education and training is one of the most important aspects of an organizations security posture and perhaps the greatest non-technical measure available and cost-effective solution for human factors and security [2]. Security topics and requirements need to be integrated into normal business behaviour, through clear policy and staff education [2]. Through a regular and comprehensive user education programme, staff can resist and be made more aware of the design (e.g. the address bar, SSL icon, web browser warning indicators, fake websites), activities and dangers involved in a phishing attack [14],[16],[26] and to report such attacks. This is substantiated by Ohaya [19] that many users do not have the underlying knowledge of how operating systems, e-mails and websites work as employees cannot tell the difference between a genuine and spoofed-website. In some cases, users frequently ignore phishing warning messages from anti-phishing tools [7],[19],[31]. For effectiveness, the training could have some incentive, fun (e.g. gameplay [26]) or humour to gain participation from staff. An added benefit, through training, allows employees to also learn other current and future threats of information security aspects e.g. scams, viruses instead of phishing attacks alone especially since attack methods are evolving. Third parties may also require education equivalent with full time employees however, effective education may prove difficult in outsourced environments where providers are growing rapidly [2]. It is essential for all employees to be an above-average computer user, especially in using email and internet, as it exposes the user and organisation to other potential threats. This requirement can be enforced in the recruitment policy (*Organisation Aspects*).

Awareness Programmes: According to ISO/IEC 27002 [25], critical success factors, based on experience, have shown that information security awareness is important. Awareness programmes should aim to enhance levels of trust between employer and employee by developing an understanding of the reasons for the security

policies and controls that have been applied, as it will help staff be more aware of the issues [3] thus reducing the likelihood of accidental breaches and increase the probability of malicious activity being detected and reported. Staff needs to understand the implications of not obeying such policies.

Staff Lack in Security Behaviour: Unacceptable, non-malicious behaviour by staff should be taken seriously. Organisation policies can ensure that employees cannot plead ignorance to the rules as many insider problems stem from ignorance rather than malicious motivation [2]. However, mere accidents can potentially cause large implications e.g. social networking sites are a playground for social engineers [10] thus, if staff are spending excessive time on social network sites during office hours, this may put the organisations reputation and financial well-being at risk.

Technical staff must be educated in their duties and define proper technical procedures and apply the relevant technological controls to implement those procedures e.g. prevent users from accessing risky sites.

Monitoring: Some organisations emphasise that monitoring can benefit staff where employees are reassured that the organisation is safeguarded against confidential leaks and hence possible damage to its reputation or financial loss.

Conclusion

It has been established that HOT dimensions in an organization require strengthening to address phishing [9]. Human factors have been mentioned to be the greatest risk and as such require the most focus. Much research has been placed either on education, training and awareness [14],[16],[21],[26] or technical controls. Although each HOT dimension has its own weaknesses or vulnerabilities, as all encompass some human involvement, education can close the gap between all the dimensions (e.g. should the technical controls fail; humans can be aware and knowledgeable in addressing a phishing attack) thus resulting in a multi-level defense model.

References

Beznosov, K. & Beznosova, O.: On the imbalance of the security problem space and its expected consequences. Information Management & Computer Security, pp.420--431.15, Emerald (2007)

Cobb, M.: Preventing phishing attacks: Enterprise best practices. SearchSecurity.co.uk. (2010)

Colwill, C.:Human factors in information security: The insider threat - Who can you trust these days? Information Security Technical Report, 30**,** pp.1--11. (2010)

Dhamija, R., Tygar, J. D. & Hearst, M.: Why phishing works. In: SIGCHI conference on Human Factors in computing systems, pp. 581--590. Montreal,Canada: ACM.(2006)

Downs, J. S., Holbrook, M. & Cranor, L. F.: Behavioral response to phishing risk. In: anti-phishing working groups 2nd annual eCrime researchers summit, pp.37--44. Pittsburgh, Pennsylvania: ACM. (2007)

Drake, C. E., Oliver, J. J. & Koontz, E. J.: Anatomy of a Phishing Email. Conference on Email and Anti-Spam (CEAS). Citeseer. (2004)

Egelman, S., Cranor, L. F. & Hong, J.: You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In:26th annual SIGCHI conference on Human factors in computing systems, pp. 106--1074. Florence, Italy: ACM (2008)

Fette, I., Sadeh, N. & Tomasic, A.: Learning to detect phishing emails. In: 16th international conference on World Wide Web, pp. 649--656. Banff, Alberta, Canada: ACM (2007)

Frauenstein, E. D. & von Solms, R.: Phishing: How an organisation can protect itself. In: Information Security South Africa, pp. 253--268. 6-8 July 2009 Johannesburg, South Africa (2009)

Frauenstein, E. D. & von Solms, R.: The Wild Wide West of Social Networking Sites. South African Information Security Multi-Conference, pp. 74--88. 17-18 May 2010 Port Elizabeth, South Africa (2010)

Garera, S., Provos, N., Chew, M. & Rubin, A. D.: A framework for detection and measurement of phishing attacks. In: 2007 ACM workshop on Recurring malcode, pp. 1--8. Alexandria, Virginia, USA: ACM (2007)

Herzberg, A. & Jbara, A.: Security and identification indicators for browsers against spoofing and phishing attacks. ACM Trans. Internet Technol., 8**,** pp. 1--36. (2008)

Hinson, G.: Human factors in information security. http://www.infosecwriters.com/text_resources/pdf/human_factors.pdf. (2003)

Jakobsson, M.: The Human Factor in Phishing. Privacy & Security of Consumer Information. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.68.8721&rep=rep1&type=pdf.(2007)

Kraemer, S., Carayon, P. & Clem J.: Human and organizational factors in computer and information security:Pathways to vulnerabilities. Computers & Security, 28, pp. 509--520. (2009)

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F. & Hong, J.: Teaching Johnny not to fall for phish. ACM Transactions on Internet Technology, pp. 1--31. 10, ACM (2010)

Leavitt, N.: Instant Messaging: A new target for hackers, pp. 20--33. IEEE Press (2005)

Mitnick, K. D., Simon, W. L. & Wozniack, S.: The Art of Deception: Controlling the Human Element of Security, New York, Wiley (2002)

Ohaya, C.: Managing phishing threats in an organization. In: 3rd annual conference on Information security curriculum development, pp. 159--161.Kennesaw, Georgia, ACM (2006)

Ollman, G.: The Phishing Guide (white paper), http://www.ngssoftware.com/papers/NISR-WP-Phishing.pdf.(2008)

Orgill, G. L., Romney, G. W., Bailey, M. G. & Orgill, P. M.: The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems. In: 5th conference on IT education, pp. 177--181. Salt Lake City, UT, USA: ACM (2004)

Patel, D. & Luo, X.: Take a close look at phishing. In: 4th annual conference on Information security curriculum development, pp. 1--4. Kennesaw, Georgia:. ACM (2007)

Raffetseder, T., Kirda, E. & Kruegel, C.: Building Anti-Phishing Browser Plug-Ins: An Experience Report. In: 3rd International Workshop on Software Engineering for Secure Systems. IEEE Computer Society (2007)

Robila, S. A. & Ragucci, J. W.: Don't be a phish: steps in user education. In: 11th annual SIGCSE conference on Innovation and technology in computer science education. pp. 237--241. Bologna, Italy: ACM (2006)

SANS, Information technology-Security techniques-Code of practice for information security management. ISO/IEC 27002:2005. Standards South Africa.(2008)

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J. & Nunge, E.: Anti-Phishing Phil: the design and evaluation of a game that teaches people not to fall for phish. In: 3rd symposium on Usable privacy and security, pp. 88--99. Pittsburgh, Pennsylvania: ACM (2007)

Sophos, Phishing and the threat to corporate networks (white paper).: http://www.sophos.com/whitepapers/sophos-phishing-wpuk.pdf.(2005)

Thomson, K.-L., von Solms, R. & Louw, L.: Cultivating an organizational information security culture. Computer Fraud & Security. (2006)

von Solms, S. H. & von Solms, R.: Information Security Governance, New York, Springer. (2009)

Werlinger, R., Hawkey, K. & Beznosov, K.: Human, Organizational and Technological Challenges of Implementing IT Security in Organizations. In: Human Aspects of Information Security and Assurance, pp. 35--48. Plymouth, England. (2008)

Wu, M., Miller, R. C. & Garfinkel, S. L.: Do security toolbars actually prevent phishing attacks? In: SIGCHI conference on Human Factors in computing systems, pp. 601--610. Montreal, Quebec, Canada, ACM (2006)

Zhang, Y., Hong, J. I. & Cranor, L. F.: Cantina: a content-based approach to detecting phishing web sites. In: 16th international conference on World Wide Web. pp.639--648. Banff, Alberta, Canada:. ACM (2007)