Australian Government
Department of Defence
Defence Science and
Technology Organisation

Human Factors and Information Security: Individual, Culture and Security Environment

Kathryn Parsons, Agata McCormac, Marcus Butavicius and Lael Ferguson

Command, Control, Communications and Intelligence Division
Defence Science and Technology Organisation

DSTO-TR-2484

ABSTRACT

The application of information security technologies do not always result in improved security. Human factors play a significant role in computer security; factors such as individual difference, cognitive abilities and personality traits can impact on behaviour. Information security behaviours are also greatly influenced by an individual's perception of risk. All of these factors are also affected by the organisation culture and security environment in which they occur. These factors interact with one another and can result in behaviours that are often detrimental to information security. This report provides recommendations as to how these human and cultural factors can be influenced to result in more positive behaviours and lead to more secure information environments.

Published by

Command, Control, Communications and Intelligence Division
DSTO Defence Science and Technology Organisation
PO Box 1500
Edinburgh South Australia 5111 Australia

Telephone: (08) 8259 5555
Fax: (08) 8259 6567

AR-014-705
October 2010

APPROVED FOR PUBLIC RELEASE

Human Factors and Information Security: Individual, Culture and Security Environment

Executive Summary

The numerous technical advances in information sciences do not always produce more secure environments. Therefore, information security cannot be understood or described as solely a technical problem. Computers are operated by people and this means that information security is also a human factors issue. Human factors influence how individuals interact with information security technology; it is this interaction that is often detrimental to security.

It is evident that solely technical solutions are unlikely to prevent security breaches. Organisations need to instil and maintain a culture where positive security behaviours are valued. The usability challenges associated with information security need to be understood and resolved. This means that security functions need to be meaningful, easy to locate, visible and convenient to use. Employees need to be educated about the importance of security awareness, and this should incorporate behavioural training.

How individuals interact with computers and how decisions are made in regard to information security is certainly a very dynamic and complex issue. There are many factors that need to be considered. For example, it is important to acknowledge the influence of individual differences, personality traits and cognitive abilities. There are also biases and heuristics that affect how individuals perceive risk. These are important because they help to explain why individuals make certain decisions and why specific behaviours may be observed.

Both risk perception and individual differences are also affected by the environment in which they occur. Culture and climate can certainly have a significant impact on values, attitudes and behaviours. That is why understanding an organisation's culture and security climate can provide great insights into why certain behaviours do and do not take place.

A major concern within information security is the threat of social engineering attacks. Social engineering attacks are conducted in an effort to gain sensitive information, and this information is often used maliciously to the detriment of individuals and organisations. Social engineering poses a real threat to all organisations and to diminish this threat, individuals need to not only be aware of potential attacks, but also taught the appropriate tools to reduce their chances of becoming a target and a victim.

Given the complexity of human factors issues in information security, recommendations will be made about how to promote positive security behaviours through awareness, education and training, in conjunction with improvements in physical and computer security.

Authors

Kathryn Parsons
Command, Control, Communications and Intelligence

Kathryn Parsons is a research scientist with the Human Interaction Capability Discipline in C3ID where her work focuses on cognitive and perceptual psychology, information visualisation and interface design. She obtained a Graduate Industry Linked Entrepreneurial Scheme (GILES) Scholarship in 2005, with Land Operations Division, where she was involved in human factors research, in the Human Sciences Discipline, specifically in the area of Infantry Situation Awareness. She completed a Master of Psychology (Organisational and Human Factors) at the University of Adelaide in 2005.

Agata McCormac
Command, Control, Communications and Intelligence

Agata McCormac joined DSTO in 2006. She is a research scientist with the Human Interaction Capability Discipline in C3ID where her work focuses on cognitive and perceptual psychology, information visualisation and interface design. She was awarded a Master of Psychology (Organisational and Human Factors) at the University of Adelaide in 2005.

Marcus Butavicius
Command, Control, Communications and Intelligence

Marcus Butavicius is a research scientist with the Human Interaction Capability Discipline in C3ID. He joined LOD in 2001 where he investigated the role of simulation in training, theories of human reasoning and the analysis of biometric technologies. In 2002, he completed a PhD in Psychology at the University of Adelaide on mechanisms of visual object recognition. In 2003 he joined ISRD where his work focused on data visualisation, decision-making and interface design. He is also a Visiting Research Fellow in the Psychology Department at the University of Adelaide.

Lael Ferguson
Command, Control, Communications and Intelligence

Lael Ferguson graduated from the University of South Australia in 1997 with a Bachelor of Applied Science (Mathematics and Computing) and began working for the Department of Defence in Canberra as a software developer. In 1999 she transferred to Geraldton and worked as a system administrator. In 2000 she transferred to the Defence Science Technology Organisation at Edinburgh as a system administrator/software developer, managing a computing research laboratory, and developing concept demonstrators and experimental software.

Contents

1. Introduction

Information security refers to the protection of the confidentiality, integrity and access to information (Kruger & Kearney, 2006). Evidence suggests that, regardless of the number of technical controls in place, organisations will still experience security breaches (Schultz, 2005; Besnard & Arief, 2004). In fact, the 2007 CSI Computer Crime and Security Survey reported that although 98% of users have anti-virus software, 52% were still infected with viruses (Richardson, 2007). This is because information security is not only a technical problem, but is also a 'people' problem (Schulz, 2005). It is, however, necessary to note that even anti-virus software used in the optimal manner will not protect against all viruses, which means that this is not solely a 'people' problem, but is also a technical problem. Despite this, some evidence suggests that employees' failure to comply with information security guidelines is the cause of the majority of breaches in information security (Chan, Woon & Kankanhalli, 2005). In support of this finding, results of the 2007 Global Security Survey, in which information security professionals were interviewed, indicated that 79% of respondents perceive human error to be the root cause of failures of information systems (Deloitte, 2007).

This report will highlight the human factor issues that are likely to influence how individuals interact with information security technology. This will include an analysis of the factors that influence an individual's ability to accurately perceive risk, and the aspects of an organisation's culture that are likely to lead to an environment where positive security behaviours are rewarded and maintained. The importance of effective communication, including appropriately framing information regarding security behaviours, will also be examined. Furthermore, this report will examine the influence of social engineering within an information security context, including the factors that tend to increase an individual's susceptibility, an analysis of previous studies that have attempted to investigate social engineering, and a review of effective defences against social engineering. Finally, recommendations and suggestions for further empirical experimentation in the area and conclusions will be provided.

1.1 Information Security and Types of Human Factor Errors

Humans are consistently referred to as the weakest link in security (Schneier, 2000; Huang, Rau & Salvendy, 2007). An exclusive focus on the technical aspects of security, without due consideration of how the human interacts with the system, is clearly inadequate. This section includes the types of human factor errors that can lead to security violations. A number of reasons for these errors will also be discussed.

Information security breaches can be categorised in a number of different ways. Swain and Guttman (1983) distinguish five different types of human factor errors, which can be used to explain information security breaches. First, there are acts of omission, in which people forget to perform a necessary action. For instance, in an information security domain, this could involve the failure to regularly change passwords. Second, errors are commonly acts of commission, in which people perform an incorrect procedure or action, such as writing down a password. Third, a number of errors are caused by extraneous acts, which involves doing something unnecessary. Fourth, errors can be caused by sequential acts, which involve doing

something in the wrong order. Finally, Swain and Guttman (1983) refer to time errors, caused by people failing to perform a task within the required time.

Security behaviour can also be described using a two-factor taxonomy, where the two factors are intentionality and technical expertise (Stanton, Stam, Mastrangelo & Jolton, 2005). As shown in Figure 1, this creates six categories of security behaviours, where two of those behaviours (*Aware Assurance* and *Basic Hygiene*) are positive, designed to increase security, and four of the behaviours may result in breaches to security.

Intentional Destruction covers the actions of malicious insiders, who have technical expertise and the intent to do harm, whereas *Detrimental Misuse* involves personnel who have malicious intent, but lack technical expertise. *Dangerous Tinkering* covers behaviours that require technical expertise, but where there is not an intention to do harm. Perhaps the most common behaviour, which will be covered in the most detail in this report, is *Naïve Mistakes*, in which individuals with low expertise and without malicious intentions perform an action which was not intended to harm the organisation, but yet could result in a security breach.

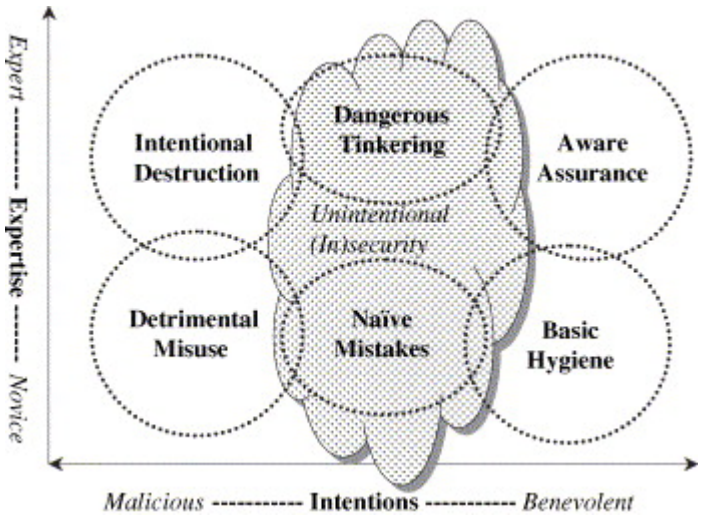

Figure 1: Two-factor taxonomy of end user security behaviours (Stanton et al., 2005)

In fact the majority of human factor errors could be described as accidental. Accidental human factor errors are associated with the way in which the individual interacts with a system, and evidence suggests that people may encounter problems in finding, understanding and using security features (Furnell, 2005).

One common human error that can lead to security breaches is referred to as a *capture error*. Such errors occur when a familiar activity or habitual routine takes over (or captures) an unfamiliar activity, leading to a cognitive failure or mistake (Norman, 1981). For example, capture errors can be used to describe the fact that people often click OK when they know that they should not. Essentially, the act of clicking the OK button is so habitual and common that people often follow this routine without properly considering the consequences. These errors are particularly common during periods of tiredness or inattention.

Inattention and tiredness can also result in *post-completion errors*, in which the individual neglects to carry out a necessary 'tidy-up' or 'clean-up' action that is required after the main goal has been completed (Anderson, 2008). For example, from an information security point of view, the main goal may involve sending an email from a secure system. Once that goal has been completed, it is then necessary to complete the final action of logging off the system. A post-completion error would involve a situation where the individual in question fails to complete that final task, leaving the system open to a possible security breach.

Related to that, a number of security procedures depend on human memory, and since the capacity of memory is limited, this can result in a decrease in security (Besnard & Arief, 2004; Sasse, Brostoff & Weirich, 2001). For instance, users generally have a vast number of passwords to remember, and often these passwords must conform to a number of stringent policies (such as adhering to a certain length or a certain combination of characters), which can further reduce ease of remembering. People are quite good at remembering meaningful items (including words), but strong passwords should be meaningless strings of numbers and letters, which are far more difficult to remember. When people are required to remember and regularly change many complicated passwords, the chance of these passwords being written down greatly increases (Adams & Sasse, 1999).

Associated with this, many anti-virus updates and other security patches require human intervention, and hence, due to limits associated with either time or human memory, such procedures may not be carried out, leading to a decrease in security.

1.1.1 The Importance of Usability

It is also necessary to highlight the importance of usability, and the interaction between poor usability and the human desire to take shortcuts. Essentially, security technologies often include complicated counter-intuitive processes that are very difficult to understand (Schultz, 2005). Such complex procedures are likely to be avoided wherever possible, and hence, the likelihood of security breaches is increased (Schultz, 2005). Similarly, the *unmotivated user property* suggests that security is a secondary goal for most people, and hence, people often lack the motivation to follow complicated security procedures (Whitten & Tygar, 1998).

Furthermore, there is a trade-off between security and usability, in which humans try to minimise mental effort, whilst maintaining an acceptable level of performance (Besnard & Arief, 2004). According to Wilde (2001), there are four motivating factors that influence this trade-off between security and usability. Users are influenced by the expected costs and benefits associated with the risky behaviour, and the expected costs and benefits associated with the safe behaviour (Wilde, 2001). Hence, if the potential gains associated with undertaking a risky activity are quite high, or if the adherence to a security system is a great inconvenience, then people are less likely to obey the policy, and are more likely to take risks (Schneier, 2003). This is supported by Schneier (2003), who indicates that an understanding of the trade-offs associated with security is essential. For example, problems associated with traffic safety could essentially be solved by dramatic changes such as a substantial decrease in speed limits (Odlyzko, 2003). However, people are not willing to live with such restrictions, and hence, the speed limit is a cost-benefit trade-off. Similarly, the security of information technology could be greatly improved through a drastic reduction in users' access and

privileges. However, people are unlikely to tolerate such stringent restrictions, and it is therefore necessary to find an adequate balance between security and usability.

Hence, it is important that security products are designed with the user in mind (Besnard & Arief, 2004). This means applying the principles of human-computer interaction into the design process. It also means that computer security needs to be focused on the goal of becoming effortless, meaning that the process should be made easier for users. Whenever possible, detailed aspects of day-to-day operational computer security should not be difficult or greatly time consuming for the end user (Besnard & Arief, 2004). For example, the systems administrator should have the responsibility of monitoring security problems and updating virus protection, along with any other security concerns specific to the network. If staff are required to scan their computer drives or update their computer, this is always done at the sacrifice of their primary work and duties, and this needs to be taken into consideration and compensated appropriately (Besnard & Arief, 2004).

Furnell, Jusoh and Katsabas (2006) also emphasise the importance of creating usable security systems. Their study found that the presentation of security functions needs to be improved in order to help users protect themselves from security threats. They concluded that usability can be improved by focusing on four broad areas: ease of understanding, location, visibility and convenience.

Security functions need to be understandable. Jargon and technical terminology can be confusing to novice and non-technically minded users, and may result in non-conformity and human factor errors. Therefore, options and descriptions need to be meaningful to the user. Security features also need to be easy to locate; a user who needs to actively search for security settings may well give up and may therefore be more exposed to security threats. Where the end-user is responsible for security, ideally, it should be visible, so that a user can see what security is being applied, and they should be informed when any updates or safeguards need to be added. Finally, where possible, security should be convenient, and it should not impede other work or responsibilities. By ensuring that these four usability recommendations are met, there is less pressure placed on the user, and they are more likely to conform to security requirements and expectations, and are less likely to make accidental mistakes (Furnell et al., 2006).

Shneiderman (1998) further expands on these recommendations to improve usability and proposes eight widely cited 'golden rules' for interface design. The eight rules aim to strive for consistency, enable frequent users to use shortcuts, offer informative feedback, design dialogs to yield closure, offer simple error handling, permit easy reversal of actions, support internal locus of control and reduce short-term memory load (Furnell, 2005).

Similarily, Katsabas, Furnell and Dowland (2005) also focus on the presentation of security information to improve usability and in turn improve security. They state that security settings should be easy to set up, and security help and documentation should be appropriate. It should also handle errors well and allow users to make customised changes, without risking further security complications. Importantly, security should not reduce performance and it should make the user feel more protected (Furnell, 2005). Furthermore, security should be suitable for all levels of users, should be visible and easy to use, and should avoid jargon and

a technical vocabulary. If security features are designed with these aspects of usability in mind, this is likely to result in more conformity and hence, fewer human factor errors.

2. Risk Perception and Information Processing Biases

When making behavioural decisions, individuals will often decide based on their estimates of the risks associated with the various options. Hence, the manner in which IT users perceive threats will influence their behavioural responses (Huang et al., 2007). It is often impractical to process all of the information that would be necessary to form a completely rational assessment of risk. Therefore, people often take shortcuts in the decision-making process, by using a number of information processing biases and heuristics to simplify the task (Kahneman, Slovic & Tversky, 1982).

These biases and heuristics can affect risk perception, and evidence suggests that people generally have an inaccurate perception of risk (Lichtenstein, Slovic, Fischhoff, Layman & Combs, 1978). Since risk perception can impede logical decision-making, understanding these perceptions is vital. Essentially, individuals who accurately perceive the risks associated with information security are more likely to act in an appropriate manner. Hence, it is necessary to understand the factors that can impede accurate risk perception.

Although there is a great deal of research in risk perception in general, there is little empirical study examining individuals' perceptions of risk within the information security domain. Huang and colleagues (2007) surveyed 602 people on their perceptions of various threats to information security. They concluded that perceptions of information security risks could be described using six factors, namely knowledge, impact, severity, controllability, possibility and awareness (Huang et al., 2007). The perceived danger of threats was significantly higher when there was little knowledge of the risk, the possible impact of the risk was high, the potential severity of the risk was high, or there was a greater possibility of the risk occurring.

A number of other authors have inferred perceptions of security risks from research in other areas. For example, Pattinson and Anderson (2005) suggest that perceptions of security risks are generally influenced by factors such as the individuals' mood at the time, recent media reports, past experiences, and knowledge of technical aspects, such as viruses. A number of psychological, social and cultural factors can also affect the way that people perceive risk (Bener, 2000). Further research has discovered that aspects such as whether a risk is voluntary, whether the risk is controllable and the implications of the risk can also have a large influence (Heimer, 1988).

The factors that tend to influence individuals' perception of security risks will now be analysed in more detail in the section below.

2.1 Availability Heuristic

One of the most common biases is known as the availability heuristic. This bias is based on the idea that people tend to judge the frequency or likelihood of an event based on how easily an example can be brought to mind (Slovic, Fischhoff, & Lichtenstein, 1979; Tversky & Kahneman, 1973). This heuristic is also closely related to the media coverage of events, as highly publicised events are also more memorable. However, studies have consistently

indicated that the media coverage of events has little or no correlation with the actual frequency of risks, and this therefore increases the chance that people will have inaccurate perception of risk (Slovic, Fischhoff, & Lichtenstein, 1976; Lichtenstein, Slovic, Fischhoff, Layman and Combs, 1978).

Generally, the frequency of very common but chronic risks, which build up over time (e.g., heart disease), are less likely to be reported, and are also significantly underestimated. In information security the more chronic issues include factors such as badly trained staff, inadequate procedures and poorly designed systems (McIlwraith, 2006). In contrast, the relatively rare but acute risks, which are more sudden and dramatic (e.g., murder) are overestimated, and also receive more media coverage. In regard to information security, the risks that are more likely to be overestimated include hacking and industrial espionage (McIlwraith, 2006).

Furthermore, since security breaches are rare, the availability heuristic is most likely to lead to an underestimation of risk. Essentially, users are more likely to recall events when incorrect procedures or non-adherence to security policies did not lead to accidents, and therefore, the actual risk of not following procedure is more likely to be underestimated (Slovic et al., 1976). In fact, each time that an individual breaches security without any consequences, this risky behaviour is likely to be reinforced, which means that it is more likely to occur in the future.

2.2 Optimism Bias

Related to this is the optimism bias, which refers to the fact that most people do not believe that they are personally at risk, and instead, tend to believe that negative outcomes are far more likely to occur to others (Gray & Ropeik, 2002). This bias was demonstrated in a study where participants were asked to judge the likelihood of various risks occurring to themselves, their family members and the general public (Sjoberg, 2000). For all risks, the average ratings were lower for the individual and the individual's family than they were for the general public (Sjoberg, 2000).

This bias is particularly prevalent in information security, as evidence suggests that most users tend to believe that hackers would not value the information on their computers, and hence, users are unlikely to see themselves as potential targets (McIlwraith, 2006). This belief has little regard for the fact that industrial spies or hackers could target any individual in order to gain access to the overall system (which could then allow further access to more important areas of a computer network) (McIlwraith, 2006).

The optimism bias is also particularly prevalent in situations where people expect to see warning signs if they are vulnerable (Weinstein, 1987). This could be true of security risks, and evidence suggests that people will often erroneously believe that if they fail to see warning signs, they are exempt from future risks (Weinstein, 1987). The optimism bias can result in an increase in security related risks, as individuals may underestimate the risk, and may therefore fail to keep up to date with security patches, and may fail to follow other security procedures (Mitnick & Simon, 2005). Essentially, people will underestimate the likelihood that their actions or inactions could result in a security breach.

2.3 Level of Control

Individuals are also found to have an unrealistic optimism for risks that they perceive to be under their personal control (Kreuter & Strecher, 1995). Since an individual may view their actions on their personal computer to be under their control, threats may be seen as less risky. Hence, the chance that non-adherence to security policies will result in serious consequences may also be underestimated. This means that individuals might be more likely to engage in risky behaviour. This bias is commonly observed in drivers' perception of vehicle risks, in which people often show exaggerated feelings of confidence caused by their feelings of control (Slovic, Fischhoff, & Lichtenstein, 1978).

This increase in risky behaviour is generally particularly prevalent in individuals who have a high level of competence or perceived skill. Hence, it is likely that people who have skill in the area of information security could overestimate their ability to control the threat, and they may therefore take more risks.

2.4 Level of Knowledge

Conversely, risks can also be strongly influenced by individuals' lack of knowledge or education in information security. Often, it is difficult to comprehend a risk and the threat that it poses without an accurate understanding of the specifics of the risk in question. This is particularly true of some security risks, as people may need technical knowledge to understand the magnitude or implications of potential security breaches. Without this knowledge, effective decision-making and risk perception can be seriously affected (Fischhoff, 2002). Essentially, many users will not comprehend the underlying technology, and hence, their decisions might not be based on an accurate understanding of what being 'secure' means (Lacohee, Phippen & Furnell, 2006).

For example, a study by Adams and Sasse (1999) found that users had an inadequate knowledge of what constitutes a secure password, and very few users understood how passwords could be cracked. Hence, users often chose very insecure passwords, without realising that they were doing so. A lack of knowledge can also lead to a lack of security motivation, as people may not understand the seriousness of the potential risk, and the associated need for security procedures. These factors emphasise the importance of effective security awareness and risk communication, which will be covered in more detail in a subsequent section.

2.5 Risk Homeostasis

It is also possible that a phenomenon known as risk homeostasis or risk compensation may influence individuals' behaviour, and lessen the likelihood that people will accurately understand the seriousness of information security risks (Stewart, 2004). This theory states that people will generally accept a particular level of risk, and then, as situations change, behaviour will change to remain at the desired level of risk (Wilde, 2001). In other words, if conditions are perceived to be less risky, then people may take more risk, and if the conditions are perceived to be more risky, then the amount of risk taken may be reduced.

This theory was demonstrated when antilock brakes were first introduced on motor vehicles. With the introduction of this new technology, it was expected that the accident rate would go down. However, this was not the case. The theory supposes that people took into account the increase in driving safety, and therefore drove more aggressively (which resulted in more injuries). Although there is some debate about the validity of this theory (O'Neill & Williams, 1998), it may well help to explain why people who are aware of security procedures do not always adhere to security principles. It is possible that individuals may perceive that improved firewall protection or other security mechanisms may have decreased any possible threat, and they may therefore change their behaviour, and act in a more risky manner. For example, if a system is in a highly controlled access area, people might be less diligent about protecting the computer (Mitnick & Simon, 2005).

2.6 Cumulative Risk

Many of the risks associated with information security are of a cumulative nature. This means that the likelihood of an event occurring on a given day or at a given time might be extremely small, but over time, this chance increases (Fischhoff, 2002). For example, if someone chooses an insecure password, the chance that this non-adherence to procedure will be exploited might be very small on a particular day, but over the weeks and months, this chance builds up.

It is also necessary to take into account the cumulative risk posed by different people all taking small risks. For instance, the risk associated with one person failing to follow one procedure may not be high, but if a number of individuals create different vulnerabilities, the cumulative risk might be substantial. However, individuals are generally quite poor at understanding this cumulative risk (Slovic, 2000), and hence, they might be more likely to take small risks, as they may not appreciate the full consequences.

2.7 Omission Bias

Individuals' behaviour can also be influenced by the omission bias. Essentially, people rate an omission (or a failure to act) as more acceptable than an act of commission (Ritov & Baron, 2002). Many security breaches (such as the failure to regularly change passwords) can be viewed as omissions, and such inactions may therefore be seen as more acceptable than the equally risky action of writing a password down. Post-completion errors, which were mentioned previously, are a form of omission bias. Essentially, since the omission bias suggests that inactions are generally seen as less morally questionable than actions, this bias is likely to increase the occurrence of post-completion errors.

2.8 The Influence of Familiarity

Evidence suggests that the familiarity of a risk can also influence the manner in which it is perceived. Novel and unfamiliar risks are less likely to be underestimated, whereas people can become complacent with common risks that they have lived with for a long time. Hence, familiar risks are more likely to be underestimated. In other words, people are more likely to take risks when they are familiar with a task. This could apply to information security, as people can become complacent with tasks that they complete each day, such as locking their

computer when it is unattended. The complacency could then lead to an increase in risk-taking behaviour.

It is, however, necessary to note that the opposite is sometimes true. A study assessed compliance with safety instructions on various products, and found that participants were more likely to follow precautions when using product brands with which they were more familiar (Ortiz, Resnick & Kengskool, 2000). This links back to the influence of a users' knowledge, as it indicates that people will be likely to continue to adhere to the necessary safety instructions of a familiar risk if they understand the reason for the precautions. Hence, this highlights the importance of user education, which will be covered in more detail in a subsequent section.

2.9 The Influence of Framing

The manner in which a risk is described or framed can also influence individuals' perception of risk. For instance, when a risk is specified with an emphasis on the possible losses, a risk-taking strategy is more common, whereas a risk-aversion strategy is more likely when the risk is described in regard to the possible gains (Kahneman & Tversky, 1979). This is based on the prospect theory, with the idea that people have subjective values for losses and gains (Schneier, 2003).

The effect of framing was clearly demonstrated in a study by McNeil, Pauker, Sox and Tversky (1982). Participants in this study were asked to imagine that they had lung cancer, and were then provided with treatment options. When participants were provided with probabilities framed in terms of the chance of dying (32%) rather than the chance of surviving (68%), the percentage of people choosing the treatment dropped from 44% to only 18% (Slovic, 1986). This has important implications for information security, as it suggests that people can be strongly influenced by the manner in which the risk is communicated. For example, this suggests that people may be more likely to follow information security guidelines if the outcome is described with an emphasis on the possible gains. This will be covered in more detail in the risk communication section, to follow.

2.10 Personality and Cognitive Style

Individual differences in regard to factors such as personality and cognitive style may also influence the perception of (and tendency to take) risks (Lion & Meertens, 2005). O'Neill (2004) suggests that people can be categorised based on how they deal with risk, from those who are very risk averse, to those who seek out risk. These differences are likely to influence the way that people perceive the information around them, which, in turn, is likely to influence their behaviour. A study by Lion and Meertens (2001) examined the amount of information that participants looked up in regard to a drug, and found that there were considerable differences between risk takers and risk avoiders.

Sensation seekers, or people who seek out risk, will often take risks to maintain physiological arousal, and are more likely to focus on the rewards associated with risky behaviour (Horvath & Zuckerman, 1993). In contrast, people who are more risk averse or rule-conscious are more likely to focus on the costs associated with risk-taking, and they are generally more moralistic,

and less likely to disregard security procedures (Lion & Meertens, 2005). These are, however, more theoretical hypotheses as opposed to consistent traits that have been empirically proven.

2.11 The Influence of Social Factors

Group norms can also influence individuals' security behaviour. People generally follow group norms, and therefore if the group considers information security to be an important and serious problem, then it is more likely that the individuals within that group will value and follow the security policies. Conversely, if risk-taking is accepted within the group, then it is likely that greater risks will be taken.

Group norms can also affect individuals' password behaviour. For instance, according to McIlwraith (2006), password sharing can be considered to be a sign of trust in a colleague, and therefore, refusing to share a password could be seen as a sign that people do not trust their colleagues. If such norms are present within an organisation, then a great deal of education will be necessary to change these behaviours.

A social effect known as the *bystander effect* could also influence the manner in which people respond to, or perceive, risks. This effect is based on the idea that as the number of people present increases, people will shift their responsibility, so that the likelihood of any one person responding decreases. Hence, in large groups, individuals may feel less personal responsibility for security. These social and group factors are strongly related to organisational culture, which will now be defined and explained in more detail.

3. Organisational Security Culture

Security culture cannot be assessed in isolation from the overall culture within a work environment; this is because an organisation's culture has a strong impact on organisational security (Ruighaver, Maynard & Chang, 2007). Therefore to understand security culture it is first important to have a grasp on the wider literature of organisational culture.

3.1 Definitions and Theory of Organisational Culture

The concept of culture is not clearly understood; in fact no two theorists or researchers define culture in the same way (Ivanchevich, Olekalns & Matterson, 2000). Culture is defined differently, measured differently and evaluated differently (Schein, 1985). This lack of consensus on the construct of culture has resulted in a great deal of controversy and debate (Needle, 2000).

It is Schein's definition of culture that is the most widely accepted (Huczynski & Buchanan, 2001). Schein defines organisational culture as:

> *"a pattern of basic assumptions – invented, discovered, or developed by a given group as it learns to cope with the problems of external adaptation and internal integration – that has worked well enough to be considered valid, and therefore, to be taught to new members as the correct way to perceive, think and feel in relation to these problems" (Schein, 1985, p.9).*

Schein's model of culture consists of three levels: *artifacts and creations*, *values and beliefs*, and *basic assumptions* (Schien, 1985). *Artifacts and creations* comprise the first level and represent the most visible and apparent aspects of an organisation. According to Schein (1985), this level includes the elements of culture that can be seen and heard and easily interpreted by employees, customers and the public, including furniture and clothing, symbols, objects, the language used within the workplace, as well as slogans, rituals and stories (Huczynski & Buchanan, 2001; Schein, 1985).

The second level of culture comprises *values and beliefs* that underpin *artifacts and creations* (Schein, 1985). Values are the wants and desires that guide behaviour; they are devised by senior management to provide direction and guidelines for the behaviour of their employees (Huczynski & Buchanan, 2001). Peters and Waterman (1982) highlight the importance of values within an organisation, arguing that values hold all other elements of culture together and are the key to high organisational performance. Shared values are deemed to be crucial because if employees do not have shared values, the organisation cannot operate effectively (Ivancevich et al., 2000). However, Buono, Bowditch and Lewis (1985), state that the strength of values is questionable, primarily because senior management generates values, and as a result they are not necessarily influential on actual employee behaviour.

According to Schein (1985) it is the third level of culture, *basic assumptions*, which actually represents and captures an organisation's culture. Basic assumptions are hidden, elusive and invisible, making the core concepts of culture difficult, not only to understand, but also to assess (Schein, 1985). These basic assumptions include the "assumptions individuals hold

about the organisation and how it functions, they relate to aspects of human behaviour, the nature of reality and the organisation's relationship to its environment" (Huczynski & Buchanan, 2001, p.633). Culture evolves and develops over time and this complexity is a contributing factor to the debate over what the construct of culture actually represents (Huczynski & Buchanan, 2001).

Some researchers suggest that organisational culture can be viewed and understood in three different ways; as an internal variable from within the workplace, as an external variable brought into the workplace, or as a root metaphor, meaning that culture is something an organisation has or is (Smirchich, 1983). According to Thompson and Luthans (1990) culture is best understood by linking these three perspectives together, emphasising that culture is not a static but rather a constantly evolving construct.

The strength of an organisation's culture is observed through the socialisation of new members (Van Mannen & Schein, 1979). Socialisation is a process that continues throughout an individual's association with an organisation, because as an organisation changes and develops, individuals need to adapt to new changes. Individuals are most aware of the socialisation process when they first join a company or are shifted to different departments or teams (Feldman & Brett, 1983). In essence, socialisation can be viewed as a form of organisational integration (Ivancevich et al., 2000). Specifically, socialisation "is a strategy for achieving congruence of organisational and individual goals … [and] is an important and powerful process for transmitting the organisational culture" (Ivancevich et al., 2000, p.605).

Organisations with strong cultures are considered to operate under a cohesive set of values and norms (George & Jones, 1996). These values and norms unite team members together and generate a commitment from employees to achieve organisational goals (George & Jones, 1996). In weak cultures, minimal direction and guidance is provided to employees, and in these environments it is the formal organisational structure that guides behaviour, rather than values and norms (George & Jones, 1996). Peters and Waterman (1982) argue that strong cultures are able to generate high performance and have reported that successful and culturally strong organisations have three things in common.

First, strong organisational cultures encourage their employees to take risks and value autonomy and entrepreneurship. Second, these organisations have a clear understanding of their organisational mission; they are able to focus on their core business and continue to maintain and develop it. Third, they have established values and norms that motivate their employees. They believe that productivity is attainable through people and are strongly committed to investing in their human resources (Peters & Waterman, 1982).

Some researchers argue that a strong culture does not necessarily result in strong performance (Thompson & McHugh, 1995). For instance, the implicit culture experienced by employees may not be the culture explicitly expressed by management. It has been shown that strong cultures can at times impede an organisation from moving forward as members may be more resistant to change (Thompson & McHugh, 1995). Culture is certainly not a uniform phenomenon and within a culture, subcultures can also exist (Hampden-Turner, 1990).

Subcultures can be observed in different levels, functions and roles within an organisation resulting in differences in attitudes, beliefs and values among the members of an organisation (Hampden-Turner, 1990). Martin and Siehl (1983) refer to three types of subcultures: enhancing subcultures, orthogonal subcultures, and counter subcultures. Enhancing subcultures are often the strongest type of subculture and occur when assumptions, beliefs and values are compatible with the overall or dominant culture of the organisation. In an orthogonal subculture, although the basic assumptions of the organisation's culture are accepted, some assumptions are unique to that particular group (Martin & Siehl, 1983). In a counter culture the assumptions are in direct conflict with the organisation's unitary culture (Martin & Siehl, 1983). Subcultures within an organisation can be problematic and can negatively affect performance when the subcultures have different priorities and agendas (Furnham & Gunter, 1993).

Much of the research conducted in the area of organisational culture has supported the belief that perceptions of work environment and organisational culture have important and significant relationships with organisational behaviour. These include job satisfaction, commitment, motivation, well-being, communication, performance and security behaviours (Ruighaver et al., 2007, Parker et al., 2003; DeCotiis & Summers, 1987; Muchinsky, 1977). Security is not just a matter of applying the latest technology; effective security is strongly embedded within the corporate culture (Ruighaver et al., 2007).

3.2 Eight Dimensions of Organisational Culture Framework As Applied to Information Security

Ruighaver et al. (2007) explain that within an organisation, information security is primarily a management problem and how management deals with information security is a direct reflection of an organisation's culture. Security culture can be understood by utilising the organisational culture framework. This framework was developed by Deter, Schroeder and Mauriel (2000), and it divides culture into eight dimensions.

The eight dimensions are as follows: the basis of truth and rationality; the nature of time and horizon; motivation; stability versus change, innovation or personal growth; orientation to work, task, co-workers; isolation versus collaboration or cooperation; control, coordination and responsibility; and orientation and internal or external focus (Ruighaver et al., 2007).

3.2.1 The Basis of Truth and Rationality

The basis of truth and rationality is the first component of the organisational culture framework, and it refers to the truth in security beliefs and actions. For example, is management supportive of appropriate security behaviours and policies, both in what is stated by management, and what actions and behaviours are observed in the work environment? If management have strong security policies in place, and reflect these policies in day-to-day operations, this means that employees are more likely to also adopt similar security ideals (Ruighaver et al., 2007).

3.2.2 The Nature of Time and Horizon

The nature of time and horizon refers to how an organisation plans for their future. For example, some organisations have long-term goals and strategic plans in place, looking many years into the future. Other organisations operate by meeting short-term and immediate goals. Long term strategic planning allows an organisation to make a strong commitment to security. For example, they are able to set aside money that can be specifically used to enhance and improve information security; this increases the chance that an appropriate level of funding will be available. This long-term planning means that security is, and is likely to remain, a high priority (Ruighaver et al., 2007).

3.2.3 Motivation

Employees need to be motivated to adopt secure behaviours and practices, and management need to be able to identify what motivates their staff. For example, do individuals respond to intrinsic or extrinsic motivators, do rewards work better than punishments, or vice versa? It has been suggested that motivation occurs when employees are personally responsible for security. Horizontal social participation has also been suggested to increase motivation. This occurs when staff members from various areas of the organisation discuss shared security issues and are actively involved in decision-making processes (Koh, Ruighaver, Maynard & Ahmad, 2005).

3.2.4 Stability Versus Change/Innovation/Personal Growth

This component of the framework emphasises that security must never remain static (Shinn, 2000). Security culture requires appropriate change management and therefore organisations need to be proactive rather than reactive when dealing with security issues. Management is also encouraged to promote innovative approaches to dealing with the constant challenges that occur within a security environment (Ruighaver et al., 2007). Organisations that are willing to take risks are often more innovative than organisations that are risk averse.

3.2.5 Orientation to Work, Task, Co-workers

This framework primarily refers to finding the right balance between security and employee access to assets. Ultimately, the more management restricts access, the more secure the environment. However, management need to ensure that restrictions are not enforced to the detriment of employees. For example, management would not want their employees to become resentful of any restrictions imposed on them. To overcome this problem, management need to ensure that employees feel responsible for the security within their work environment. This means listening to suggestions and implementing them where appropriate (Ruighaver et al., 2007). Education is also an important action; educating employees about their responsibilities will increase a feeling of ownership (Freeman, 2000). In order to be successful, education needs to be continually reinforced.

3.2.6 Isolation Versus Collaboration/Cooperation

In many organisations, security decisions are made by a small team of IT specialists and managers, and often the decisions that are made by this team are ignored or altered to cope with day-to-day operations. Therefore, it is important for employees, who apply security protocols on a daily basis, to be consulted in the decision-making process. Ensuring collaboration is likely to result in more comprehensive security processes and structures, and greater acceptance of these processes and structures. The flow on effects can also include an increase in motivation and orientation to work (Ruighaver et al., 2007).

3.2.7 Control, Coordination and Responsibility

The way in which security decisions are made can vary. For example, decision-making may be strictly or loosely controlled. Tight controls are observed in organisations where a small group is responsible for making all security related decisions. Or alternatively, policies and procedures are more loosely controlled where security decisions are delegated throughout an organisation (Ruighaver et al., 2007). Both approaches can be successful. However, in either instance, it is necessary to provide clear guidelines concerning the decision-making processes, so that it is evident who is responsible for each particular aspect of security. Individuals who are responsible also need to be held accountable, and this is facilitated through effective communication and support from all levels of management (Ruighaver et al., 2007).

3.2.8 Orientation and Focus – Internal and/or External

Organisations need to take into consideration both internal and external security factors. Those organisations that have a balance between internal and external factors will have an awareness of the external security environment in which they operate. They will also be able to internally strengthen their security processes and procedures. It is this balance that will enable an organisation to be proactive in the way they approach and deal with security issues and challenges (Ruighaver et al., 2007).

3.3 Information Security and Safety Climate

The concept of organisational climate is similar to that of organisational culture (Reichers & Schneider, 1990). Organisational climate is a concept that is described as "shared perceptions of organizational policies, practices, procedures, both formal and informal" (Reichers & Schneider, 1990, p.29).

The constructs of culture and climate do overlap and share many similarities. They are both used to explain the ways in which individuals make sense of their work environments. Both concepts stress that culture and climate are learned through socialisation and interaction with others. Importantly, both attempt to "identify the environment that affects the behaviour of people in organizations" (Reichers & Schneider, 1990, p.29). However, according to Reichers and Schneider, "culture exists at a higher level of abstraction than climate, and climate is a manifestation of culture" (1990, p.29). Despite the fact that many similarities exist between them, both culture and climate are complex and multilevel constructs that have developed quite separately in the research and literature (Pettigrew, 1990).

According to Morrow (1983) the reasons why the two constructs are differentiated in the literature, despite their similarities, is a reflection of the pressure to keep concepts separate from one another in the scientific world. There are different scientific backgrounds associated with culture researchers and climate researchers, hence a resistance to place an emphasis on the similarities of the two constructs (Morrow, 1983).

Zohar (1980) identified eight dimensions of a safety climate: the importance of safety and training, the effects of safe conduct on promotion, the effects of required workplace safety, the effects of safe conduct on social issues, the management's attitudes towards safety, the level of risk in the workplace, the status of safety officer and the status of safety committee. All eight dimensions are based on employee perceptions of their workplace environment (Zohar, 1980).

Chan and colleagues (2005) found a relationship between safety climate and information security compliance behaviours. In this study, information security was viewed as an aspect of safety climate, and individuals who perceived a strong safety climate in their workplace were more conscious of information security. This study also found that, in organisations with a strong information security climate, where work practices were consistent with information security policies, people did, in fact, work safer. In addition to exploring the impact of perception of information security climate, Chan et al. (2005) also explored the impact of self-efficacy on security behaviours. Self-efficacy is an individual's belief in their ability to succeed in any given situation, and is a necessary antecedent of compliant behaviour.

The model presented by Chan and colleagues (2005) encompasses Zohar's (1980) dimensions of safety climate. Chan et al. (2005) explain that an individual's compliant behaviour is an interaction between an individual's perception of their climate, which includes the variables of co-worker socialisation, their direct supervisor practices, and upper management practices. Along with an individual's observation of climate, self-efficacy also has an influence on the resultant behaviour (Chan et al., 2005).

Their findings show that compliant behaviour in information security is influenced by both organisational factors and personal factors (Chan et al., 2005). The overall results suggest that compliant behaviours can be increased by promoting self-efficacy, ensuring that there is a positive perception of information security climate, and ensuring that all levels of the organisation (co-workers, supervisors and upper management) apply security guidelines to their everyday behaviours (Chan et al., 2005). Essentially a positive relationship between safety climate and employee behaviour will more than likely improve the level of information security within an organisation.

4. The Communication of Information Security

There are various factors that affect individuals' understanding and perception of the risks associated with information security, and a number of factors that influence the effective communication of information security. O'Neill (2004) describes risk communication as:

> *"an interactive process of exchanging information and opinions between stakeholders regarding the nature and associated risks of a hazard on the individual or community and the appropriate responses to minimise risks"* (O'Neill, 2004, p.14).

Essentially, the manner in which information security is communicated can strongly influence how it is interpreted and whether it is then acted upon (Van der Pligt, 1996). Communication is far more likely to be effective if there is an adequate understanding of the gaps in current beliefs, and a clear and concise message of what the target audience needs to know (Fischhoff, 2002). Often an appropriate understanding requires both qualitative information (e.g., where the risk originates and how it is assessed) and quantitative information (e.g., the frequency of the risk), and ideally, this will give qualitative meaning to the quantitative statistics (Fischhoff, 2002). It is important to note that effective communication is not only influenced by the actual facts regarding certain risks, but is also influenced by the factors that influence risk perception, highlighted previously (Slovic, 1986).

Risk can be communicated through a number of different media, including one-on-one discussions, group meetings, awareness seminars, emails and flyers (Pattinson & Anderson, 2007). The language used is also very important, and evidence suggests that it is unlikely that one particular technique will be appropriate for all communication media. Instead, it is often necessary to tailor the information based on the particular method of communication (Pattinson & Anderson, 2007). For instance, less formal and structured communication could be appropriate for one-on-one discussions, whereas an awareness seminar might be more effective if a highly structured format is utilised.

Information should also be tailored, as it is important to ensure that the message remains relevant to the intended audience (McIlwraith, 2006). It is also necessary to ensure that the information is not overcomplicated or negative, as it has been suggested that the vocabulary used within the information security field includes many terms that have "traditionally been used to talk down to people" (McIlwraith, 2006, p.70). For example, commonly used words include authority, compromise, violation, failure and control.

Furthermore, as mentioned previously, people are strongly influenced by the availability heuristic, and are more likely to act upon information that is easily recalled or remembered. Therefore, communication is more likely to be effective if it is phrased in a manner that should increase its memorability (Slovic, 1986). For example, it is possible that people may be more likely to follow information security guidelines if provided with case studies, describing incidents when individuals caused breaches, rather than just providing security rules. These specific incidents may be easier to remember, and hence, more likely to influence behaviour. Since people are more likely to remember information that they can relate to or identify with,

specific case studies that directly relate to the organisation in question are more likely to be effective (McIlwraith, 2006).

However, since many businesses do not view information security as a core aim, effective communication can be a difficult task, and it is therefore also necessary to ensure that all aspects of security are directly related to the strategy and objectives of the organisation in question (ISO, 2005). Also, businesses are generally more likely to act upon a potential risk if it is shown that the cost of mitigating techniques is lower than the potential cost posed by the risk (Dillon & Paté-Cornell, 2005). Furthermore, since organisational culture can have such a strong influence on the security of an organisation, when attempting to communicate information security aims, it is vital to frame the message so that it is both consistent with, and relevant to, the current culture (ISO, 2005).

The importance of appropriately framing or targeting information security messages is also emphasised by Pattinson and Anderson (2005). Messages can be framed or worded in different ways to place a different emphasis on certain aspects of the communication. For instance, some people might be more influenced by a message that stresses the organisational image and reputation, and the social costs associated with security breaches, whereas other people might be more influenced by their self image and how the information will influence them personally (Pattinson &Anderson, 2005).

Furthermore, computer users range from IT experts, who are more likely to be interested in the technical aspects of any potential risks, to novices, who are more likely to want information regarding exactly how and why any potential changes may influence their job role. Hence, it could be beneficial for information explaining why certain procedures are required to be targeted towards specific groups.

Evidence also suggests that aspects of individuals' personality or cognitive style are likely to influence the manner in which they respond to information regarding risk. This variation in regard to risk-taking behaviour means that it is extremely difficult to word a message so that it appeals to all users. Hence, the effectiveness of risk communication could be increased if the message is framed towards the various cognitive styles, with different messages for different styles (Pattinson & Anderson, 2005).

According to O'Neill (2004), people can be divided into four types based on the manner in which their behaviour is influenced by risk; some people seek out risk, others are risk tolerant, some are risk averse, and some deny risk. Since information regarding potential security threats is likely to influence these groups in very different ways, O'Neill (2004) argues that specifically designed messages are necessary for these different groups. For example, people who avoid or deny risk may be more influenced by information based on the worst possible outcomes and may be more likely to be reassured by positive information (Lion & Meertens, 2005). In contrast, information based on the worst outcomes may be less likely to influence people who thrive on risk-taking, and instead, such people could be more interested in information regarding the potential rewards or opportunities associated with their behaviour (Lion & Meertens, 2005).

Pattinson and Anderson (2005) suggest that the dimensions of Field Dependence and Field Independence could be used to frame threat scenarios relating to computer security, with the assumption that individuals should be more influenced by information aligned with their cognitive style. Field Dependence versus Field Independence relates to the extent to which individuals tend to perceive the more global and contextual elements of a situation. Generally, individuals with a more Field Dependent cognitive style are more people oriented, and place more focus on the overall implications of any situation. Hence, information aimed towards Field Dependent types should be framed to emphasise the social and global implications, the effect on people, and what individuals can do to prevent the risk (Pattinson & Anderson, 2005). In contrast, individuals with a more Field Independent style are less likely to be influenced by context or the social consequence of any decision (Pattinson & Anderson, 2005). Instead, information is more likely to be effective if it is framed to emphasise more practical and pragmatic solutions rather than the implications for people (Pattinson & Anderson, 2005).

There are also some factors that can decrease the effectiveness of communication. Although repeated exposure to a message can increase its memorability, and therefore increase the likelihood that people will appropriately respond to the risk, the opposite is also possible. Over-exposure can lead to automatic behaviour in which people disregard the message and appear apathetic (Pattinson & Anderson, 2007). Evidence also suggests that people prefer to receive factual information regarding exactly what will happen rather than statements of probability (Slovic, 1986). Finally, effective communication should be a two-way process, in which each side respects and values the insights provided by the other (Slovic, 1986). Without this cooperative process, communication breakdown is common.

5. Social Engineering

Social engineering is a term used to describe how one person persuades another person to give them the information that they want. In the context of information security, social engineering is very effective as it can utilise strategies that bypass computer technology (Schneier, 2000). Therefore, organisations that employ secure protocols and procedures, use cryptography, and have secure hardware and software are equally susceptible to social engineering attacks as those organisations where technical and computer security is lacking (Schneier, 2000). Social engineering is predominantly concerned with finding and exploiting vulnerabilities, and in most organisations the most vulnerable element is the employees; the human factor (Schneier, 2000).

Schneier (2000) explains that there are five steps to ensure a successful social engineering attack. First, the individual or target is chosen and all relevant information concerning that target is collected. Such information can include job advertisements, tender documents, published reports, company brochures and any other publicly available information, with the aim of gathering enough to heighten the perceived legitimacy of the attack (Aiello, 2008). Second, the collected information is then analysed and a vulnerability, which can be used to reach an objective, is determined. Third, access to the individual is then established. After all this preliminary work has been completed, then the attack can be performed. Finally, the attack can be completed and all evidence of the attack destroyed or removed (Schneier, 2000).

Schneier (2000) also discusses countermeasures that can be employed to reduce risk and vulnerability. Countermeasures consist of three parts that work in tandem: protection, detection and reaction. Since protection can never be guaranteed, a greater emphasis should be placed in detection and reaction. This should increase the chance that an organisation will know when a security breach has taken place and actions could then be taken to address that threat (Schneier, 2000).

Mitnick and Simon (2005) believe that social engineering attacks are very hard to detect and this makes them almost impossible to defend against. Mitnick and Simon (2005) classify social engineering attacks into three main categories: direct requests, contrived situations and personal persuasion.

Direct requests are the simplest approach, as attackers clearly and plainly ask for the information they require. Not surprisingly, this is the least successful approach, because it does tend to raise suspicion. Contrived attacks, however, are generally more successful. The attackers add information to make their story sound more convincing. For example, attackers may say that they have forgotten their password and require access into the system. Personal persuasion requires the most skill. When using personal persuasion the hacker aims to manipulate the individual into believing that they provided the information voluntarily, and by using this approach, the individual does not perceive any risk (Mitnick & Simon, 2005).

An example of social engineering was provided by Schneier (2000). In France, 1994, Anthony Zboralski contacted the FBI in Washington; he used a contrived situation and claimed to be an FBI representative who was currently working at the US embassy in France. His aim was to

discover how to use the phone conferencing system. This information was given to him by FBI staff and the consequence of this security breach was an FBI phone bill of a quarter of a million dollars (Schneier, 2000). He did not have to use any technical knowledge or strategies to gain this information. All he had to do was to fabricate a convincing story and ask for the information.

Another example was provided by the US Treasury Inspector General for Tax Administration, during their 2007 audit of the Internal Revenue Service (IRS) (Anderson, 2008). In this audit, 102 IRS staff from different levels of employment were contacted via telephone. These employees were asked to provide their user ids, and were also instructed to change their passwords to a provided value. Out of the 102 staff contacted, 62 did as they were instructed. Since IRS staff have access to extremely sensitive financial information, this disclosure indicated a huge potential security breach, and, if this was a genuine social engineering attack, the repercussions were potentially devastating. It was somewhat surprising that so many staff were so easily manipulated, especially given that similar audits were conducted in both 2001 and 2004 (Anderson, 2008).

Another common form of social engineering is referred to as *phishing*. Phishing is defined as:

> *"a form of social engineering in which an attacker, also known as a phisher, attempts to fraudulently retrieve legitimate users' confidential or sensitive credentials by mimicking electronic communications from a trustworthy or public organisation" (Myers, 2007,p1.).*

Phishing is usually done through email and phishers are most interested in obtaining passwords, and credit card and account numbers.

Data suggests that approximately five percent of individuals become victims of phishing attacks, and as a result, provide sensitive information to fake websites (Dhamija, Tygar & Hearst, 2006). However, since it is possible that some people may not admit their mistake, and others may not realise that they have unnecessarily disclosed sensitive information, it is difficult to obtain a valid approximation of the number of people who fall victim to phishing attacks (Egelman, Cranor & Hong, 2008). The Anti-Phishing Working Group maintains an archive of phishing attacks, and in January 2008 alone, 29,284 unique phishing reports were submitted, indicating that phishing is a common and serious problem (Anti-Phishing Working Group, 2008).

5.1 What Makes People Susceptible?

There are a number of factors that tend to increase an individual's susceptibility to social engineering attacks. Generally, social engineering attempts are more likely to appear legitimate if the attacker can form a trust relationship with the victim, making them more vulnerable to instruction (Aiello, 2008). There are also a number of individual factors or personality traits that can increase the likelihood of an individual falling victim to social engineering attacks. Additionally, there are a number of strategies used in phishing emails and illegitimate websites that can increase their effectiveness. This section will highlight these various factors that can increase an individual's susceptibility to attack.

5.1.1 Psychological Triggers and Individual Factors that Increase Susceptibility

As mentioned previously, social engineers will often use a contrived situation or personal persuasion to increase the chance that their request will be successful. The success of such attacks can also be increased by creating a situation in which certain psychological responses are triggered within the victim. Furthermore, it is possible that certain individuals are more likely to exhibit certain psychological responses, and therefore, peoples' susceptibility is likely to be associated with both the social engineers' ability to trigger responses, and also with aspects of the individuals' personality. These factors are described in detail below.

According to Workman (2008), susceptibility is greatly associated with individuals' likeability and trust, and people who are more trusting are more likely to succumb to social engineering attacks. Mitnick and Simon (2002) explain that it is human nature to trust people, particularly when their requests seem reasonable, and when they do not have any reason to be suspicious. Generally, people have a desire to be helpful, and they often lack appropriate assertiveness. Hence, social engineers can use this knowledge to exploit people, and they will often attempt to build a friendly rapport, knowing that victims are more likely to comply with any requests if they like or trust the attacker (Gragg, 2002).

People are also unlikely to be suspicious of requests that seem innocuous. If a social engineer asks for a small piece of seemingly harmless information, people generally want to be helpful, and are therefore likely to comply. Hence, social engineers often manage to obtain small pieces of information from various sources, and the various victims of the attack may not realise that they have been socially engineered, and have exposed useful information. For example, revealing the version of a particular piece of software or the name of a supervisor may not seem like important information, but a piece of information such as that could then be used to assist an attacker to socially engineer another employee.

Another effective technique involves creating an increased affect or heightened emotional state in the victim, which then enables the attacker to make requests that might be refused under normal circumstances (Gragg, 2002). When emotions such as surprise, excitement, anger, panic or fear are heightened, the victim is more likely to be easily distracted, and less likely to logically evaluate and question the attacker's story (Gragg, 2002). For example, an attacker could create a contrived situation in which the victim's job is threatened for misuse of company resources. The attacker could then offer to fix the problem, and could request the victim's password in order to complete this task (Aiello, 2008). In such a situation, the victim could be overwhelmed by the risk to his or her job, and may therefore be willing to comply with the request in order to eliminate the problem.

Similarly, feelings of guilt or moral outrage can also effectively reduce an individual's ability to logically validate any requests. Social engineers may therefore generate situations designed to create empathy, and the victim may comply with the request in order to help diminish the requester's problem (Aiello, 2008). Such techniques are particularly successful if the social engineer is able to build a connection with the target, and create a situation where the victim is able to identify with the attacker's trouble. In order to assist in this, social engineers will often gather information prior to any contact, which can be used to appeal to certain aspects of the target's personality or character, or can be used to make the target believe that they are

very alike (Gragg, 2002). Requests such as this are also more likely to be successful if the victim is led to believe that their action or inaction will have important consequences (Gragg, 2002). For example, the attacker may claim that the company could have a disastrous loss, which would be mitigated if the victim is able to help.

This idea is referred to by Workman (2008) as *affective commitment*. Essentially, when people feel an attachment or emotional bond to the social engineer, they are more likely to feel committed to divulge sensitive information (Workman, 2008). Generally speaking, peoples' level of commitment influences their susceptibility, and people who have higher levels of commitment are more likely to become victims of social engineering attacks. This is also supported by Cialdini (2006), who argues that once people have made a decision, they then feel pressure to remain consistent with that choice, and this pressure is often strong enough for people to act in ways that are contrary to their own interests.

Related to this, Workman (2007) also describes *normative commitment*, which is associated with the idea of reciprocation. Evidence suggests that people like to reciprocate when they have been assisted or have received a benefit (Cialdini, 2006), and people who are more normatively committed than the average person are more likely to feel obligated, and hence, are more likely to succumb to social engineering. Social engineers can use this to their advantage by appearing to act in a generous manner, resulting in a situation where the victim is more likely to provide reciprocal assistance to the attacker. An example of this form of psychological triggering is known as *reverse social engineering*, and it involves a situation where the attacker creates a problem, and then offers to assist the victim (Aiello, 2008). Since the victim in this example is unaware that the attacker was the one to cause the problem, he or she is likely to want to show gratitude or appreciation by assisting the attacker with any subsequent requests. Social engineers can also use reciprocation by requesting more than they actually want, and then reducing their requests. Evidence suggests that if one person yields on a point, the other person is likely to also yield on some part of the request (Cialdini, Green & Rusch, 1992).

Requests are also more likely to be followed if the target is overloaded with information. Hence, when flawed arguments are heard rapidly, and are listed together with convincing truths, people are more likely to be overloaded, and are therefore less likely to question the accuracy of the facts (Gragg, 2002). Similarly, people are also less likely to question unreasonable requests when they are faced with time pressure. Therefore social engineers will often call at unexpected or inconvenient times (such as at the end of the day) and will often indicate that a particular item or offer is scarce or only available for a short period of time (Cialdini, 2006). Evidence suggests that people tend to desire something more when there are limits placed on their ability to obtain it (Cialdini, 2006).

Evidence also suggests that social engineering is more effective when a bias known as *diffusion of responsibility* is utilised (Gragg, 2002; Aiello, 2008). Essentially, individuals are more likely to make decisions or provide information if they do not feel solely responsible for any consequences. Hence, the social engineer will often create situations designed to dilute the individual's feeling of personal responsibility, and the victim may then be more willing to assist the attacker (Gragg, 2002). This could include claiming that the individual's colleagues have already provided similar information, as the individual may then want to conform.

Furthermore, people are generally more likely to comply if they feel that they are only following orders, and therefore, social engineers may claim that the decision has been authorised by a supervisor or manager.

The influence of authority on individuals' decision-making abilities has been widely studied, and research has concluded that people are far more likely to obey a request when it is given by someone in a position of power (Gragg, 2002). For example, a study examined whether nurses would question a doctor's orders when they were clearly in violation of hospital policy (Hofling, Brotzman, Dalrymple, Graves & Pierce, 1966). The nurses received a phone call from an unknown doctor, asking the nurse to administer twice the maximum dosage of a drug that was not authorised for use on the ward. Despite these factors (and the fact that hospital policy prohibited nurses from administering drugs without a written order), 95% of nurses obtained the dosage, and would have administered it if they were not stopped by an observer (Hofling et al., 1966). This example shows that people often fail to question an authority figure, even when the orders clearly violate policy. Hence, social engineers can increase their chance for success by pretending to be someone in a position of power, and Workman (2007) suggests that people are more likely to become victims when they are more obedient and less resistant to pressure or threat.

5.1.2 Strategies used in Phishing Attacks and Illegitimate Websites to Increase Susceptibility

A small number of studies have also attempted to examine which social engineering strategies work, and why (Dhamija et al., 2006; Wu, Miller & Garfinkel, 2006; Friedman, Hurley, Howe, Felten & Nissenbaum, 2002).

A study by Dhamija and colleagues (2006) presented participants with twenty websites, and asked them to indicate the fraudulent sites. It was found that 23% of participants did not use common browser based cues such as the address bar, status bar and the security indicators. Consequently incorrect choices concerning the authenticity of a website were made at a rate of about 40%.

Dhamija et al. (2006) highlighted a number of characteristics that generally increased an individual's susceptibility to phishing attacks. They concluded that visual deception was a very successful strategy. Phishers often use visual tricks to convince the user that the text, images and windows that they are looking at are legitimate. This study illustrates that even in a situation where users are expecting to be presented with illegitimate websites they still have difficulty distinguishing a legitimate website from a fraudulent website. In fact, one of the phishing websites used in the study was able to deceive over 90% of participants. Dhamija et al. (2006) believe that these results reflect a lack of knowledge of how computer systems work, and highlight a lack of understanding of security systems and security indicators.

In a study conducted by Jackobsson, Tsow, Shah, Blevis and Lim (2007), participants were also required to evaluate selected websites and emails, and they were instructed to watch for signs of phishing. The aim of the study was to discover what cues subjects were using to determine if a website was authentic or a scam. They concluded that individuals paid close attention to URLs in websites, they were influenced by the layout of a web page and legitimacy was often

judged by content. It was also found that recognised third party endorsements strengthened confidence, and conversely, too much of an emphasis on security decreased confidence and increased suspicion. Likewise, padlock icons on websites did not always enhance trust. Personalisation, however, did tend to elicit trust; trust was also strengthened when there was the opportunity available to validate the site, such as a contact number to verify authenticity. Overall, participants were more likely to be suspicious of emails more than web pages and certainly more than phone calls (Jackobsson et al., 2007).

A study conducted by Egelman and colleagues (2008) examined the effectiveness of phishing warnings used in web browsers. The warnings provided by web browsers were either active or passive; active warnings interrupt a user's primary task, whereas passive warnings will not interrupt a user's task, and therefore do not demand as much attention. Sixty individuals participated in the study and it was found that when no warnings were presented, 97% of participants fell for at least one phishing email that directed them to a fraudulent website. When the web browser warnings were instigated, Egelman et al. (2008) found that active warnings were more successful that passive warnings. An active warning resulted in a 79% success rate, whereby the user did not divulge any personal information; this is in contrast with a much lower success rate of 13% when passive warnings were used. Given these findings, Egelman and colleagues (2008) recommended that web browsers should employ active warnings that interrupt the primary task and draw the attention of the user. They also suggested that these active messages need to make clear recommendations to the user about what actions they should take.

These studies show that current security indicators are not proving to be effective and therefore there is a need to develop new strategies to deal with ever more sophisticated social engineering and phishing attacks.

5.2 Previous Studies of Social Engineering

A small number of studies have attempted to empirically analyse how people respond to social engineering attacks. For example, Jagatic, Johnson, Jakobsson and Menczer (2007) conducted a study on the social engineering phenomenon of phishing. In their study, Jagatic and colleagues (2007) launched actual phishing attacks on 921 Indiana University students, with the aim of studying whether people would be more likely to respond to phishing style emails when they were sent by friends rather than an unknown person. This area of study is particularly important, as phishing attacks are increasingly using contextual elements, and, based on the psychological triggers that tend to make people more susceptible, targeted attacks are potentially much more dangerous (Jagatic et al., 2007).

Using information gained on publicly available sites, they discovered social networks, and then sent emails to students, pretending to be a friend. A control group received emails from a fictitious university email address. The link in the email took participants to a webpage, where they were asked to enter their university ID and password. Participant selection was dependent on the amount and quality of publicly available information accessed on social networking websites. This study was somewhat controversial as participants could not be informed of the details of the study (and provide their consent) prior to commencement, as this would have influenced responses (Jagatic et al., 2007).

The phishing acts carried out on the control group, where no social context was used, had a success rate of 16%, compared to a success rate of 72% when using information gathered from social networks (Jagatic et al., 2007). It was concluded that using a social context resulted in participants ignoring important cues, making them more vulnerable to attack. Gender differences were also observed, with females being more easily targeted, and there was also a correlation with age, with younger participants being more susceptible. Interestingly, particularly for males, the attack was more effective when it appeared as though the email was sent by a person of the opposite gender, with the response rate for males increasing from 53% when the message was from a male, to 68% when it was sent by a female. This research is important as it was the first study to report a baseline figure for phishing attacks, both traditional attacks and those completed within a social context (Jagatic et al., 2007).

Another study examined the behaviour of employees at a South African university (Steyn, Kruger & Drevin, 2007). One of four types of emails was sent to 1600 participants. The first two emails were both questionable and designed to be suspicious. The first email contained an HTML link; participants were informed that this link would provide beneficial information about personal finances. Of the 400 randomly selected staff members who received this email, 295 opened the email, and of those staff members, 147 (49.8%) clicked on the link. The second suspicious email requested participants to open an attachment. In this instance, 213 participants opened the email, and 53 of those staff members (24.9%) opened the attachment. The success rate of this particular email was the lowest of the four types of emails that were sent, and this is most likely due to a high level of awareness among users about virus threats. Emails three and four were designed to appear to be legitimate. Email three requested staff members to follow a web link which asked participants to disclose private information, which could be used for identity theft. Of the 400 participants who received this email, 320 participants opened the email, and 171 (53.4%) of those participants provided sensitive information. The fourth email asked participants to run an executable file, which would improve computer performance, and 117 of the 265 individuals who opened the email (44.2%) complied with the request (Kruger, Drevin & Steyn, 2007).

A similar study conducted at West Point Military Academy highlighted the influence of regulations and authority (Ferguson, 2005). A bogus email was sent from a fictitious colonel to 512 cadets, informing them of a problem with their grade. The provided location for the fictitious colonel was deliberately fabricated (the seventh floor of a building that does not have seven floors), and despite regularly visiting this building, the vast majority of the cadets failed to notice this cue. An average of 80% of students clicked on the embedded link, and this number rose to ninety percent for the freshmen, despite the fact that the freshmen had received four hours of security awareness training (Ferguson, 2005). This study highlights the influence of authority on individuals' decision-making abilities.

Furthermore, the study also emphasises the effect that a heightened emotional state can have on an individuals' ability to rationalise a decision. The cadets received the email towards the end of the semester, which is a time when students are likely to be particularly responsive to any reference to their grades. The fact that the email mentioned a 'problem' with their grades may have created anxiety in the cadets, resulting in a situation where they were less likely to

focus on the cues that should have made them suspicious about the email, and hence, this may have increased the probability of them clicking on the link.

5.3 Defences Against Social Engineering

According to Schneier (2000), there are three parts to an effective set of countermeasures, which should work in tandem. These are protection, detection and reaction. If an organisation has strong protection then it may be possible to place less emphasis on detection and reaction mechanisms. Conversely, if an organisation has weak protection mechanisms, it needs to invest in its detection and reaction mechanisms (Schneier, 2000).

There are several defences that an organisation can use to protect itself against social engineering threats, and many of these are common sense actions that are simple to implement. Essentially, many of the defences against social engineering are associated with effective security awareness and training. Security awareness and training is explained in more detail in a subsequent section. Despite this, the aspects of security awareness that are specifically relevant to social engineering will be outlined below.

These defences include ensuring that everyone who enters the premises of an organisation is required to show identification, including employees, contractors, business partners, vendors and all visitors. This strategy is crucial because many social engineers simply walk into an organisation; they behave like one of the employees, and in many situations, they are not challenged. This is particularly relevant within large organisations, where employees are accustomed to seeing people who they do not recognise (Schneier, 2000).

In an effort to further secure the premises of an organisation it is recommended that workstations and servers are kept in separate rooms and that access to these rooms is through the use of secure swipe cards. Employees should only be granted access to the rooms and areas that are contingent on their work roles. This makes it easier to monitor who enters a room and helps to ensure that only authorised individuals have right of entry. Of course, employees will have to be diligent to ensure that the door is always securely closed once they have entered so that unauthorised personnel cannot follow them in.

Another very simple strategy is to invest in shredders; sensitive and valuable information can be easily obtained by going through the rubbish bins of an organisation. Information found in this manner could be used by a social engineer to increase the credibility of any request. A policy in which all paper documents are required to be shredded rather than placed in a bin would eliminate this threat (Schneier, 2000). Following on from this, there is a need to apply technology wherever possible. As an example, an organisation can ensure that there is sufficient physical security and computer security, such as firewalls, and organisations should also ensure that they can trace phone calls and place a limit on the number of phones that can be used to make overseas calls. This is important as it can minimise the financial loss to an organisation.

Sensitivity when dealing with passwords is another major concern in information security (Gragg, 2002). Social engineers are quite successful at contacting employees and obtaining password details and often this is achieved simply by pretending to be a system

administrator. Password details are commonly left stuck on computers or written down in diaries. Social engineers know where to look for this information. Therefore employees need to be educated about these dangers; they need to know that under no circumstances should they ever provide password details over the phone, and that they should never leave password information lying around the office. Of course, to achieve this, employees need to be educated about how to behave and the consequences of their actions. It is recommended that organisations regularly check workstations to ensure that passwords have not been written down and cannot be easily located.

Another message that should be reiterated to employees is the danger of revealing sensitive information over the phone; password details should certainly never be communicated over the phone and great care needs to be taken when providing any other information. For example, if an employee is contacted by someone asking for sensitive information, who claims to be from an internal helpdesk, the employee should advise the caller that they will call them back shortly; this gives the employee time to check credentials first before they provide any information. Related to this, it is also important to ensure that employees are educated on what exactly constitutes 'sensitive' information.

Employees also need to be vigilant about the safety of their laptops. Laptops are much more difficult to secure within an organisational environment and they often contain a great deal of important and sensitive information. Therefore all laptops should be required to be kept as secure as possible, which means keeping them locked in secure areas when they are not in use and ensuring that they are encrypted and use secure password protection.

Another simple strategy that can improve security is to ensure that all staff 'lock' their computer whenever they leave their workstation. Even if they are only leaving their workstation for a short period of time, the computer should always be locked and secured to prevent unauthorised use.

Although all employees are vulnerable to social engineering attacks there are those employees who are more vulnerable than others. This vulnerability and increased susceptibility is usually a direct result of job roles and responsibilities. Positions most at risk include those where there is a high level of contact and interaction, either with the public, customers, service providers or even internal employees. This may include positions in administration, human resources and help desks. Individuals in these roles are more accustomed to dealing with strangers and are exposed to a wide variety of requests. To illustrate, consider an organisation that has a human resource position which requires an employee to be the contact for all job applications and enquires. This job has a great deal of external interaction with name and contact details supplied on all job advertisements. This makes the employee a target and certainly more susceptible to a possible attack. What is appealing to a social engineer is that they now know their name, contact details and position, without having to ask and raise unnecessary suspicion.

Social engineers will often use intimidation and display elusive behaviours. For example, they may not provide any contact details and they may rush a conversation. It is also common for them to drop names of important people within the organisation and the listener will find that they often make small mistakes about details or information. The target should certainly

become cautious when a caller requests information that is forbidden or classified, as a fellow employee should know not to ask for such information. By becoming familiar with common techniques, an employee will be better equipped to identify a potential threat. Employees should also be trained in regard to what response needs to be made once a potential threat has been identified. All employees should know what policies are in place and who they need to contact to initiate a fast and effective response.

For example, organisations could implement an 'Information Security Threat Checklist' that is similar to the 'Bomb Threat Checklist' that many organisations already use. The checklist would prompt employees to gather standard or general information, such as the gender of the caller, any characteristics of their voice, any distinct or identifiable background noises, what they asked for and whether they appeared to have any familiarity with the computer system (Kovacich & Jones, 2006). It is suggested that the checklist also provide a list of social engineering techniques that are used to obtain sensitive information, which would assist in alerting the employee to suspicious behaviour. The checklist should also provide information on reporting procedures and advise the employee on what to do with the call and who they need to contact to initiate further action (Kovacich & Jones, 2006). In terms of communication, prevention and reaction, such a list could be very effective.

6. Security Awareness, Training and Education

Security awareness, training and education are some of the most effective countermeasures against the human factor threats to information security. Various aspects of these countermeasures have already been mentioned throughout this report. This section will expand on the information already provided, outlining a number of components associated with effective awareness, training and education.

According to the National Institute of Standards and Technology (NIST) report on security awareness and training, "[l]earning is a continuum; it starts with awareness, builds to training, and evolves into education" (Wilson & Hash, 2003, p.7). The goal of awareness is to ensure that individuals are aware of potential IT security concerns and know how to recognise and react to such concerns (Wilson & Hash, 2003). Training goes a step beyond this, and aims to produce the required security skills and competencies. The aim of education is to integrate those security skills and competencies into a body of knowledge, and education "strives to produce IT security specialists and professionals capable of vision and pro-active response" (Wilson & Hash, 2003, p.9).

Besnard and Arief (2004) emphasise the education of staff, stressing that although education may not alter behaviour on its own, education makes people aware of the consequences of their actions. It ensures that individuals are conscious of the threats and the potential damages that can result from insecure behaviours (Besnard & Arief, 2004). However, despite the importance of education as a defence against information security threats, it is often lacking. According to the 2007 SCI Computer Crime and Security Survey, 18% of organisations do not use any form of awareness training and 35% of organisations who do train their staff do not measure the effectiveness of their security awareness programs (Richardson, 2007).

In another recent survey (Ernst & Young, 2007), it was found that security training and awareness rate in the top five concerns for executives. Although executives are able to recognise its importance, the implementation of the training programs can be difficult. Essentially, the design of any awareness or training program is complicated and is dependent on the organisation in question. Hence, in order to be successful, any information security initiative should begin with a needs assessment.

A needs assessment involves gathering information regarding the current processes in place, the knowledge that is required of staff, and the gaps in the current information security initiatives (Wilson & Hash, 2003). There are a number of sources that can be utilised to obtain such information. For example, members of the organisation could be asked to complete surveys or questionnaires. These generally aim to determine how regularly the employees perform certain duties, whether they have previously received training in the information security procedures associated with those duties, and if so, the sort of training that was provided. For more detailed information, executive management, security personnel, systems administrators and other relevant staff members could be interviewed to obtain a more thorough understanding of their security awareness and training needs (Wilson & Hash, 2003).

When performing a needs assessment, it is also important to examine and review all current material. Furthermore, an analysis of any measurements associated with current or past training and awareness programs is also useful. This could include information such as the number of people from various roles who have previously received training. Similarly, it is also important to examine any information regarding previous information security beaches or events. Such information is useful as it may highlight a need for training for a particular group of people, or in a particular area of information security.

Once an organisation's information security needs have been determined, it is then possible to develop a strategy and plan for the program. This plan should cover a number of aspects: the goals, the learning objectives and frequency of the program; the topics to be addressed; the mode of presentation; the methods of feedback and evaluation; and the roles and responsibilities of all people involved in the design, development, implementation and maintenance of the information security initiative (Wilson & Hash, 2003). It is also necessary to develop priorities for the information security program, which could be influenced by aspects such as budget constraints and resource availability (Wilson & Hash, 2003). For example, there are a number of important topics in information security, but since the resources and funds may not always be available to provide extensive awareness, training and education to all employees in all areas, it is usually necessary to prioritise.

Following this, the information security initiative can be developed. Essentially, any behaviour that should be reinforced can be addressed in awareness programs, and any skills that the employees need to learn and apply can be addressed in a training program (Wilson & Hash, 2003). As mentioned previously, the information security message can be disseminated through a number of different media. For example, an awareness message could be disseminated via methods such as posters, screensavers, newsletters, DVDs, awards programs, computer-based sessions, and in-person, instructor-led sessions (Wilson & Hash, 2003). Training programs are most likely to involve video-based, computer-based or instructor-led training sessions. It is important to make any awareness or training program interesting and current, and users' retention of information can be increased through repetition of the message and dissemination of the message using multiple techniques (Wilson & Hash, 2003).

There are also a number of factors that should be taken into account when developing a successful awareness or training program. For example, according to Wilson and Hash (2003), the success of any information security initiative is strongly associated with the manner in which the program is aligned with the organisation's mission. This is also supported by Ernst and Young's 2007 Global Security Survey, which indicates that any information security initiatives should be developed with the strategic objectives of the organisation in mind (Ernst & Young, 2007). Furthermore, rather than having a reactive approach, where information security is viewed as a "cost of doing business", (Ernst & Young, 2007, p.5), it is instead vital to view information security as critical to the business.

Furthermore, in order to be successful, learning needs to be personal, meaningful and contextualised, as evidence suggests that programs are more likely to be successful if the users feel that the subject matter and issues presented are relevant to their own needs (Wilson &

Hash, 2003). Unfortunately, most awareness and training programs are generic in design, with a 'one size fits all' approach. This approach tends to fail because the needs of individual staff members are not taken into consideration, and therefore the impact of the training message can be compromised (Ernst & Young, 2007).

Not only should training be individually tailored, it should also be structured in a way that is memorable and leaves a lasting impression. As mentioned previously, case studies are an effective way to communicate a message to an audience (McIlwraith, 2006). Case studies generally involve specific, real-life examples, and evidence suggests that they promote active engagement in the learning process, and allow students to obtain a greater understanding of the meaning and application of theory (Brooke, 2006). The value of case studies was also demonstrated by Herreid (1994), who reported an increase in student attendance from 50-65% for traditional lectures, to 95% when case studies were utilised. Training also needs to be reinforced, and should be designed with follow up training sessions conducted at future dates to strengthen the security message.

The use of positive reinforcement could also assist to strengthen the security message. Psychological research has demonstrated that positive reinforcement, in which desired behaviours are rewarded, is an extremely effective tool in shaping behaviour (Skinner, 1953). Hence, this suggests that positive information security behaviours could be increased by rewarding those who have demonstrated the correct information security behaviours. In other words, rather than simply punishing those who are found to breach security rules, the people found to obey them would be rewarded. Despite the effectiveness of this technique, the results of the 2007 Global Security Survey indicated that only 3% of organisations list the recognition of exemplary behaviour as a tool in information security awareness and training (Deloitte, 2007).

Employees also need to be educated about risk perception biases such as the availability heuristic and the optimism bias. As already discussed, these biases can influence an individual's ability to make sensible decisions regarding possible risk. For example, the availability heuristic implies that individuals are more likely to underestimate the risk of ignoring procedures if they had previously ignored procedures without adverse consequences (Slovic et al., 1976). The optimism bias states that people are more likely to underestimate a risk to themselves and overestimate a risk to others (Gray & Ropeik, 2002). Furthermore, an individual's perception of risk can be influenced by personality and cognitive styles, social factors, framing and familiarity. It is by educating employees about these phenomena that may contribute to a positive change in behaviour; by increasing the level of knowledge you can potentially decrease the risk.

Training programs also need to educate staff on common techniques used by social engineers in an effort to better protect themselves from becoming a victim (Gragg, 2002). Employees should be able to recognise key strategies used by social engineers and some of these psychological strategies have already been described. For example, social engineers will often avoid providing contact details, they may call at unexpected times and they may attempt to produce an emotional response. Effective training should ensure that employees are aware of these possible social engineering techniques, and are equipped with appropriate responses.

Generally speaking, there is also a need for security policies to be strengthened to provide clear guidelines and instructions. They should cover areas where security breaches are most likely to occur. For example, they need to explain what the procedure is to change passwords, what the procedures are to contact the helpdesk, and in what situations and how the helpdesk contacts individual employees. Policies should explain access privileges, security restrictions in sensitive areas, privacy policies, how to handle sensitive information and how to deal with and report security violations. These guidelines and instructions, when combined with sound education and training programs, should reduce the success of social engineering attacks (Gragg, 2002).

Although the utilisation of effective procedures is essential when promoting a positive safety culture, it is also necessary to ensure that organisations do not put procedures in place just for the sake of having the procedures there (Besnard & Arief, 2004). Individuals are more likely to follow procedures when they know why they are necessary. This is an important recommendation because people very rarely follow procedures to the letter; they often make changes to simplify the process and reduce their workload. It is therefore important to ensure that employees understand the procedures, and the reasons why adherence to those procedures is required.

Mitnick and Simon (2005) make many similar recommendations to the ones stated above. They also add that an organisation needs to clearly state its security protocol to all its employees, along with having simple rules that define what information is sensitive to the organisation; this can be effectively achieved by using a data classification system. Mitnick and Simon (2005) also stress the importance of having a rule in place by which anyone who is requesting sensitive information will be required to provide verification of their identity. They also encourage security awareness training programs to be implemented, along with training specific to social engineering, specifically teaching staff how to resist social engineering attacks. Their final recommendation is for organisations to test their level of security by conducting an independent security assessment, which will provide feedback on both security strengths and weaknesses (Mitnick & Simon, 2005).

Essentially, employees should be provided with awareness training when they start working for an organisation and this training should be reinforced regularly, and appropriately evaluated. It is important for management to set the example for IT security, by displaying the desired behaviours (Wilson & Hash, 2003).

6.1 The Evaluation of Security Awareness, Training and Education

To determine the effectiveness of any security awareness, training and education program, evaluation and feedback mechanisms need to be established. Feedback and evaluation are necessary to determine if security objectives have been effectively communicated, to gauge how the current program is working, and to identify where changes and improvements to the program can be made (Wilson & Hash, 2003).

Feedback can be obtained through various means, including evaluation forms and questionnaires, focus groups, interviews, observations and formal reports. Another strategy that can be used is known as security program benchmarking. This approach is longitudinal

and requires the collection of extensive data and information from various organisations over at least a five year period. The performance of each organisation is compared to the performance of other organisations; this benchmarking approach explores various aspects of organisational performance including security awareness, training and education (Wilson & Hash, 2003).

Another central component to effective awareness, training and education programs is the management of change. This is crucial to ensure that the program and strategies remain current and relevant to a particular organisation and its unique culture (Wilson & Hash, 2003).

7. Conclusions

It is important to keep in mind the human factors that influence behaviour. These factors have been extensively described and examined in this report. They include the ways in which individuals make decisions and the biases and heuristics that affect risk perception, including the availability heuristic and the optimism bias (Lichtensteiner et al., 1978). They also include the impact that knowledge and control can have on decision-making processes; if individuals' level of knowledge is limited then they may not understand the magnitude of a security risk (Fischhoff, 2002). Individuals' level of control is also important; if people feel a great sense of control over what they are doing, they tend to take more risks and overestimate their ability to control a threat (Slovic et al., 1978).

Understanding a threat or a risk can also be compromised by risk homeostasis, where individuals are observed to take more risks in situations that are perceived as less risky and reduce risk-taking in situations that are perceived as more risky (Wilde, 2001). It is also important not to overlook the impact of cumulative risk, which is observed when a group of individuals take small risks, which, on their own, may be perceived as harmless, but the accumulation may create substantial vulnerabilities (Slovic, 2000). The omission bias, the familiarity of a risk and the way in which the risk is described can also influence the perception of a risk.

Of course, the impact of individual differences and social factors cannot be overlooked. Personality factors and cognitive styles contribute to differences in risk perception (Lion & Meertens, 2005). Group norms in various social settings greatly influence how individuals will not only perceive a risk, but also how they will respond to that risk. Related to this is the effect of the organisational culture and climate.

The culture of organisations can differ greatly. The socialisation process or integration experienced by employees is a reflection of an organisation's culture (Feldman & Brett, 1983). Culture can also be affected by various employment factors such as job satisfaction, motivation, leadership and commitment. Sub-cultures often also develop within an organisation's culture (Hampden-Turner, 1990). All of these factors intertwine and impact on attitudes, behaviours and values. Security culture is part of the overall culture and has been explained in this report by using the organisational culture framework. Organisational climate is a similar construct to organisational culture and research has shown that a positive relationship between safety climate and employee behaviour tends to improve information security (Chan et al., 2005).

One form of security threat that is continuing to increase is the threat of social engineering attacks. All organisations are vulnerable to social engineering attacks, and one of the most common social engineering attacks is known as phishing. Phishing attacks are orchestrated through email and often their primary aim is to obtain credit card and bank account details and passwords (Myers, 2007). Some individuals are more susceptible to such attacks than others; this is because of individual differences, such as personality traits (Workman, 2008).

Phishing email attacks and fraudulent websites are increasing in sophistication. They employ visual tricks and rely on the failure of current security indicators for success (Dhamija et al., 2006). Several defences against social engineering can be used to reduce the threat and they include such actions as using shredders to destroy sensitive information, employing sufficient physical security and computer security measures, and importantly the education, training and awareness of staff. Since humans are the targets of social engineering attacks, education is one of our greatest defences. Education and training need to be individually tailored, continually reinforced, and implemented effectively and appropriately to make a significant impact (McIlwraith, 2006).

Human factors in information security certainly present many complex and dynamic issues. There are many variables that need to be taken into account, including not only individual differences and differences in personality traits, but also interactions and influences of organisational culture and climate. There is a need for more empirical studies and research, particularly in the areas of phishing, social engineering, and education and training. The issue of security also needs to be assessed as the economic issue that it is, with tradeoffs between costs and benefits (Odlyzko, 2003). Users want both security and flexibility, and finding a balance between these two factors is certainly challenging. There is no one solution to improving information security, but rather, several complementary approaches should be implemented to improve computer security and human interaction with security systems.

8. Reference List

Adams, A. & Sasse, M.A. (1999). Users are not the enemy. *Communications of the ACM, 42(12)*, 41-46.

Aiello, M. (2008). Social engineering. In L.J. Janczewski & A.M. Colarik (Eds.), *Cyber Warfare and Cyber Terrorism* (pp. 191-198). Hersey, PA: IGI Global.

Anderson, R.J. (2008). *Security Engineering: A Guide to Building Dependable Distributed Systems* (2nd ed.). New York: Wiley.

Anti-Phishing Working Group, (2008). *Phishing Activity Trends: Report for the Month of January, 2008*. Accessed online June 2008, http://www.antiphishing.org/reports/apwg_report_jan_2008.pdf

Bener, A.B. (2000). *Risk Perception, Trust and Credibility: A Case of Internet Banking*, PhD thesis, London School of Economics and Political Sciences, London.

Besnard, D. & Arief, B. (2004). Computer security impaired by legitimate users. *Computers and Security, 23*, 253-264.

Brooke, S. (2006). Using the case method to teach online classes: promoting Socratic dialogue and critical thinking skills. *International Journal of Teaching and Learning in Higher Education. 18(2)*. 146.

Buono, A. F., Bowditch, J.L. & Lewis, J. W (1985). When cultures collide: The anatomy of a merger. *Human Relations, 38(5),* 477-500.

Chan, M., Woon, I. & Kankanhalli, A. (2005). Perceptions of information security at the workplace: Linking information security climate to compliant behavior, *Journal of Information Privacy and Security, 1(3)*, 18-42.

Cialdini, R.B. (2006). *Influence: The Psychology of Persuasion* (Rev. ed.). New York: HarperCollins.

Cialdini, R.B., Green, B.L. & Rusch, A.J. (1992). When tactical pronouncements of change become real change: The case of reciprocal persuasion. *Journal of Personality and Social Psychology, 62(1)*, 30-40.

DeCotiis, T.A. & Summers, T.P. (1987). A path Analysis of a Model of the Antecedents and Consequences of Organizational Commitment. *Human Relations, 40(7)*, 445-470.

Deloitte (2007). 2007 Global Security Survey: The Shifting Security Paradigm. Deloitte Touche Tohmatsu.

Deter, J., Schroeder, R. & Mauriel, J. (2000). A framework for linking culture and improvement initiatives in organisations. *The Academy of Management Review, 25(4)*, 850-863.

Dhamija, R., Tygar, J.D. & Hearst, M. (2006). Why phishing works. *Proceedings of the ACM CHI 2006 Conference on Human Factors in Computing Systems.* April 22-27. pp. 581-590.

Dillon, R.L. & Paté-Cornell, E. (2005). Including technical and security risks in the management of information systems: a programmatic risk management model. *Systems engineering. 8(1)*, 15-24.

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 ACM CHI 2008 Conference on Human Factors in Computing Systems.* April 5-10, 2008. pp. 1065-1074.

Ernst & Young (2007). 10th Annual Global Information Security Survey: Achieving a Balance of Risk and Performance. Ernst & Young.

Feldman, D.C. & Brett, J.M. (1983). Coping with new jobs: A comparative study of new hires and job changers. *Academy of Management Journal*, *26(2)*, 258-272.

Ferguson, A. (2005). Fostering e-mail security awareness: The West Point Carronade. *Educause Quarterly, 28(1)*, 54-57.

Fischhoff, B. (2002). Assessing and communicating the risks of terrorism. In A.H. Teich, S.D. Nelson, & S.J. Lita (Eds.), *Science and technology in a vulnerable world* (pp. 51-64). Washington, DC: AAAS.

Freeman, E. (2000). E-merging risks: operational issues and solutions in a cyber age. *Risk Management , 47(7)*, 12-15.

Friedman, B., Hurley, D., Howe, D., Felten, E., Nissenbaum, H. (2002). Users' conceptions of web security: a comparative study. *CHI '02 extended abstracts on Human factors in computing systems*, Minneapolis, Minnesota, 746-747.

Furnell, S. (2005). Why users cannot use security. *Computers and Security, 24*, 274-279.

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

Furnham, A. & Gunter, B. (1993). Corporate Culture: Diagnosis and Change. In Cooper, C.L. & Robertson, I.T. (Eds.), *International Review of industrial and Organisational Psychology*. Chichester: Wiley.

George, J.M. & Jones, G.R. (1996). *Understanding and Managing Organizational Behavior*. Reading, MA: Addison-Wesley Publishing Company.

Gragg, D. (2002). A multi-level defense against social engineering. White paper, SANS Institute,
Retrieved on June 12, 2008 from http://www.sans.org/rr/papers/51/920.pdf

Gray, G.M., & Ropeik, D.P. (2002). Dealing with the dangers of fear: The role of risk communication. *Health Affairs, 21*, 106-116.

Hampden-Turner, C. (1990). *Corporate Cultures: From vicious to virtuous circles.* London: Random House.

Heimer, C.A. (1988). Social structure, psychology, and the estimation of risk, *Annual Review of Sociology, 14*, 491-519.

Herreid, C. F. (1994). Case studies in science: A novel method of science education. *Journal of Computer Science and Technology, 23(4)*, 221-229.

Hofling, C.K., Brotzman, E., Dalrymple, S., Graves, N. & Pierce, C.M. (1966). An experimental study in nurse-physician relationships. *Journal of nervous and mental disease, 143(2)*, 171-180.

Horvath, P., & Zuckerman, M. (1993). Sensation seeking, risk appraisal, and risky behavior. *Personality and Individual Differences, 14*, 41-52.

Huang, D., Rau, P.P. & Salvendy, G. (2007). A survey of factors influencing people's perception of information security. In J. Jacko (Ed.). *Human-Computer Interaction, Part IV*. Heidelberg: Springer.

Huczynski, A. & Buchanan, D. (2001). *Organizational Behaviour: An Introductory Text* (4th ed.). United Kingdom: Prentice Hall.

ISO (2005). ISO/IEC 17799 Information technology - Security techniques - Code of practice for information security management. Second edition 2005-06-15. Reference: ISO/IEC 17799-1:2005(E). Pages 1-115.

Ivancevich, J., Olekalns, M. & Matterson, M. (2000). *Organisational Behaviour and Management.* Sydney: McGraw Hill.

Jakobsson, M., Tsow, A., Shah, A., Blevis, E & Lim, Y. (2007). What Instils Trust? A Qualitative Study of Phishing. 11th International Conference, FC 2007, and 1st International Workshop on Usable Security, USEC 2007, Scarborough, Trinidad and Tobago, 365-361.

Jagatic, T.N. Johnson, N.A., Jakobsson, M. & Menczer, F. (2007). Social phishing. *Communications of the ACM, 50(10)*, 94-100.

Kahneman, D., Slovic, P., & Tversky, A. (1982). *Judgment under uncertainty: Heuristics and biases*. New York: Cambridge University Press.

Kahneman, D., & Tversky, A. (1979). Prospect Theory: An Analysis of Decision under Risk, *Econometrica, XLVII*, 263-291.

Katsabas, D., Furnell, S.M. & Dowland, P.S. (2005). Using human computer interaction principles to promote usable security, *Proceedings of the Fifth International Network Conference (INC 2005)*, Samos, Greece.

Koh, K., Ruighaver, A.B, Maynard, S. & Ahmad, A. (2005). Security governance: its impact on security culture. *Proceedings of the Third Australian Information Security Management Conference*, Perth, Australia, September.

Kovacich, G.L & Jones, A. (2006). *High-Technology Crime Investigator's Handbook: Establishing and Managing a High-Technology Crime Prevention Program*. Boston: Butterworth-Heineman.

Kreuter, M.W., & Strecher, V. (1995). Changing inaccurate perceptions of health risk: Results from a randomised trial. *Health Psychology*, *14*, 55-63.

Kruger, H., Drevin, L., & Steyn, T. (2007). Email Security Awareness – A Practical Assessment of Employee Behaviour. In L. Futcher & R. Dodge (Eds.) *IFTP International Federation for Information Security Education*. Boston: Springer, 33-40.

Kruger, H.A. & Kearney, W.D. (2006). A prototype for assessing information security awareness. *Computers and Security, 25*, 289-296.

Lacohee, H., Phippen, A.D. & Furnell, S.M. (2006). Risk and restitution: Assessing how users establish online trust. *Computers and Security, 25*, 486-493.

Lichtenstein, S., Slovic, P. Fischhoff, B., Layman, M., & Combs, B. (1978). Judged frequency of lethal events. *Journal of Experimental Psychology: Human Learning and Memory, 4,* 551-578.

Lion, R. & Meertens, R.M. (2001). Seeking information about a risky medicine: effects of risk-taking tendency and accountability. *Journal of Applied Social Psychology, 31*, 778-795.

Lion, R. & Meertens, R.M. (2005). Security or opportunity: the influence of risk-taking tendency on risk information preference. *Journal of Risk Research 8(4)*, 283-294.

Martin, J. & Siehl, C. (1983). Organizational cultures and counterculture: an uneasy symbioses. *American Management Association, 12(2)*, 52-64.

McIlwraith, A. (2006). *Information Security and Employee Behaviour: How to Reduce Risk Through Employee Education, Training and Awareness*. Aldershot, UK: Gower Publishing Limited.

McNeil, B.J., Pauker, S.G., Sox, H.C., & Tversky, A. (1982). On the elicitation of preferences for alternative therapies. *The New England Journal of Medicine, 306*, 1259-1262.

Mitnick, K.D. & Simon, W.L. (2005). *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers*. Indianapolis, ID: Wiley Publishing, Inc.

Mitnick, K.D. & Simon, W.L. (2002). *The Art of Deception: Controlling the Human Element of Security*. Indianapolis, ID: Wiley Publishing, Inc.

Morrow, P.C. (1983). Concept of redundancy in organizational research: The case of work commitment. *Academy of Management Review, 8*, 486-500.

Muchinsky, P.M. (1977). Organizational communication: Relationships to organizational climate and job satisfaction. *Academy of Management Journal, 20(4)*, 592-607.

Myers, S. (2007). Introduction to phishing. In M. Jakobsson & S. Myers (Eds.). *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft* (pp. 1-29). New York: Wiley-Interscience.

Needle, D. (2000). Culture at the level of the firm: organizational and corporate perspectives. In J. Barry, J. Chandle, H. Clarck, R. Johnson & D. Needle (Eds.). *Organization and Management: A Critical Text*. London: Business Press.

Norman, D. A. (1981). Categorization of action slips. *Psychological Review, 88(1)*, 1-15.

O'Neill, B. (2004). *Developing a Risk Communication Model to Encourage Community Safety from Natural Hazards*, paper presented at the Fourth NSW Safe Communities Symposium, Sydney, NSW.

O'Neill, B. & Williams, A. (1998). Risk homeostasis hypothesis: a rebuttal. *Injury Prevention, 4*, 92-93.

Odlyzko, A.M. (2003), Economics, psychology, and sociology of security, in R.N. Wright (Ed.). *Financial Cryptography: 7th International Conference, FC 2003*, Springer, New York, NY, Lecture Notes in Computer Science No. 2742, pp.182-9.

Ortiz, Resnick & Kengskool, (2000). The effects of familiarity and risk perception on workplace warning compliance. *Proceeding of the International Ergonomics Association*, San Diego, CA., 826–829.

Parker, C.P., Baltes, B. B., Young, S.A., Huff, J.W., Altmann, R.A., Lacost, H.A. & Roberts, J.E. (2003). Relationship between psychological climate perceptions and work outcomes: a meta-analytic review. *Journal of Organizational Behavior, 24*, 389-416.

Pattinson, M. & Anderson, G. (2007). How well are information risks being communicated to your computer end-users? *Information Management and Computer Security, 15(5)*, 362-371.

Pattinson, M. & Anderson, G. (2005). Risk communication, risk perception and information security. In P. Dowland, S. Furnell, B. Thuraisingham and X. Wang (Eds.). *Security Management, Integrity, and Internal Control in Information Systems*, Proceedings of *IFIP TC-11 WG 11.1 & WG 11.5 Joint Working Conference on Security Management, Integrity, and Internal Control in Information Systems*, 175-184, Virginia.

Peters, T.J. & Waterman, R.H. (1982). *In Search of Excellence: Lessons from America's Best-Run Companies.* New York: Harper & Row.

Pettigrew, A.M. (1990). Organizational Climate and Culture: Two Constructs in Search of a Role. In B. Schneider (Ed.). *Organizational Climate and Culture*. San Francisco: Jossey-Bass Publishers.

Reichers, A.E & Schneider, B. (1990). Climate and Culture: An Evolution of Constructs. In B. Schneider (Ed.). *Organizational Climate and Culture*. San Francisco: Jossey-Bass Publishers.

Richardson, R. (2007). 2007 CSI Computer Crime and Security Survey. Computer Security Institute.

Ritov, I. & Baron, J. (2002). Status-quo and omission biases, *Journal of Risk and Uncertainty, 5*, 49-61.

Ruighaver, A.B., Maynard, S.B. & Chang (2007). Organisational security culture: Extending the end-user perspective. *Computers and Security, 26,* 56-62.

Sasse, M.A., Brostoff, S. & Weirich, D. (2001). Transforming the 'weakest link' – a human/computer interaction approach to useable and effective security. *BT Technology Journal, 19(3)*, 122-131.

Schein, E.H. (1985). *Organizational Culture and Leadership.* San Francisco: Jossey-Bass.

Schneier, B. (2003). *Beyond Fear: Thinking Sensibly About Security in an Uncertain World*, New York: Springer-Verlag.

Schneier, B. (2000). *Secrets and Lies: Digital Security in a Networked World*, Indianapolis, IN: Wiley Publishing, Inc.

Schultz, E (2005). The human factor in security. *Computers and Security, 24*, 425-426.

Shinn, M.T. (2000). Security for your e-business. *Enterprise Systems Journal, 15(8),* 615-620.

Shneiderman, B. (1998). *Designing the User Interface: Strategies for Effective Human-Computer Interaction*. 3rd ed. Reading, MA: Addison-Wesley.

Sjoberg, L. (2000). Factors in risk perception. *Risk Analysis*, *20,* 1-11.

Skinner, B. (1953). Science and human behavior. New York: MacMillan.

Slovic, P. (2000). What does it mean to know a cumulative risk? Adolescents' perceptions of short-term and long-term consequences of smoking. *Journal of Behavioral Decision-making, 13*, 259-266.

Slovic, P. (1986). Information and educating the public about risk. Risk *Analysis, 6(4)*, 403-415.

Slovic, P., Fischhoff, B., & Lichtenstein, S. (1979). Rating the risks. *Environment*, *21,* 14-20, 36-39.

Slovic, P., Fischhoff, B., & Lichtenstein, S. (1978). Accident probabilities and seat belt usage: A psychological perspective. *Accident Analysis and Prevention, 10*, 281-285.

Slovic, P., Fischhoff, B., & Lichtenstein, S. (1976). Cognitive processes and social risk taking. In J. S. Carroll & J. W. Payne (Eds.). *Cognitive and Social Behavior (pp. 165-184)*. Potomac, MD: Lawrence Erlbaum Associates, Inc.

Smircich, L. (1983). Concepts of culture and organizational analysis. *Administrative Science Quarterly, 28*, 339-358.

Stanton, J.M., Stam, K.R., Mastrangelo, P. & Jolton, J. (2005). Analysis of end user security behaviours. *Computers and Security, 24*, 124-133.

Stewart, A. (2004). On risk: perception and direction. *Computers and Security, 23*, 362-270.

Steyn, T., Kruger, H.A. & Drevin, L. (2007). Identify theft: Empirical evidence from a phishing exercise. In H. Venter, M. Eloff, L. Labuschagne, J. Eloff & R. von Solms (Eds.) *IFIP International Federation for Informaiton Processing, Volume 232, New Approaches for Security, Privacy and Trust in Complex Environments*. (pp. 193-203). Boston: Springer.

Swain, A. D., & Guttman, H. E. (1983). *Handbook of human reliability analysis with emphasis on nuclear power plant applications*. NUREG/CR-1278, U.S. Nuclear Regulatory Commission, (Washington D.C.).

Thompson, K.R. & Luthans, F. (1990). Organizational Culture: A Behavioral Perspective. In B. Schneider (Eds.). *Organizational Climate and Culture.* San Francisco: Jossey-Bass Publishers.

Thompson, P. & McHugh, D. (1995). *Work Organization: A Critical Introduction* (2nd ed.). London: McMillan.

Tversky, A., & Kahneman, D. (1973). Availability: A heuristic for judging frequency and probability. *Cognitive Psychology, 5,* 207-232.

Van der Pligt, J. (1996). Risk perception and self-protective behaviour. *European Psychologist, 1,* 34-43.

Van Maanen, J. & Schein, E.H. (1979). Towards a theory of organizational socialization. *Research in Organizational Behavior Vol. 1*, JAI Press, Greenwich, CT.p.209-264.

Weinstein, N.D. (1987). Unrealistic optimism about susceptibility to health problems: Conclusions from a community-wide sample. *Journal of Behavioral Medicine, 10*, 481-500.

Whitten., A & Tygar., J. (1998). *Usability of Security: A Case Study*, Carnegie Mellon University Computer Science Technical Report CMU-CS-98-155.

Wilde, G.J.S. (2001). *Target Risk 2: A New Psychology of Safety and Health*. Toronto: PDE Publications.

Wilson, M. & Hash, J. (2003). *Computer Security: Building an Information Technology Security Awareness and Training Program*. Information Technology Laboratory National Institute of Standards and Technology, Gaithersburg, MD 20899-8933.

Workman, M. (2007). Gaining access with social engineering: An empirical study of the threat. *Information Systems Security Journal, 16*, 315-331.

Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technolgoy, 59(4)*, 662-674.

Wu, M., Miller, R.C., & Garfinkel, S.L. (2006). Do security toolbars actually prevent phishing attacks? *Proceedings of the ACM CHI 2006 Conference on Human Factors in Computing Systems.* April 22-27, 601 – 610.

Zohar, D. (1980). Safety Climate in Industrial Organizations: Theoretical and Applied Implications. *Journal of Applied Psychology, 65(1)*, 96-102.

DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION
DOCUMENT CONTROL DATA

1. PRIVACY MARKING/CAVEAT (OF DOCUMENT)

2. TITLE

Human Factors and Information Security: Individual, Culture and Security Environment

3. SECURITY CLASSIFICATION (FOR UNCLASSIFIED REPORTS THAT ARE LIMITED RELEASE USE (L) NEXT TO DOCUMENT CLASSIFICATION)

Document	(U)
Title	(U)
Abstract	(U)

4. AUTHOR(S)

Kathryn Parsons, Agata McCormac, Marcus Butavicius and Lael Ferguson

5. CORPORATE AUTHOR

DSTO Defence Science and Technology Organisation
PO Box 1500
Edinburgh South Australia 5111 Australia

6a. DSTO NUMBER	6b. AR NUMBER	6c. TYPE OF REPORT	7. DOCUMENT DATE
DSTO-TR-2484	AR-014-705	Technical Report	October 2010

8. FILE NUMBER	9. TASK NUMBER	10. TASK SPONSOR	11. NO. OF PAGES	12. NO. OF REFERENCES
2008/1101574/1	INT 07/012	Brian Palm	45	107

13. URL on the World Wide Web

http://www.dsto.defence.gov.au/corporate/reports/DSTO-TR-2484.pdf

14. RELEASE AUTHORITY

Chief, Command, Control, Communications and Intelligence Division

15. SECONDARY RELEASE STATEMENT OF THIS DOCUMENT

Approved for public release

OVERSEAS ENQUIRIES OUTSIDE STATED LIMITATIONS SHOULD BE REFERRED THROUGH DOCUMENT EXCHANGE, PO BOX 1500, EDINBURGH, SA 5111

16. DELIBERATE ANNOUNCEMENT

No Limitations

17. CITATION IN OTHER DOCUMENTS Yes

18. DSTO RESEARCH LIBRARY THESAURUS http://web-vic.dsto.defence.gov.au/workareas/library/resources/dsto_thesaurus.htm

Information security, Human factors, Human behaviour

19. ABSTRACT

There have been many technological advances in information security that should, theoretically, result in more secure environments. However, in contrast to these expectations this is not always the case. Human factors play a significant role in computer security; factors such as individual differences, cognitive abilities and personality traits can impact on behaviour. Information security behaviours are also greatly influenced by an individual's perception of risk. All of these factors are also affected by the organisational culture and security environment in which they occur. These factors interact with one another and can result in behaviours that are often detrimental to information security. This report provides recommendations as to how these human and cultural factors can be influenced to result in more positive behaviours and lead to more secure information environments.