Al-Awadi, Maryam (2009) *A study of employees' attitudes towards organisational information security policies in the UK and Oman.* PhD thesis.

http://theses.gla.ac.uk/860/

Copyright and moral rights for this thesis are retained by the author

A copy can be downloaded for personal non-commercial research or study, without prior permission or charge

This thesis cannot be reproduced or quoted extensively from without first obtaining permission in writing from the Author

The content must not be changed in any way or sold commercially in any format or medium without the formal permission of the Author

When referring to this work, full bibliographic details including the author, title, awarding institution and date of the thesis must be given

Glasgow Theses Service
http://theses.gla.ac.uk/
theses@gla.ac.uk

A study of Employees' Attitudes Towards Organisational Information Security Policies in the UK and Oman

Maryam Abdullah Al-Awadi

PhD

2009

Department of Computing Science

Faculty of Information and Mathematical Sciences

Contents List

List of Figures

List of Table

Abstract

There is a need to understand what makes information security successful in an organization. What are the threats that the organization must deal with and what are the criteria of a beneficial information security policy? Policies are in place, but why employees are not complying?

This study is the first step in trying to highlight effective approaches and strategies that might help organizations to achieve good information security through looking at success factors for the implementation. This dissertation will focus on human factors by looking at what concerns employees about information security. It will explore the importance of information security policy in organizations, and employee’s attitudes to compliance with organizations' policies.

This research has been divided into four stages. Each stage was developed in light of the results from the previous stage. The first two stages were conducted in the Sultanate of Oman in order to use a population just starting out in the information security area. Stage one started with a qualitative semi-structured interview to explore and identify factors contributing towards successful implementation of information security in an organization. The results suggested a number of factors organizations needed to consider to implement information security successfully. The second stage of the research was based on the first stage’s results. After analysing the outcomes from the semi-structured interviews a quantitative questionnaire was developed to explore for information security policy. The findings did suggest that the more issues the organization covers in their security policy the more effective their policy is likely to be. The more an organization reports adoption of such criteria in their security policy, the more they report a highly effective security policy. The more the organization implements the ‘success factors’ the more effective they feel their security policy will be.

The third stage was conducted in the UK at Glasgow University because employees are somewhat familiar with the idea of information security. It was based on the findings derived from the analysis of the quantitative questionnaire at stage two. The findings revealed different reasons for employee’s non-compliance to organization security policy as well as the impact of non-compliance.

The fourth stage consolidates the findings of the three studies and brings them together to give recommendations about how to formulate a security policy to encourage compliance and therefore reduce security threats.

Acknowledgments

Many people have contributed to the completion of this thesis and I wish to express my heartfelt appreciation to all of them. Space does not allow me to mention everyone by name but there are a number of individuals and bodies that deserve recognition.

This study would have never been completed without the painstaking, humble and companionate guidance of Dr. Karen Renaud and Professor. Chris Johnson, who introduced me to the beauty of doing research, guided me through all the various stages of my research and provided a steady and supportive hand over the four fruitful years.

I also wish to thank Professor. Norman Reid and Professor. Rex Whitehead, who were always willing to share their expertise and knowledge. I am also grateful to my friends for their continuous support.

Finally, this thesis would not have been possible without participants' willingness to respond to the questionnaire and interviews. Last, but not the least, my big thanks to family who helped me and encouraged me throughout the process.

Chapter One

Thesis Statement

This chapter presents the thesis statement and outlines the thesis.

1.1 Introduction

Investigating literature on information security brings to the fore many questions regarding what is needed to have good implementation of information security, including: why are organizations, after working with security for such a period of time, continuing to struggle to achieve good information security?; why is organization security policy not working properly?; what does a security policy need to cover in order to have good information security?; and why are policies in place but employees are not complying with these? Such problems show the need for more research to be done in information security to help organizations achieve better information security.

This research was conducted to identify important aspects in the implementation of information security through reviewing organizations' different information security practices and to find out the success factors for implementing information security. It also investigates what makes an effective security policy that can help to reduce security threats. Moreover, it explores the reasons behind employees' non-compliance with organization security policy and investigates the impact of non-compliance of employees with organization security policy. Some recommendations about how to formulate a security policy to help to encourage employees' compliance are also presented.

My thesis statement is: it is possible to formulate an organization information security policy, based on:

- Best practice identified from the literature;
- An investigation of the success factors from implementing information security;
- An investigation into the effectiveness of information security policy; and
- An investigation into employee compliance with information security policy.

Such a policy will accommodate an organization's need to protect its assets thereby allowing employees to appreciate the security policy and practice security comfortably, and thus can be used to encourage employee compliance to therefore reduce security incidents.

To support my thesis statement I have had to carry out the following studies:

T1: Semi-structured interview to find what factors help organizations to implement successful information security procedures. There are factors that influence an organization’s implementation of information security. However, to the best of researcher’s knowledge, after surveying the literature, there has not been any study conducted to explore such factors.

T2: After analysing the outcomes of the existing techniques in T1, more investigation was required on trying to confirm the findings by using different techniques and exploring effectiveness of information security policies. Therefore, a quantitative technique was applied to confirm the results of the previous findings and to find out if information security policies could reduce organizational security breaches.

T3: After analysing the outcomes of the existing techniques, in T2, further investigation tried to understand the reasons for employees' non-compliance with the organization’s security policy. However, to the best of researcher’s knowledge, there has not been a study that has investigated the reasons for employees' non-compliance with organizational security policy. In an effort to fill this gap, this research investigates this matter a semi-structured interview was used to find the reasons for such non-compliance with security policies.

T4: Findings from the literature was combined with the findings from T1, T2, and T3 to determine what makes an effective information security policy in an organization. All the findings were investigated on real-life examples of existing security policies from different organizations to give recommendations about how to formulate a security policy to encourage employee compliance and therefore reduce security threats.

1.2 Outline of the Thesis

The rest of this thesis is organised as follows:

Chapter Two reviews the literature on information security. This chapter describes the field of information security and highlights the gap in the field for our research.

Chapter Three explains the methodology used to justifies the choice of the research method. It also list research questions used in this research.

Chapter Four identifies important aspects of the implementation of information security in Oman and to suggest some ‘success factors’ for implementing information security in government organizations. Qualitative analysis of the organizations’ experience formed the basis of the study.

Chapter Five covers the analysis of the results from the previous chapters using different research methods and focuses in more detail on information security policy.

Chapter Six describes an investigation of the findings from previous studies. It suggests investigating employees' compliance with their organization information security policy. This investigation uses a qualitative method.

Chapter Seven gives recommendations on how to formulate a security policy to encourage employees' compliance in order to reduce security incidents.

Finally, Chapter Eight summarises the main results of this research and suggests future research.

Chapter Two

Introduction

This chapter reviews the literature of information security in organizations. It explores in detail some elements to information security such as threats and vulnerabilities, organization security policy, related organization security culture and employees compliance.

This chapter is organized as follows. The first section outlines the background of information security. Section 2.2 explains what information security is. Section 2.3 covers elements related to information security such as threats, vulnerabilities and countermeasures. Section 2.4 reviews the use of information security in organizations. Section 2.5 explains international laws and standards relating to information security. Section 2.6 discusses information security policy. Section 2.7 describes organization information security culture. Section 2.8 discusses the human element in information security. Finally, section 2.9 presents the conclusion of this chapter.

2.1 Background to Information Security

The need for security in organizations is not a new problem (Greenwald, 1999); organizations have always been concerned with protecting their valued resources. Before the widespread use of computers, some staff would be assigned to safeguard paper records that were often kept in filing cabinets. Usually one person had a key for the cabinets, and maybe a secretary of the head of the organization would have a copy of those records in case of emergency. Recently, however, most organizations are adopting computer technology to organize and access information. There is no doubt that computers and networks are cost effective ways of getting work done and certainly they have made sharing information easier than before (Huff & Munro, 1985).

Von Solms (1996) suggests that information security has evolved through three stages. The first stage began in the 1960s when the main concern was to maintain physical security control over the hardware and to limit circulation of printed data. The second stage started in the mid-1970s, information security was handled in line with the restrictions of the organizations, despite the fact that the scope of information security extended radically. In the third stage, with more advanced technology, organizations are required to link their IT services together and move from a closed environment with a mainframe to complex environment working in distributed networks, including the Internet. The fourth stage will concentrate more on the human issues which include, according to Hitchings, “*the objectives of personnel, which may conflict with those of the organization; the culture of the people involved; and attitudes which can be influenced by low morale or good esprit de corps*” (1995, p. 377).

Blakley et al. (2002) argue that information security is needed because the technology applied to information brings risks. For example, Internet facilitates to put a value on information (Dourish et al., 2004) and present a threat to information. Whilst anyone can enjoy the benefits of access to the Internet as a source of information, the Internet will never guarantee safety of information security; in fact it guarantees the opposite. Therefore information security is equivalent to information protection (LeVeque, 2006).

One of the biggest scandals related to information security occurred when the whole UK was shocked by the news in November 2007 that a government official lost the personal data of 25 million people (BBC, November 2007). This data went missing from the civil service because of ignored security procedures and a breaking of the rules by downloading the data to disc and sending it through a courier that was neither recorded nor registered. The data was sent for auditing to the National Audit Office in London. The junior official downloaded the details of 25 million people in two discs with only password protection, these details included name, address, date of birth, national insurance number and bank details. Unfortunately the data could be compromised in the long term if it falls into the wrong hands. The banking account details could apparently not be at risk if they have been disclosed as the banking code in the UK allows banks to pay back their customers' money if any fraud has occurred. However, the other non-changeable data such as the person's name and date of birth could have the potential for making identity theft possible. There are three major failures in this case: the data was not encrypted; it was not transmitted via a secure mechanism and, most importantly, unnecessary personal information was not removed from the data before it was sent.

An organization is "*a series of information-handling activities*" (Dhillon, 2006, p. 2). When organizations grow in size and complexity, handling information becomes much less manageable and, at the same time, more and more important (Hoffer & Straub, 1994). The importance of information security in organizations also depends on the type of environment they work in. As explained, organizations depend increasingly on computers and control of information has been brought down to an individual level, on the desktop of the employee. More employees interact with technology to undertake their daily tasks than in the past. This could be compared with human interaction with their pets. The potential harm does exist because of the infections naturally transmitted between pets and people. According to Brodie et al. (2002) this risk potential can be minimized through simple measures and simple guidelines relating to health care for the animal and education on the risk of the animal, as well as careful hygiene practices. Information security in an organization requires the same approach of measures and guidelines to be considered and implemented in order to minimize any risks that come from their employees.

Given that the number of security breaches in organization is increasing (Workman et al., 2008) and the greater accessibility of the information, the greater the hazards, it is inevitable that security will need to be tightened (Brown & Duguid, 2002). Indeed with such high security breaches, organizations face difficulties in managing their information security effectively (Straub & Welke, 1998). When organizations fail to manage their information security, the organization's integrity will be compromised and loss of money could occur (Blakley et al., 2002). An example of such a case is what happened to the UK’s biggest building society, Nationwide, in 2007 when one of its employees took the company laptop home. This laptop held some private information about their customers. Unfortunately this laptop was stolen from the employee's home and Nationwide was given an almost one million pound fine after this incident (BBC, February 2007).

Also, with the increased number of violations, lack of confidence and trust will inevitably grow among people (Henry, 2007b). A recent incident happened to the NHS, UK in July 2008, when a laptop was stolen from an NHS manager whilst he was on holiday (Fernandez, 2008). The laptop contained encrypted records of over 20,000 patients with their details, including their names, postcodes and treatment plans. Such accidents put the well-being of patients at risk because if a patient’s health information becomes public knowledge it will affect their personal life. The personal details about the name and postcode could also result in an identity theft.

Information security has been regularly considered to be a technological problem with a technological solution (Ruighaver et al., 2007). That is simply untrue because information security is about managing risk (Whitman et al., 2005) and managing risk is about discovering and measuring threats to information assets (Lampson, 2002; and Garbars, 2002) in the organization and taking actions to respond to those threats. Understanding that organization information stored on and spread over networks is subject to threats from various sources. With the availability of technologies it is possible for information to be collected, shared, sold, exchanged and distributed without permission or knowledge of the holder (Varney, 1996). While not denying that technology can protect organization assets, the risk is still there because technology is easy to fool (Schneier, 2001).

Lampson (2002); Sasse & Flechais (2005); and Schneier (2003), highlight that security is a '*people*' problem, not just a technology problem because people are the ones who are going to implement information security. No matter how powerful the security system is or how hard regulations or policies are to break, there will be a continuous threat, disturbance to information security; because technology is a tool used or misused by people. As in the complex environment, sensitive material can be downloaded to a pen drive and disappear. With the press of a button, the information can be transferred in seconds.

Von Solms & von Solms (2004, p. 372) present some problems in organizational practices that lead to an organization lacking good information security. They explain that organizations have a problem in implementing a successful information security plans and can suffer from the 'ten’ deadly sins. These ten ‘sins’ are based on the many years of experience of authors in teaching information security and working on information security consultancy projects in various companies. A summary of these 'ten’ deadly sins of information security is illustrated in Table 2-1 below.

Table 2-1 Ten Deadly Sins of Information Security (von Solms & von Solms, 2004, p. 372).

Von Solms & von Solms (2004) go on to explain that from their experience if even one of these aspects is overlooked by the organization a serious problem will arise in introducing and maintaining information security in the organization.

Economics also plays a serious part in implementing information security in organizations (Cavusoglu, 2004). Many security holes are left undealt with because organizations cannot see the tangible benefits so that they pay more to maintain the desired level of security. Organizations are run by managers who spend money on to get a return from such good investment (Blake, 2000), and it is not easy for an IT department or the security specialists to provide statistics to demonstrate that information security is an investment. Anderson & Moore (2008) argue that there is a shortage of statistics about information security failures for the reason that the data is fragmentary or not available.

Lack of information on security policy and a lack of skills and experience in formulating security policy (Doherty & Fulford, 2005) prevent the good implementation of information security. Fung et al. (2003) explain that the information security policy is the keystone of good information security management. In addition, an adequate information security policy will facilitate protecting an organization's information resources (LeVeque, 2006).

Strong technology to secure an information system will not reduce the vulnerabilities of information. A combination of people, processes and technology is required to achieve a successful information security (Nicastro, 2007). Therefore, when organizations are equipped with the proper security technology, people are armed with knowledge and documented processes are available, then organizations can defend against most threats.

Figure 2-1 below summarizes this concept.

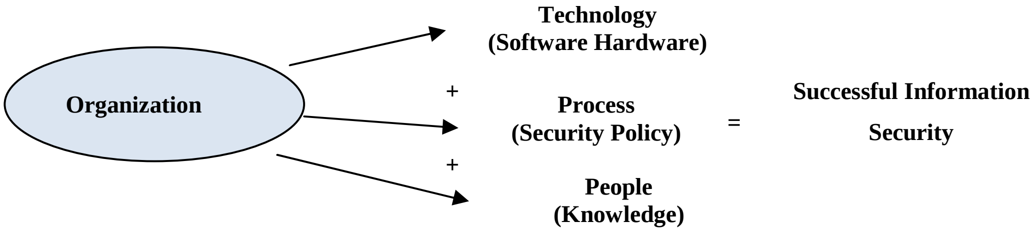


Figure 2-1 People, Process and Technology are Key to Achieve Successful Information Security.

At the same time organizations should be aware that information security covers not only information but also the entire infrastructure that facilitates its use. It covers hardware, software, knowledge of threats, physical security and the human element. Accordingly, information security is a combination of these elements, where each of these components has their own characteristics. None of the mentioned components can be ignored by any organizations if they are serious about information security.

The mentioned incidents earlier suggest that organizations are struggling to manage their information security. Therefore, what is required is to understand where the problem originates from. For the purpose of this study and to cover the objectives of the study (more information in Chapter Three) the following Figure 2-2 gives a brief detail of this chapter.

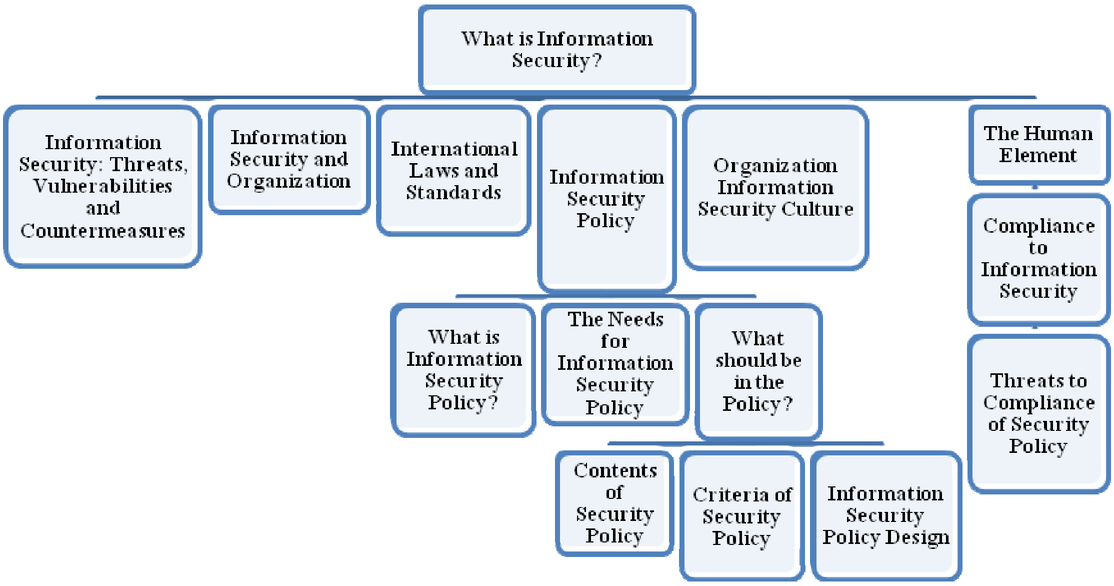

What is Information Security?
Information Security: Threats, Vulnerabilities and Countermeasures
Information Security and Organization
International Laws and Standards
Information Security Policy
Organization Information Security Culture
The Human Element
Compliance to Information Security
Threats to Compliance of Security Policy
What is Information Security Policy?
The Needs for Information Security Policy
What should be in the Policy?
Contents of Security Policy
Criteria of Security Policy
Information Security Policy Design

Figure 2-2 An Overview of this Chapter.

2.2 What is Information Security?

Wood (1982, p. 9) states that security is a huge subject, "*it ranges over physical security of buildings, fire protection, software and hardware, personnel policies and financial audit and control*". Von Solms (1999) explain that information security is a multi-dimensional area and, in order for an organization to ensure a secure environment for their information assets, they have to take into account all aspects. He further identifies these dimensions as being: the corporate governance; the organizational; the policy; the best practice; the ethical; the certification; the legal; the insurance; the personal/ human; the awareness; the technical; the measurement/metrics; and the audit dimension.

Information security is more than preventing intruders from accessing of confidential data. Organizations must be aware that any type of attack could damage their assets. Organizations are not all the same in the level of security they have and they vary in terms of security needs (Garbars, 2002). Each organization will protect its assets, comparing its security need against the associated threats through appropriate controls while maintaining cost effectiveness. Therefore, a definition of information security is important to help the organization to properly address all that has been discussed (Anderson, 2003).

The international standard for information security management, ISO I7799/ISO 27002 states that "*information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities*".

Therefore the organization’s information should not be disclosed to unauthorized individuals, should be protected from unauthorized modification and needs to be available to users when requested.

2.2.1 Information Security Principles

The protection of information is concerned with three aspects, which are confidentiality, integrity and availability (CIA), (Gollmann, 1999; Pfleeger & Pfleeger, 2003; and Denning, 1999). The terms are defined below.

Confidentiality: to ensure that information is accessible only to those authorized to have access. Not all of the information is equal in sensitivity and confidentiality, some information is more sensitive and needs a high level of confidentiality. Such information as health records, financial information or criminal records would be considered confidential. Security mechanisms, such as encryption and logical and physical access controls could be used to provide confidentiality.

Integrity: to identify unauthorized changes to information and processing methods. Information should be accurate, complete and protected from unauthorized changes. Integrity of information is very important. For instance, accountants need to have information that is accurate to make the budget plan for the organization.

Availability: to ensure that the information, system and other resources are available to users when required, so productivity will not be affected. Users need access to information when it is requested so that they can carry out their daily tasks. For example, when there is a problem with a highly used database the productivity of the organization can be affected due to the unavailability of specific information. A backup mechanism should be used to ensure continuity of the available resources.

Dhillon & Backhouse, (2000, p. 127-128) argue that CIA principles are not enough to address information security because they apply to information that is seen as data held on a computer system. They suggest extra principles such as responsibility, integrity, trust and ethicality (RITE). These additional principles are related to employees in an organization and are the initial steps in securing organization assets. These are described as:

Responsibility (and knowledge of roles): members are expected to develop their own work practices on the basis of a clear understanding of their responsibilities.

Integrity (as requirement of membership): information has great value; therefore organizations need to consider how to uphold and support integrity since the integrity of people may change over time.

Trust (as distinct from control): the organization depending more on self control and responsibility, there have to be common systems of trust.

Ethicality (as opposed to rules): ethical content of informal norms and behaviour.

The securing of an organization's information could be defined as protection against attack or failure. The breach of information security is related to three possible things: loss of confidentiality, breach of integrity and breach of availability (Workman et al. 2008). These breaches result from threats, and are likely to disturb the organization's daily functioning. This implies that the organization's information system is surrounded by different kinds of security threats. These threats might be caused by blameless users or by hackers challenged to find out, break-in and control system resources. Anderson & Moore (2008) state that the traditional assumption with information security specialists is that there are two types of user. The first one is the honest user who demonstrates straightforward, direct behaviour. The second one is the malicious user who would try to cause havoc at any cost. When defenses fail and a breach occurs in an organization's system it will affect the confidentiality, integrity and availability of the organizations systems. For example, a breach of confidentiality is when information is revealed to unauthorized people; a breach of integrity is when the system is not processing correctly; and a loss of availability is when the system does not provide the services that it is required to at the expected time.

What follows are the different types of security threats and vulnerabilities that organizations are experiencing.

2.3 Information Security: Threats, Vulnerabilities and Countermeasures

Security threats are "*circumstances that have the potential to cause loss or harm*" (Pfleeger, 1997, p. 3) to information security**.** So, what could cause a threat to information security? According to Cooper (1984) and Payne (2003) there are two types: accidental and deliberate. Threats can also be classified as external and internal. The list of threats and vulnerabilities could be endless but many publications and surveys such as Hinde (2002); Whitman (2003); Ernst & Young (2004); Doherty & Fulford (2005); and DTI (2006) enumerate the variety and consequence of threats that face organization information security. The following threats have been identified by these surveys:

External threats:

- **Computer viruses, Worms and Trojan horses**: Computer programs that have the capability to automatically replicate themselves across systems and networks.
- **Natural disaster**: Damage to computing facilitates or data resources caused by phenomena such as earthquakes, floods, or fires.
- **Spam e-mails (opening)**: Unsolicited e-mail.
- **Hacking incident**: The penetration of organizational computer systems by unauthorized outsiders, who are then free to access and manipulate data.

Internal threats:

- **Installation /use of unauthorized hardware, peripherals or software**: Information systems, especially financial systems, are vulnerable to individuals who seek to defraud an organization.
- **Abuse of computer access controls**: The deliberate abuse of systems and the data contained therein by users of those systems.
- **Physical theft of hardware /software**: Theft of valuable hardware, software and information assets.
- **Human error (violation)**: The accidental destruction or incorrect entry of data by computer users.
- **Deliberate damage by displeased employees**: Disgruntled employees may seek revenge by damaging their employees' computer systems.
- **Use of organization resources for illegal communications or activities (porn surfing, email harassment)**.

Organizations often experience some form of security breach, either external or internal (Whitman, 2003). The DTI (2006) survey found that every company in the UK currently experiences several security incidents a day, increased from approximately one a month in 2004. Madigan et al. (2004) explain that internal abuse is more costly for the organization compared to external abuse. An external attack relies a lot on employee errors which allow access to the information system of the organization. Doherty & Fulford (2005) state that computer viruses and human errors are very frequent types of breaches. According to Brostoff & Sasse (2001, p. 43) "*security breaches are often deliberate (and so are likely to happen again and again)*". Actions related to these threats make them security breaches. For example, spam email is a threat but when any employee opens this spam email the result is a security breach.

Vulnerabilities in organizations are related to any weaknesses in computer or network software or hardware that open them to an attack or damage. For example, organizations are good at creating user accounts but there is often a lack of follow-up to deactivate or remove user accounts when employees leave the organization. This could expose the organization's information system to risk and constitute a threat.

A countermeasure is a procedure or mechanism that reduces the probability that a specific vulnerability will be exploited, or reduces the damage that can result from a specific exploitation of vulnerability. Examples of countermeasures include security policy, access control mechanisms, a security guard and security awareness training.

After organizations have defined their threats and vulnerabilities, they need to define their assets according to their need for confidentiality, integrity and availability (Garbars, 2002; LeVeque 2006; and Anderson 2003) under a proper balance of expense (Kaplan, 2007). Different environments have different priorities. For instance, in a university environment integrity and availability comes first and for a banking environment integrity takes preference. Even within an organization different departments have different priorities. For example, an organization's website needs more availability than confidentiality, whereas a financial process may need a high level of integrity and confidentiality and have less need for availability.

Knowing what the organization wants to protect, what to protect it from and not waiting for several bad incidents, will help organizations to decide how to invest in securing information. This can be done by determining an organization's assets, threats and vulnerabilities in order to take appropriate actions according to the organization's resources; in other words this is risk management (Siegel et al., 2002). Risk management is a "*keystone to effective performance and for targeted, proactive solutions to potential incidents"* (Henry, 2007b, p. 321). In information security a risk is any hazard or danger to which an organization's information and assets is subject. Risk assessment will help organizations to know their presence and gives an approach to managing the dilemma of how to deal with such threats (Swanson & Guttman, 1996). Risk assessment is an organization's responsibility: “*While there is no universal 'recipe' for minimizing risks, IT professionals will have to evaluate the nature of the organizational environment before considering whether and how to implement any IT based solutions*” (Dhillon & Backhouse, 1996, p. 73-74).

Wood (1982, p. 84) explains that organizations can perform risk assessment through the following steps:

- “Gathering information about the organization: what it does, how it operates, its assets and resources;
- Identifying the risks to these assets and resources and assessing them, their impact and likely frequency;
- Identifying countermeasures to these risks, their costs, and likely effectiveness;

- Preparing security programmes and submitting them to management;
- Preparing plans for implementing authorized security programmes; and
- Monitoring and reviewing the effectiveness of these programmes”.

2.4 Information Security and Organization

Loch et al. (1992, p. 173) state that concern regarding information security in organizations has been shifted from "*forced entry into computer and storage rooms to destruction by fire, earthquake, flood, and hurricane*" to "*protecting information systems and data from accidental or intentional unauthorized access, disclosure, modification, or destruction*".

It is impossible to achieve perfect security (Schneier, 2001), regardless of organization resources. Organizations nowadays are depending more and more on information technology to share information and other resources, in order to get work done (Dhillon & Backhouse, 1996). Once organizations place their vital information on databases and make these databases accessible through the Internet, they are consequently increasing existing risk (Dourish et al., 2004) as anyone can gain access to them. Employees' behaviour towards an organization’s assets has the potential to harm the organization.

Siegel et al. (2002) state that there is no ‘*magic bullet*’ for security; neither money nor time will deliver a completely impenetrable system. Money does play an important role in selecting security measures and many organizations are turning to technology to help shore up their defenses, but information security problems cannot be dealt with only from a technical perspective (Posthumus & von Solms, 2004). No one denies how important technology is but perfection in information security is not attainable and no security technology produces absolute security (Wood, 1982).

There is much discussion in the literature related to what hinders the implementation of information security in an organization. A summary of these problems is going to be discussed in the following Figure 2-3.

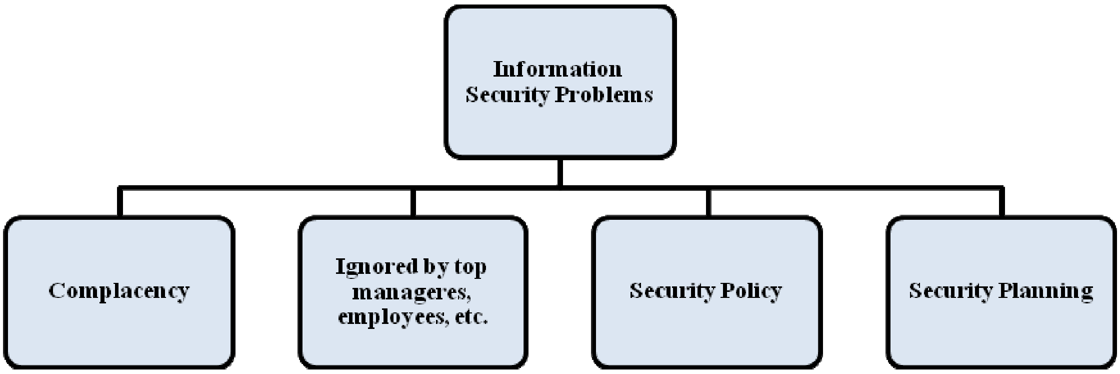

Information Security Problems
Complacency
Ignored by top manageres, employees, etc.
Security Policy
Security Planning

Figure 2-3 Some Problems with Information Security.

Organizations are not looking for perfect security but they are looking for reasonable security where no serious breaches can lead the organization to "*litigation, financial losses, damage to brands, loss of customer confidence, loss of business partner confidence, [or] even cause the organization to go out of business*" Rainer et al. (2007, p. 100). According to Workman et al. (2008) security breaches continue to grow as managers and organizational developers are not sure how and when to intervene when a breach occurs. Kessler (2001) states that the problem in organizational security is not the lack of technology, tools and products, but the lack of consideration of security risks and recognizing the importance of a secure system. Information security aims to ensure business continuity (von Solms, 1999) and decrease the likelihood of security breaches (LeVeque, 2006; and Kudo et al., 2007). No matter how big or small the organization is, security planning is vital to enhance the security of the organization (Fitzgerald, 2007).

Planning in security is a vital issue. Fitzgerald (2007, p. 21) states that "*planning reduces the likelihood that the organization will be reactionary concerning security needs. With appropriate planning, decisions on projects can be made taking into consideration whether they are supporting long-term or short-term goals and have the priority that warrants the allocation for more security resources*".

In security planning there are three interrelated components: strategic, tactical and operational plans (McLean & Soden, 1977).

O'Connor (1993, p. 72-73) defines these three components:

Strategic planning: the process of recognizing information systems which will provide the organization with a competitive edge. This involves both information security management and organization management.

Tactical planning: focuses on prioritizing and scheduling development efforts and starting action plans for development and performance measures to be used during operational planning. It is initiated from strategic planning efforts, employee requests, regular maintenance efforts or mandates from external organization resources.

Operational planning: involves the development of specific detailed plans for each project. This involves management and employee representatives who they are required to participate in system development, review deliverables, prototype, etc.

According to Tryfonas et al. (2001) strategic planning is what the organization would like to utilize. The tactical planning is the methods and techniques to be used during the operational planning and the operational planning describe tools and products adopted to realize a development practice.

All that has been described about security planning is summarized in the following Figure 2-4. Each of the planning stages in Figure 2-4 describes different actions. For example, if the organization wants to have an information security policy then the organization needs to implement the three stages. For the strategic planning stage the organization needs to establish security risk analysis to gather the required information to utilize an information security policy.

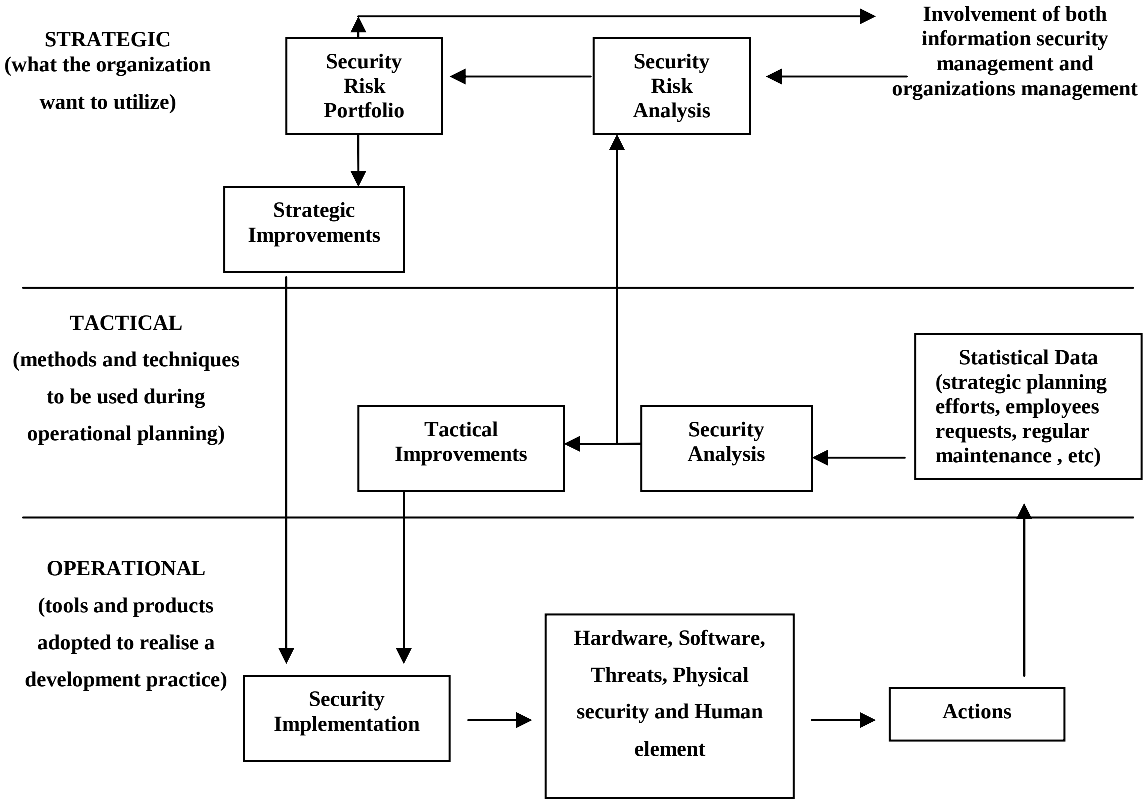


Figure 2-4 Security Planning in Organizations.

A problem occurs when organizations underestimate or overlook potential threats until they happen (Wright & Kakalik, 2007). Dhillon (2001) states many disasters happen because of such complacency of employees in an organization. Employees can be overconfident in the security of the organization and complacency appears (Gritzalis, 1997). Therefore, when the organization security system is running smoothly with no disturbance then complacency occurs. Employees know that there are specialists in security in their organization therefore they rely on them and believe that they themselves do not need to take due care. Workman (2007, p. 317) argues that, “*when people perceive that a risk has diminished, they will behave in a less cautious manner*”. Hentea et al. (2006) stress that awareness and education is crucial to avoid employee complacency.

Another problem is that, as Straub & Welke (1998, p. 441) explain, "*Information security continues to be ignored by top managers, middle managers, and employees alike. The result of this neglect is that organizational security systems are far less secure than they might otherwise be and that security breaches are far more frequent and damaging than* *is necessary*". Loch et al.’s (1992, p. 185) study reveals that management in organizations need to:

- “Become more informed on the potential for security breaches in the mainframe environment and via employees' and competitors actions;
- Increase their awareness in key areas such as penalties and laws; and
- Recognize that their overall level of concern for security may underestimate the potential risk inherent in the highly connected environment in which they operate”.

All this will help management in organizations to recognize the need for information security.

The absence of an information security policy in an organization is one reason why various security problems have occurred (Dhillon, 2006). It is crucial to ensure that an appropriate and effective security policy is developed and put into practice all through the organization (von Solms & von Solms, 2004). Verdon (2006, p. 49) presents a list of considerations for working with security policies:

- “Know all of the organization security policies.
- Involve organization security team and legal counsel early, keep them involved, work as a team to assess real compliance with policies.
- Identify organization protection needs. A risk assessment conducted with organization security group will help.
- Know the requirements of organization classification policy and ensure that organization application meets them, especially regarding destruction or retention of data.
- Keep informed on best practices in application security”.

Information security policy will be discussed in more detail later. Next is a brief description of laws and standards that deal with information security.

2.5 International Laws and Standards

In some countries there are laws governing the way that the organization operate their computer system. There are also standards or guidelines suitable to adapt for commercial reasons. The laws and standards that are available or implemented in two countries where the research was conducted, the Sultanate of Oman and the UK are discussed below.

Computer Misuse Act 1990 (Computer Misuse Act, 2008)

The Computer Misuse Act 1990 is a law in the UK that affects computer crime and makes certain activities illegal. The Computer Misuse Act falls into three sections and makes the following illegal:

- Unauthorized Access to Computer Material.
- Unauthorized Access to Computer systems with intent to commit another offense.
- Unauthorized Modification of Computer Material.

ISO 17799/ ISO 27002

This is a well know international standard; ISO I7799 updated as ISO 27002. This international standard is based on the British standard BS7799, now known as ISO 27001. Von Solms (1999); Canavan (2003); and Doherty & Fulford (2005) all agree that established standards, such as the international standard ISO I7799/ISO 27002, are a good starting point for shaping the information security policy to improve the information security in the organization. ISO I7799/ISO 27002 is organized into ten major sections:

1. Security policy
2. Organization of assets and resources
3. Assets classification and control
4. Personal security
5. Physical and environmental security
6. Communications and operations management
7. Access control
8. Systems development and maintenance
9. Business continuity management
10. Compliance.

ISO I7799/ISO 27002 placed some successful implementation of the information security policy aimed at senior management to take decisions and then pass on the essential action to those in charged. ISO I7799/ISO 27002 (p. xi) deals with:

- “security policy, objectives and activities that properly reflect business objectives;
- an approach to implementing security that is consistent with the organizational culture;
- visible support and commitment from management;
- a good understanding of the security requirements, risk assessment and risk management;
- effective marketing of security to all managers and employees;
- distribution of guidance on information security policy and standards to all employees and contractors;
- providing appropriate training and education;
- a comprehensive and balanced system of measurement which is used to evaluate performance in information security management and feedback suggestions for improvement”.

However, Siponen (2001) disapproves of ISO I7799/ISO 27002 from a philosophically scientific perspective and disagrees that these standards are scientifically justified, since they are based on personal observation and not universally valid. On the other hand von Solms (1999, p. 57) concludes that ISO I7799/ISO 27002 "*can certainly provide the basis to ensure safe driving on the information super highway.”* Moreover, Fitzgerald (2007) believes that the standard can be used as a basis for developing security procedures and good practices within an organization. Indeed the organization does not need to start from scratch to address information security in their organization; using ISO I7799/ISO 27002 will help them to have an overall picture of security and define the important points in order to ensure good implementation of information security. Von Solms (2000) states that following such a baseline code of practices will assure the organization that most of the security aspects needed in order to be tackled will be covered by a good code of practice. Also, standards will ensure the organization that they are going along with international best practices to implement appropriate information security. Of course, everything relating to these departments in charge of information security needs to ensure that standards are up to date, such as software, hardware, etc.

May (2003) argues that standards are one of the best methods for organizations to develop a practical strategy for information security. He further explains that the organization will benefit from standards in two ways. The first is in developing a strong, consistent and structured strategy for information security. The second is by showing the strength of an organization's security.

Data Protection Act 1998 (Data Protection Act, 1998)

This act relates to storing and processing information about people. Organizations in the UK ranging from those with a simple mailing list for names and addresses of customers to those with huge databases of employee information (i.e. salary, gender, etc.) need to register with the Information Commissioner. It is illegal in the UK to make use of information for purposes other than those which have been stated. People have the right to request a copy of the information that an organization holds about them, but for a fee.

Email Law

In the UK, organizations are legally responsible for the content of any email that has been sent from their system regardless of whether it is a personal or a work related email. The Data Protection Act 1998 in the UK states that all confidential information must be handled and transmitted securely. Therefore, sending such information via email without taking steps to encrypt it will result in committing a criminal offence.

E-Transactions Law (E-Transactions Law, 2008)

The Sultanate of Oman has issued the e-Transactions Law formalized by Royal Decree 69/2008. This law was issued recently on the 17th of May 2008 in a shift towards creating a suitable environment for secure electronic transactions. One of the main purposes of this law is to facilitate electronic transactions which are very important to e-government and e-commerce applications in Oman.

Next is a detailed discussion about organization information security policy.

2.6 Information Security Policy

As noted earlier, there is a growing recognition that organizations need to enforce some controls to ensure that the information retains its confidentiality, integrity and availability (CIA). One of the vital controls of CIA is the information security policy (Hone & Ellof, 2002). However, combining the elements of the CIA together is hard, especially when policy is interpreted from a written medium to a practical one (Hare, 2007). For example, when organizations ask their employees to use many passwords for different software they need to work with these and at the same time not write the passwords down.

Lindup (1995); Higgins (1999); and Cuppens & Saurel (1996) describe several types of information security policies that exist, such as:

- **System security policy**: this policy defines the basic security needs of the planned system.
- **Product security policy**: this policy describes the security policy leading to the proper functionality of the product.
- **Community security policy**: this policy has it is origin in the government networks.
- **Corporate information security policy**: this policy relates to the different levels in the organization.

According to Canavan (2003), at the organizational level there are three levels of policies which apply to the organization management, the IT department and the employees. Each of these levels tends to view security needs differently. For example, management is concerned about expenditure versus production, IT support is concerned with simplicity of managing the network and the systems and the employees are concerned about finishing work without various controls getting in the way.

The organizational information security policy for each of the three levels may vary from one organization to another depending on the organization's culture (Baskerville & Siponen, 2002; Luker & Petersen, 2003; and Hare, 2007). However, in general these are described as:

A- Organization Policy

This policy covers policies for the organization as a whole; the overall security policy aim. Its purpose as well as to state how that information security is important to the organization. Also, it needs to totally outline the responsibilities of everyone in the organization in addition to what is needed to be protected and the reasons for it being protected.

B- IT Department Policy

This policy covers the responsibilities of the IT department in keeping the organization network secure and stable. It should also define backup policy, threat incidents, client policy, hardware and software policy and other relevant policies.

C- Employees Policy

This policy defines the processes of an employee, in order to keep the organization’s asset and network resources secure. This policy includes guidelines regarding passwords, organization information use, internet usage and system use.

Ultimately, everyone in the organization has a different role in information security; for example, employees must know the difference between appropriate and inappropriate use of computing resources. To determine methods of hardware and software usage, as well as to enable all the employees of the organization to be on track, organizations apply information security policies. This research will focus on the employee-level policy called the acceptable use policy (AUP), hereafter referred to as information security policy.

2.6.1 What is an Information Security Policy?

An information security policy is a plan identifying the organizations vital assets with a detailed explanation of what is acceptable, unacceptable and reasonable behavior from the employee in order to effectively ensure information security (Hone & Eloff, 2002). For Nijhof et al. (2003, p. 67) policy is "*an instrument for responsibilisation within the organization*".

An information security policy is a combination of principals, regulations, methodologies, techniques and tools (Tryfonas et al., 2001) established to protect the organization from possible threats. These policies will help an organization to define their information assets and define its attitude to information (Canavan, 2003).

2.6.2 The Needs for Information Security Policy

David (2002, p. 506) states that "*Security is not what you do, it is not what you do not do, it is not what you allow, and it is not what you prevent. Security has nothing to do with how safe your data and system are. Security is how well you adhere to your formal security policies*”. Security in organization is related to having a formal security policy and how employees follow and practice organization policies. Hence, an efficient information security policy is a strategy in which the employees are able to recognize what is expected from them in terms of managing information resources. Therefore, the effective information security policy does not only depend on the correct details of the policy but also relatively in terms of how the employees understand these policies can achieve the information security objectives of the organization (Hone & Eloff, 2002).

The benefit of an information security policy in an organization does not merely involve all the employees in securing the organization's assets but also minimizes the human factor issues that can frustrate the implementation of a policy (Adams et al., 1997). Hare (2007) explains that organizations need a security policy because of the need for controls. With the changes in the organizational environment, where computing control has been brought down to the individual desktop of the employee, organizations need to protect their assets from unpleasant activities. The information security policy can determine the hardware and software usage as well as guide all the employees of the organization to be on right track. The assets of the organization that can be looked at in order to identify the vulnerabilities are hardware, software and individuals. The purpose of the security policy is "*to create a shared vision and an understanding of how various controls will be used such that the data and information is protected in an organization*" (Dhillon, 2006, p. 6). Zuccato (2004) states that security policies are used to obtain security requirements for organizations, in terms of what they want to protect and how to protect it.

An empirical study conducted in the United Kingdom by Doherty & Fulford (2005), based on a mailed questionnaire, targeted IT managers within big organizations and received a total of 219 valid responses from 2,838 questionnaires. It suggests that there is no statistically significant relationship between the adoption of information security policies and the incidents or severity of security breaches. These results contradict what has been discussed earlier about the benefits of security policies in organizations. The study's author's call for more studies to investigate the benefits of security policy and suggest some possible reasons for the results found (Doherty & Fulford, 2005, p. 34-35):

- **Difficulties of Raising Awareness**: if employees are not made aware of an organization's policy, then there will be a risk that it will become a dead document rather than a dynamic and effective security management device.
- **Difficulties of Enforcement**: if organizations cannot put their security policy into practice then employees will have difficulties reading and paying attention to policies.
- **Policy Standards are too Complex**: lack of skills and experience in formulating an information security policy can make employees confused in implementing good security.
- **Inadequate Resourcing**: lack of proper resources will hinder the monitoring and enforcement of organization security policy.

- **Failure to Tailor Policies**: organizations' security policy requirements depend on the types of information and the culture of the organization.

A DTI (2006) survey reports that the number of companies with a formal security policy in place has never been higher compared to some earlier studies, as shown in Figure 2-5. Three-fifths of UK businesses still do not have a formal security policy. The report also revealed that 55% of companies that give a high or very high priority to security have a security policy.

Figure 2-5 UK Businesses who have a Formally Documented and Defined Information Security Policy.

The above findings raise many questions to be investigated and explored regarding what makes an effective security policy in an organization. Figure 2-6 gives a summary of the dilemmas of implementing an information security policy in an organization. For example, if an organization adopts a security policy, is the organization secure? Or, will a documented security policy help an organization to reduce threats? Also, is the policy the right one or not? These dilemmas are examined in Chapter Five.

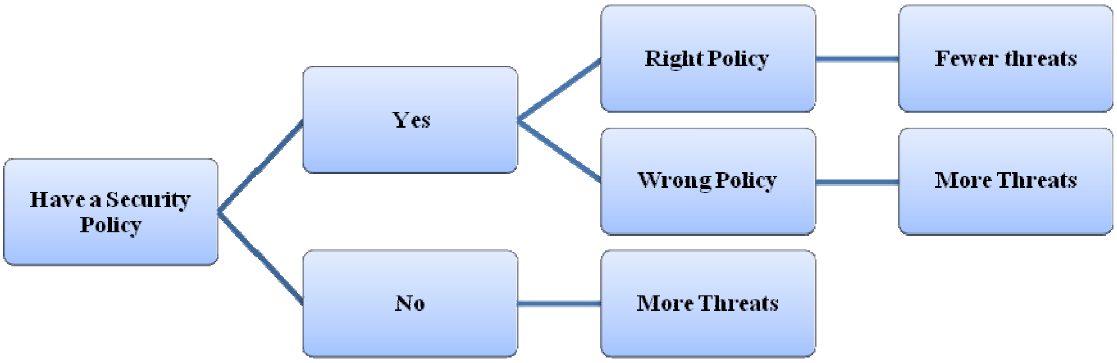


Figure 2-6 Some Questions about Security Policy.

2.6.3 What should be in the Policy?

The policy's content is what an organization needs to address in terms of protecting its assets (Zuccato, 2004). According to Verdon (2006, p. 48) a good policy "*must be reasonable, understandable to their audience, and practicable, with very few exceptions*". It should be reasonable in the sense that each organization needs to run security according to their requirements (Hone & Ellof, 2002). It should also be understandable by employees in terms of what they read, understand and acknowledge (McIlwraith, 2006) in the policy as well as the implementation of the policy in the organization. Its practicability can be determined in terms of balancing the nature of the information and related amount of threats (Wright & Kakalik, 2007).

Also, Whitman (2004, p. 52) states that "*A good security policy should outline individual responsibilities, define authorized and unauthorized uses of the systems, provide venues for employee reporting of identified or suspected threats to the system, define penalties for violations, and provide a mechanism for updating the policy… specific to an organization and its systems, but contain many commonalties*".

This leads to the question, what should be in the security policy document?

2.6.3.1 Contents of the Security Policy

Many authors have discussed what should be contained within a security policy document. Some advise that it needs to be short so that it will be read by employees (Shorten, 2007) and some say that it should be in bullet-point form because policy does not give details but states what should be done (Hare, 2007). Organizational security policy is divided into different sections. Each section covers what activities the organization needs from employees to perform for security controls to meet organizational objectives.

Below are common topics that have been discussed by many authors in this area, such as Barman (2001); Whiteman (2004); and Shorten (2007):

- **User Login Responsibilities**: this section explains employees responsibilities related to their login name and passwords. For example, they need to be aware to avoid any familiar names for their passwords, not to share their passwords with their colleagues or even write down their password.

- **Use of Organization System & Network**: this section illustrates how employees deal with organization resources such as computers, laptop, software, hardware and network.
- **Internet Access**: this section specifies if employees are allowed to use the internet or not and how they use it. For example, employees are not allowed to use any chat websites.
- **Viruses, Worms & Trojans**: employees may be required to use the anti-virus software before opening any internet files or report any virus incidents to the concerned person or department.
- **Disclosure of Information**: this section is related to what information assets must be protected, how sensitive information must be handled or if any encryption is needed.
- **Definition of Responsibilities**: this section tells employees to whom security breaches and violations should be reported.
- **Email Usage**: this section describes the usage of emails in the organization by each employee. For example, if they can use email for either organizational matters or also private matters, not to open or distribute spam emails.
- **Adoption of some Standards**: the policy needs to mention if the organization adopts any laws. For example: International standards (ISO 17799/ISO 27002).
- **Personal Usage of Organizational Resources**: this section deals with employee’s use of organization resources such as computers, laptop, software, hardware. For example, advice might include not to use your personal laptop in an organizational system without any authorization from the concerned department.
- **Explanation the Consequences of Violations and Breaches**: this section of the policy describes and explains to employees what the consequences are of failing to obey or comply with their organization's policy. At the same time it must give the management flexibility when deciding what sanction is applied (Hare, 2007). For example, an organization will not sack an employee for a minor breach.
- **Feedback System for Suggesting Policy Improvements**: this section addresses how employees could input to process and communicate the information security policy improvement.

Figure 2-7 summarizes the policy contents.

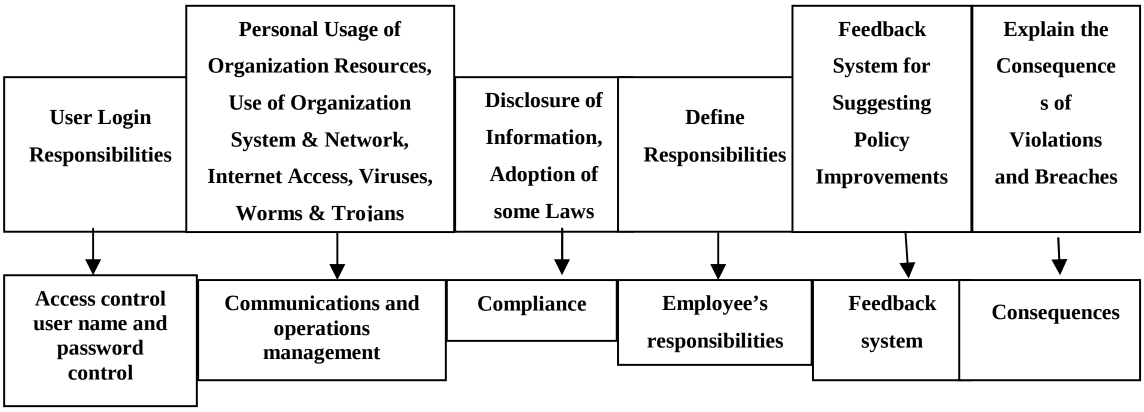

User Login Responsibilities
Personal Usage of Organization Resources, Use of Organization System & Network, Internet Access, Viruses, Worms & Trojans
Disclosure of Information, Adoption of some Laws
Define Responsibilities
Feedback System for Suggesting Policy Improvements
Explain the Consequence s of Violations and Breaches
Access control user name and password control
Communications and operations management
Compliance
Employee's responsibilities
Feedback system
Consequences

Figure 2-7 Policy Contents.

2.6.3.2 Criteria of an Effective Information Security Policy

Organizations develop a security policy to reduce threats from viruses and to prevent such incidents from happening again (Hinde, 2003). Also, they may wish to change the habits of their employees in the organization. There are some criteria that the information security policy needs to consider to give good results in securing organizational assets. These criteria have been summarized by different authors Baskerville & Siponen (2002); Salter et al. (1998); Madigan et al. (2004); and Luker & Petersen (2003). The policy must:

- **Fit the organizational culture**: the security policy of an organization mostly depends on the common organizational culture. Organizations differ in their security requirements. What is suitable to one organization may not be suitable to another.
- **Have a style which is consistent with the organization's general communication style**: a common format makes the policy easier for employees to understand the purpose of it;
- **Be effective and dynamic**: organizational policy should be revised and changed regularly, a minimum period of time could be six months or less to avoid any threats from happening and help to also define new threats;
- **Easy language**: Not described as a technical document, but uses simple language to ensure it is not difficult to understand. It should be free of jargon or technical terms, easy to understand and also be written in a solid language rather than an abstract language to stop any confusion for employees regarding policy.

- **Specify the job responsibilities**: allow employees to find out what their responsibilities are and what they are required to do to follow the policy;
- **State the purpose of the policy and the scope of the organization:** the policy has to state the reasons for the policy and what the organization's aim is, in order to let the employees understand the benefit of such policy; and
- **Explain what activity is acceptable and what is not**: this will make it clear to employees what is acceptable behaviour and what is not.

The next sections concerns how information security policy is designed.

2.6.3.3 Information Security Policy Design

The following Figure 2-8 describes the process of designing the information security policy.

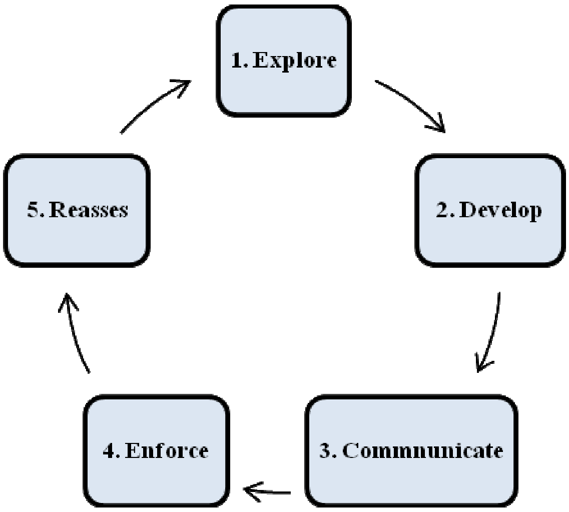


Figure 2-8 Information Security Policy Designing Process.

Barman (2001) describes that an organizational security policy plan process goes in a cycle of exploring, development, communication, enforcement and reassessment.

- **Exploring**: The first step required for structuring a security policy is a detailed exploration of the organization's network, any other vital asset this step, the organization's critical information resources, as well as identifying the possible threats. In order to identify the vital assets of the organization, their use and functionality, these questions should be considered: what is to protect, whom to protect from and how to protect?

- **Development**: After identifying the assets, the formation of a list outlining the possible threats should be included to be used in managing all of the threats that might be posed by each of the defined resources in the organization.
- **Communication**: Employees need to have notice in advance that a new policy is being developed and the reason for the new policy. Once the policy is in shape it needs to be reviewed and commented on before the organization approval step.
- **Enforcement**: Following the approval step is the enforcement step where the policy is to be put in place within the organization. The policy needs to be circulated to all the employees to ensure that they understand the policy and know their responsibilities.
- **Reassessing**: The organization should reassess and revise the policy regularly, once or twice a year to cover new technology or new threats to information.

Once the policy has been revised and updated it needs go back to follow the policy design method. Therefore, an information security policy is a vital consideration in an organization for any security program. Once the organization defines the value of its information it needs to develop a set of policies to help to protect it and prevent threats to it. Most organizations develop their own policies, which manage how staff should treat their organization's assets.

2.7 Organization Information Security Culture

A culture exists when members of an organization share identity and mission (Schein, 2004). Generally organizational culture is "*shaped by the basic beliefs, ethics, and ideologies that underlie the value judgements and value systems described above. Such beliefs, ethics, and ideologies might deal with the merits of competitive entrepreneurship and capitalism; the need for co-operation, partnership and communitarianism; or the need for service and social responsibility, (etc.)*" (Morden, 2004, p. 159). For Martins & Eloff (2002) employee’s behaviour towards information security shapes information security culture.

According to Westrum (1993, p. 401) culture determines:

- “What tasks organizations set themselves;

- How they address these tasks;
- How successful they are likely to be in coping with them; and
- How they react when things go wrong".

Two terms, organizational climate and organizational security are used in two different contexts. For example, organizational security climate refers to awareness of policies, procedures and practices (Neal & Griffin, 2002) relating to security in the organization. Organizational security culture deals more with attitudes, beliefs and perceptions shared by employees in defining norms and values that determine how they respond in relation to threats (Hale, 2000). Security climate is positively linked with security compliance since employees needs to comply with an organization's security policy and this mostly depends on the common organizational culture (Zuccato, 2004).

According to Thomson & von Solms (2004), there are three different types of environment that can be evidenced in organizations: coercive, utilitarian and goal consensus. Coercive is when employees perform tasks because they must, rather than because they agree with the actions and decisions of senior management. A utilitarian environment is when employees will do as senior management wishes because of an incentive system and not because they necessarily agree. Finally, the goal consensus environment is when employees identify with the organization and share the same beliefs and values of senior management. They willingly strive towards the vision of their senior management for information security in the organization.

Literature indicates that information security policy helps in the formation of organizational culture by identifying what is an accepted or unaccepted behaviour in terms of information security (Thomson & von Solms, 2004). Security policy progress is influenced by an organization's culture (Ruighaver et al., 2007). There is no doubt that standards and policies are important but monitoring is essential to ensure ongoing compliance (Fitzgerald, 2007). Consequently, policies are useless if not implemented and enforced (Whitman, 2004). The challenge is implementing and maintaining these policies, where an organization has to take appropriate steps in motivating their employees to take security seriously.

Ruighaver et al. (2007) highlight that when there is a security culture in an organization, employees will be expected to understand their behaviour confirms to organization's security or not. For instance, the employee will know that using the organization computer is not the same as using their home computer. In other words, if the policy is implemented properly in the organization, the behaviour of employees might change and the security culture will lead to security compliance (Thomson & von Solms, 2004). Evers & Day (1997) stress that cultural difference is a vital issue concerning attitudes towards computers and therefore employees have to apply the policy in a manner which is based on knowing their with responsibilities from the very beginning. This means that employees should not wait for crises to happen.

Security policy cannot tell employees what to do in every single situation in which they may need to perform a security decision. Leach (2003) argues that employees build their own personal policy to add to the existing organization policy by learning from their surroundings. This personal security policy is based on their experience with security incidents. For example, if an employee clicks on an email attachment from an unknown sender and this activity affects the organization, then this employee will not open an attachment again. Workman (2007, p. 317) stresses that the "*perceived severity of threat will lead people to behave in a more cautious manner if their perception of the damage or danger increases*".

2.8 The Human Element

Generally, employees work in an organization for different reasons. For some it could be related to a good salary, for others it may be about an opportunity for training that leads to other positions, or for others it might be about the social environment. Even though people practice security as an aspect of their daily life, they feel secure when they are protected from harm and will protect themselves naturally (Schneier, 2003). In information security people are the key to all security measures (Wood, 1982) and a link in the security bond (Cooper, 1984). People working for an organization carry out its business and by doing this they gain legal access to the organization's information assets and infrastructure. Organizations, to a large extent, trust their employees to handle information properly. "*User support resides in the people throughout the organization and represents a critical functional layer that could be rather useful in the overall defense strategy"* (Dhillon, 2006, p. 104). Fitzgerald (2007) explains that employees can be the "front-line" eyes and ears of the organization and inform of any security breaches for investigation i.e. employees have a dual role as threats and defense.

"*The internal security threat is a threat area encompassing a broad range of events, incidents and attacks, all connected by being caused not by external people who have no right to be using the corporate IT facilities but by the company's own staff, its authorized IT users*" (Leach, 2003, p. 685). An internal security threat does not only cover employee errors and omissions, it also covers intentional employee acts against the organization (Hitchings, 1995). In other words, employee failings can negate even the strongest security measures. Examples of this are when employees leave machines logged on while out at break time, stick notes of their passwords to the computer's monitor or reveal confidential information regarding the organization, for example.

Technology has magnified internal threats. Previously, if an employee wanted to steal some private or confidential information from a big project, they would have to physically carry out piles of paper or boxes. However, nowadays an email or a pen drive will do the job easily without anyone noticing.

A recent study by Cisco in 2006 (Cisco, August 2007) of more than 2000 remote workers and IT decision-makers in ten countries: (Australia, Brazil, China, France, Germany, India, Italy, Japan, the United Kingdom and the United States). Explored remote workers' attitudes and behaviour regarding security, as well as their perceptions and expectations of IT. Some of the findings suggest that:

- 29 percent of remote workers use the company computer for personal use.
- Nearly 40 percent of remote workers said they use their work computers for Internet shopping.
- 21 percent of the remote workers admitted that they allowed others to use their work computers.
- 38 percent of the remote workers reported that they click on unknown e-mail messages but do not open attachments.

These results indicate that technological solutions are vital in safeguarding organizational assets but the usefulness of these solutions is uncertain (Dhillon, 2006) due to employee practices. As Fitzgerald (2007) explains, employee practices could affect an organization's security to be either strengthened through compliance or otherwise compromised. As a result strong technology to secure information systems will not eliminate the vulnerabilities to information. A combination of people, processes and technology is required to achieve successful information security (Nicastro, 2007). As explained earlier this is what could be defined as in-depth protection, where the organization will protect its information through applying different mechanisms. An organization could depend solely on technology, though this protection will fail in time, or try to use a combination of mechanisms which are far harder to penetrate than a single one. For instance, firewalls alone are powerless to protect information assets without some integrated security mechanisms such as stronger authentication, access control, audit trails and encryption technologies; all will help to make the correct information available to those who have legitimate access to it.

Kevin Mitnick, one of the most famous hackers, as cited by the Economist (2002), explains that: "*The human side of computer security is easily exploited and constantly overlooked. Companies spend millions of dollars on firewalls, encryption and secure access devices, and It's money wasted, because none of these measures address the weakest link in the security chain*", where the weakest link is people (Lampson, 2002; and Sasse & Flechais, 2005). This is clearly seen in the technique of social engineering to gather any useful information by exploiting employees' lack of security awareness. Techniques of social engineering are used to manipulate people into disclosing confidential information (Mitnick & Simon, 2002) to be used to harm the organization. For example, the hacker will make a telephone call to a number of innocent employees sequentially to obtain information from them or to get them to carry out a certain task. This task could be telling the employee that this call is from the network team and they are going to update the system and they require the employee to change his/her current password to another password for some time until they get the system updated.

The benefits of an information security policy in an organization are not only that all the employees are involved in securing the organization's assets, but also that it minimizes employees' errors (Adams et al., 1997). Information security in an organization is becoming more and more an employee matter (Hone & Eloff, 2002; and Whitman et al., 2005); they cause the most information security breaches (Kotulic & Clark, 2004; and Payne, 2003). These errors are not only threatening to the integrity of organizations but are also expensive due to the loss of information or cost of fixing the problems. It can also damage an organization's reputation.

Workman (2007) clarifies that most of the research done into information security defences has investigated either the security technologies or the management of security infrastructure. He sees that to protect the organization is more about employee behaviour towards security threats. Workman et al. (2008) stress that understanding employee behaviour towards security has not been fully addressed.

The next section will discuss employee compliance to their organizational security policy.

2.8.1 Compliance to Information Security Policy

Employee non-compliance can be related to wider models of human error (Madigan et al., 2004). It is not necessarily because people do not care about security; they may not have sufficient knowledge to maintain good security (Sandhu, 2003). Zurko et al. (2002), stress that employees often are not aware of the security consequences of their actions. They do not understand enough about the impact of their security decisions. McKay (2003) argues that organizations around the world are failing to make their employees aware of the security issues and the consequences. This implies that understanding the elements of the human factor will improve information security effectively in the internet era.

As mentioned above, the behaviour of people may be influenced by a number of variables and hence risk security in a number of ways. According to Henry, "*A security program is only as good as the people implementing it, and a key realization is that tools and technology are not enough when it comes to protecting our organizations. We need to enlist the support of every member of our companies. We need to see the users, administrators, managers, and auditors as partners in security. Much of this is accomplished through understanding. When the users understand why we need security, the security people understand the business, and every one respects the role of the other departments, then the atmosphere and environment will lead to greater security, confidence, and trust*" (Henry, 2007a, p. 154).

Security policy stimulates accountable behaviour among the organization employees (Nijhof et al., 2003). According to Prenzler (2007, p. 35) "*if crime opportunities arise out of the changed routine activities of people, then we need to develop routine precautions that close down those opportunities*". There is no point in organizations having a policy without the possibility to monitor and enforce compliance with such a policy (von Solms & von Solms, 2004). For organizations it is critical to be able to always monitor and measure the effectiveness of their compliance program (Thrasher, 2003). Monitoring compliance and acting if any cases of non-compliance are found can be done by using technical and non technical measurement tools. According to von Solms & von Solms (2004) these measurement tools should not be wished for and dependent on annually or semi annual internal audit. Reviewing and monitoring regularly is the key to checking employee compliance with organizational security policy.

Leach (2003) explains that organizations have to rely on their employees to make reasonable decisions for any task that has a security or control element to it. He shows that that there are six factors that have a strong influence on employee security behaviour, as shown in Figure 2-9.

Figure 2-9 Employee's Behaviour in Security (Leach, 2003, p. 686).

As Leach (2003, p. 686- 689) explains employee behavior in security, can be seen from Figure 2-9 and is related to:

What employees are told: security policies, standards, procedures, help employees to practice security. Their behavior varies according to the policy's ease of access, completeness of its coverage, the clarity of the stated security values and the consistency of its security values.

What employees see in practice around them: employees learn from each other and they build their security behaviours and attitudes according to senior management, or colleagues’ behaviour and organizational security culture. Aspects of the security culture, such as monitoring security behaviour, rewarding good behaviour and taking action against bad behaviour, affect employee behaviour.

The user's security common sense and decision making skills: security policy cannot explain the exact security decision for every event that the employee might come across. Therefore employees will build their own personal policy to add to the existing organization policy.

The user's personal values and standards: when employees' personal values conflict with the organizational values and standards, most employees will not continue under pressure, so either they will modify their principles or quit the job.

The user's sense of obligation: employees feel psychological stress to perform according to organizational prospects and to restrict their behaviour to stay in the boundaries of accepted practice. However, if employees feel that the organization has done them wrong then they may become security enemies to the organization.

The difficulty in complying: if security controls are hard to achieve, or benefits are not clear, then employees will have reason to get around the controls.

An organization is responsible for addressing the different types of vulnerabilities and threats through policy, security mechanisms (controls), education, training and awareness programs (Whitman, 2004). As a result, when an organization institutes awareness programs employees will change their behaviour from security vulnerability to being defensive against security breaches. Siponen (2000) indicates that awareness helps to reduce employee errors. In addition, organizations should not underestimate the importance of information security awareness training (McCoy & Fowler, 2004).

Literature in information security and the international standards emphasize awareness and training of employees, where this involves all members of the organization from the top management down to the end-users. Ultimately, everyone has a different role in information security, however, there is no evidence in previous literature of the role that awareness programs have to play in reducing employee breaches or in making a difference in employee compliance to an organizational information security policy. Workman et al. (2008, p. 2) raise an important question on whether awareness will help: “*why do people who are aware of IS security threats and countermeasures neglect to implement them?*”. They further describe that this subject is not fully addressed.

Therefore, an investigation later in Chapter Six will attempt to explain the reasons behind employee non-compliance.

2.8.1.1 Threat to Compliance

The literature describes many reasons for employee non-compliances with an organization's security policy. These are discussed below:

Individual Attitudes or Personality: Thomson & von Solms (2004) highlight the fact that personal *values* and *beliefs* have an influence on employee behaviour regarding information security. Values for Posnser et al. (1987, p. 376) are defined as "*general standards by which we formulate attitudes and beliefs and according to which we behave*." Jolibert & Baumgartner (1997) clarify that values are subjective due to the social norms that lead people in their actions. Therefore, people differ in their beliefs and personal values and this affects their attitudes to organisation security policy. Reid (2006, p. 22) says attitudes "*may be based on our knowledge, our feelings and our behaviour and they may influence future behaviour*".

Finegan (1994) suggests that employees distinguish ethical dilemmas in the organization differently and that their views on the integrity of exacting behaviour are influenced by their personal values. Therefore, different employees sharing the same values will behave in a similar way when faced with any security decision, at least with respect to the organization's rules and regulations with security policy. One approach is for organizations to recruit employees sharing the same values related to security. But according to Finegan (1994), when organizations try to select employees who share the same values and beliefs, they face some possible problems. These include limitations in individual creativity and preventing the entry of a variety of cultural groups into the organization.

In addition, Leach (2003) clarifies that when employee values and beliefs do not match an organization's values and standards, this will give employees a choice of either modifying their own principles or leaving the job; in both cases this will do good for information security but also they have another option of not complying. It is more interesting that organizations have employees with different opinions but it should not go against the organization in term of following the organization security policy to protect organizational assets. This could be managed by awareness and education, as will be explained below.

Lack of Knowledge and Skill: Employee differences are directly related to knowledge, skill and motivation (Campbell et al., 1996). When an employee does not have enough knowledge of policy and skills to conform with the security policy and regulations in the organization then the employee will not be able to comply (Neal & Griffin, 2002). If an employee does not have enough motivation to comply with the security policy and regulations then the employee may not comply (Neal & Griffin, 2002).

Effective security awareness may help to modify the behaviour of employees. This is when employee behaviour towards security is related to "*defending the organization against threats, contributing to its good reputation, and cooperating with others to serve the interests of the whole*" (Dyne et al., 1994, p. 767). McIlwraith (2006), stresses that awareness is related to two areas, which are the practice of making employees aware of issues linked to information security and encouraging (cajoling, or threatening) employees to perform in a way that is proper for the value of the information they work with as part of their daily job.

These ideas do not explain the attitudes of the employees who are aware of the consequences of non-compliance as Workman et al. (2008) describe. Many are not fully complying with security policy, but do have knowledge related to their individual values, beliefs, or work pressure to get the "job done". Security awareness and training programs can provide employees with information about their organization's information security policy to sensitize them to risks and possible losses and to train them how to behave securely and use technology in-line with security procedures (Denning, 1999). There is no evidence that awareness does change employees' attitudes towards security, but it is an available choice for organizations to apply and hope that it will do change employee attitudes. Stahl (2007, p. 555) states that, "a*lthough an awareness training program can impart information security knowledge, it rarely has a significant impact on people's feelings about their responsibility for securing information or their deeper security instincts. The result is often a gap between the dictates of information security policy and the behaviours of our people*".

This issue is covered in more depth in Chapters Four and Six.

Leadership: Management plays an important role in motivating employees to perform security tasks (Neal & Griffin, 2002). When management fail to exercise what is expected from them regarding information security, employees will not take security seriously (von Solms & von Solms, 2004). A clear vision for information security from the senior management is required to effectively influence other employees' behaviour to protect the organization's information assets. Leach (2003, p. 687) explains that employees "*build their security attitudes and set their own security behaviour according to the values and attitudes and set their own security behaviour of senior management*". More about this issue is described in detail in Chapters Four and Six.

Organizational Culture: This matter was been described in detail in section 2.7.

Invisible Security Policy: Leach (2003) argues that employee security behaviour security varies according to the ease of access, as well as the clarity of the policy. Unfortunately many organizations do not have the skill or the experience to formulate an information security policy (Doherty & Fulford, 2005). A clear and visible information security policy will help employees to understand good security behaviour. Otherwise employees may try to find ways around security controls to let them do their job (Post & Kagan, 2007). Schwiderski-Grosche (2006) stresses that experience proves that security can only be provided, if it is more clear, or visible, to employees. If the policy is not clear to employees it could send the wrong message and not been taken seriously (Barman, 2001). Workman (2007, p. 328) argues that organizational security policies "*should be established that address the classification of information and the circumstances under which sensitive information can be divulged, and should also include the processes and accountability for reporting suspected incidents*". This issue has been discussed in detail in section 2.5 and will also be in Chapters Four, Five and Six.

Trust: As humans we learn what kind of information to divulge or to withhold and who can be trusted with our information (Chen & Barnes, 2007). Technology has changed the quantity and quality of information available about individuals and has also changed our perceptions of when to trust and whom to trust (Guadangno & Cialdini, 2002). Kaplan (2007, p. 301) explains the reasons in general why people trust:

- "Evidence that 'things seem to be doing their jobs'.
- Lack of evidence to the contrary.
- Anecdotal evidence from others in the community".

There is no one universal definition of trust (Castelfranchi & Pedone, 1999); it has different meanings in different situations. Instead of defining trust, much literature refers to the *effects* of the existence of trust in a relationship. The following Figure 2-10 describes what trust is about.

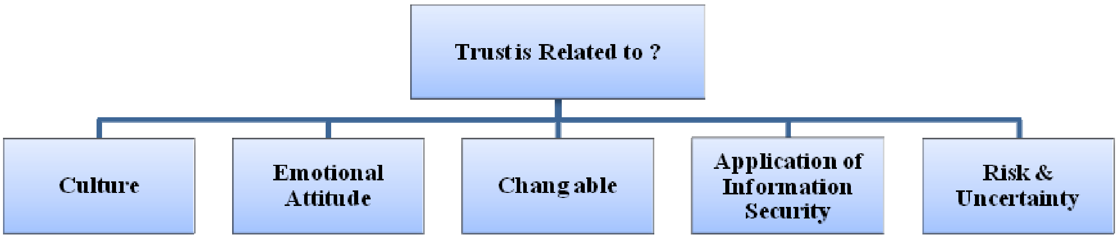


Figure 2-10 Trust is Related to?

Sasse (2004) states that trust is only required in situations characterized by risk and uncertainty, such as exist on the Internet. People will not continue to use e-commerce systems, for example, unless they trust these systems with their personal and financial details. According to Witty et al. (2001), trust is the result of applying a combination of authentication, authorization, integrity and non-repudiation controls. In other words, trust results from the effective application of information security techniques.

Reigelsberger & Sasse (2003) define trust as an emotional attitude. Trust, in the information security context, is related to the experience of the individual. For example, when an individual provides information to a doctor, a bank or insurance company. Equivalently the individual expects that the information will be used for the purpose of providing the service being requested and not for any other purpose.

Paine (2003), states that trust is only one component of the strength of relationships in business management and organizational communications. Trust is dynamic and changeable in different circumstances. It is time dependent and signals a willingness to be vulnerable (Corritore et al., 2003). An example of trusting behavior is when some employees do not log off their machine while they are absent from their office.

Trust can also be linked to culture (Kaplan, 2007) since it, too, is influenced by norms, values and beliefs, and plays an important role in the effectiveness of information security mechanisms. Individuals from one culture may well require more reassurance to increase their level of trust than someone from another culture. Understanding different cultures helps us to understand attitudes towards compliance with security policies and information security in general.

Purser (2004) argues that many issues, including trust, have grown dramatically in importance as a result of the increased use of networked applications. Employees rely on trust in various aspects of security everywhere they use the organization’s systems (Kaplan, 2007). For instance, employees often trust their organization's web browsers, they trust their organization’s firewalls to filter spam emails, they trust their organization’s anti-virus software and so forth. This trust may explain why some employees access email attachments, where it could bring the risk of a virus. They rely on specialized support to fix any problem and this brings in room for complacency.

Organizations apply security policies to help to control employee practices in security, but trust can be seen as a double sided weapon. In some cases people may be trusting when they should not have been, which might affect them adversely. As trust is totally essential in securing an organization's sensitive information people need to cope effectively with information security. Therefore, in organizations trust can be seen when employees trust an organizational system and employees trust each other. This will enhance interactions so as to make work easier and facilitate teamwork.

2.9 Conclusion

Considering what has been discussed in this chapter, it seems that there is a need to understand what makes information secure in organizations. What are the threats that the organization must deal with and what are the criteria of a beneficial information security policy? Policies are in place, but why do employees not comply? Policy encourages responsible behaviour among the organization's employees but it is not sufficient to control their behaviour. It is always better to make it clear to the employees *what they should do and what they should not do*. Organizations need to bring new ideas to engage their employees to take decisions on information security. For example, the people who develop the policy build it according to what they believe is suitable for the organization, without any sense of the practicality of the policy. They have to ask, is it applicable to employees or not? Security policy could bring risks to an organization through either being not well written or too complex in terms of employees' compliance to it. However, there could be a chance to change attitudes if employees have the chance to give their opinions about any policy as they are the ones who are going to apply it and work with it. It should not be forgotten that security policy itself can have a part in helping employees to comply with an organization's rules and regulations.

Information is not the same in terms of value or use to every organization, or in the risks that it is subject to as stated by Appleyard (2004). Organizations must institute security policies and regulations to prevent unauthorised access to their own resources. Until security issues are addressed, therefore, a crisis is the worst time to take security seriously. Huston (2001) argues that security is often not taken seriously until after a serious breach happens.

Consequently, an information security policy plays a major role in helping the new age of technology. Given that the number of organization security breaches is increasing day after day and that information is more accessible, the hazards are greater and it is more likely that stronger security will be needed (Brown & Duguid, 2002). As organizations depend more on computers, the threats are increasing. Vulnerabilities are when the organization's system is susceptible and open to attack or damage. When the number of employees, applications and systems increase, the management of the organization becomes much more difficult and consequently vulnerability will increase. Therefore, the larger the organization the greater the need for standards, written policies, procedures and guidelines to ensure the continuing consistency of organizational security (Fitzgerald, 2007).

Information security concerns people and is actually more of a managerial problem than a technical problem. Therefore it cannot be dealt with purely technically. From my personal point of view, if organizations that implemented information security in the 1990s are still facing problems with implementing a good information security then perhaps they could teach firms who are only now adopting information security. It could be helpful for the new organizations to learn from other experiences and to adopt the successful aspects of these and try to avoid their mistakes.

Finally, organizations need to think carefully when implementing information security since, as Dhillon & Backhouse (2000, p. 127) state, "*facing pressures of organizational cost containment and external competition, many companies are rushing headlong into adopting IT without carefully planning and understanding the security concerns*".

Given what has been described so far, the research that follows is going to adhere to these main objectives:

- Explore and identify factors affecting the implementation of information security.
- Investigate what makes an effective security policy.
- Investigate the effect of a security policy in reducing security threats.
- Explore different issues of information security are general issues in different environments.
- Investigate the reasons behind and impact of employees' non-compliance with an organization security policy.

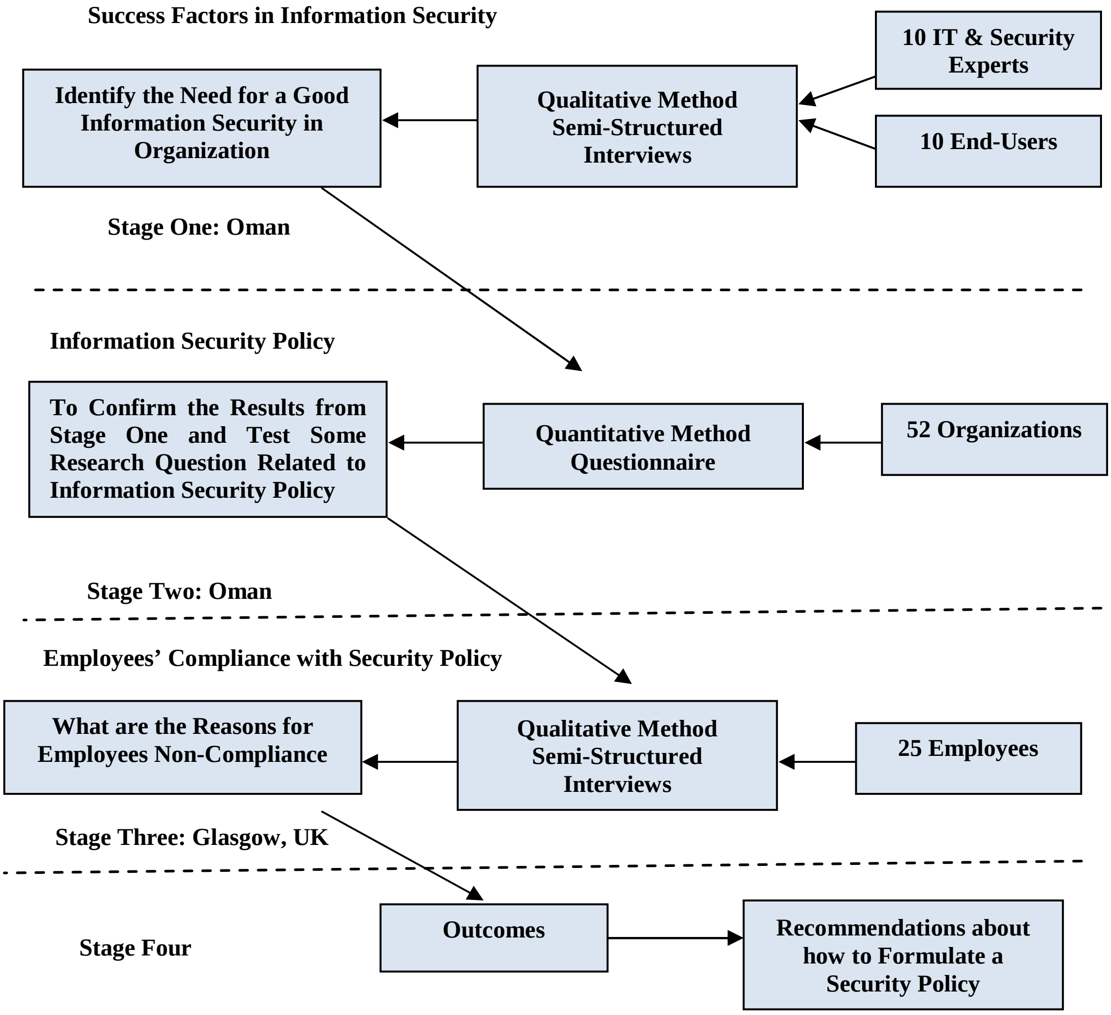
The next chapter will explain the different methods that have been used to achieve these study objectives

Chapter Three

Methodology of Research Study

The previous chapter explained issues related to information security in organizations, such as organizational security culture, information security policy, compliance to information security and threats to compliance. This chapter will explain the investigative methodology that has been used in this research study, which is briefly illustrated in Figure 3-1.

This study is divided into four stages. Each stage uses a different method. The details of the four stages will be explained later in the chapter. These four stages were developed from the literature review in the previous chapter.



Success Factors in Information Security
10 IT & Security Experts
Identify the Need for a Good Information Security in Organization
Qualitative Method Semi-Structured Interviews
10 End-Users
Stage One: Oman
Information Security Policy
To Confirm the Results from Stage One and Test Some Research Question Related to Information Security Policy
Quantitative Method Questionnaire
52 Organizations
Stage Two: Oman
Employees' Compliance with Security Policy
What are the Reasons for Employees Non-Compliance
Qualitative Method Semi-Structured Interviews
25 Employees
Stage Three: Glasgow, UK
Stage Four
Outcomes
Recommendations about how to Formulate a Security Policy

Figure 3-1 The Four Stages of the Research Study.

This research has been divided into four stages. Each stage built on the results from the previous stage. The first two stages were conducted in the Sultanate of Oman in order to use a population just starting out in the information security area. The third stage was conducted in the UK at Glasgow University because employees are somewhat familiar with the idea of information security, which provides a useful contrast.

This chapter is organized as follows. The following section constitutes the introduction. Section 3.2 presents the different method approaches. Section 3.3 discusses the different research strategies available within these approaches. Section 3.4 presents the method used for the research. Section 3.5 describes the participants. Section 3.6 presents an overview of the research. Section 3.7 explains the validity of the research method and questions. Finally, section 3.8 presents the conclusion of this chapter.

3.1 Introduction

Bell (1984) suggests that classifying an approach as quantitative, qualitative, ethnographic, survey, action research, etc., does not mean that once an approach has been selected, the researcher may not move from the methods normally related with that type. Also, Bell indicates that each approach has its strengths and weaknesses and each is particularly suitable for a particular context and that the methods of data collection will depend on the nature of the inquiry and the type of information required. Therefore, the choice of which approach to use is based on the research problem and what the researcher is seeking.

The main objectives of this study are to:

- Explore and Identify factors affecting the implementation of information security.
- Investigate what makes an effective security policy.
- Investigate the effect of security policy in reducing security threats.
- Explore if different issues of information security are general issues in different environments.
- Investigate the reasons behind employees’ non compliance with an organization's security policy.
- Investigate the impact of employees’ non-compliance with an organization’s security policy.

3.2 Methodology Research Approach

To achieve the objective of the research study, as explained above, there are two different broad methodological approaches to select, which are:

- Qualitative approach
- Quantitative approach

3.2.1 Qualitative Research Methods

Creswell (2003, p. 198-199) summarizes the characteristics of the qualitative method: "*it occurs in natural settings, where human behavior and events occur; [and is] based on assumptions that are very different from quantitative designs. Theory or hypotheses are not established a priori; the researcher is the primary instrument in data collection; the data that emerge from a qualitative study are descriptive. That is, are reported in words (primarily the participant's words) or pictures, rather than numbers; the focus is on participants' perceptions and experiences... on the process that [is] occurring as well as the product or outcome*".

Data analysis in this method involves search for pattern, themes and holistic features. Furthermore, this approach describes more in words rather than numbers and draws from a range of methods. The qualitative methods generate hypothesis as well as test them, (Glassner & Moreno, 1989) and can be of most benefit in areas where there is little pre-existing knowledge. Bjorck (2001) uses the qualitative method to define some critical success factors for the implementation and certification of information security management systems (ISMS).

Using qualitative methods lets the researcher collect data using less structured research instruments. The results can offer insights on behaviour, attitudes and motivation. The research is more concentrated and flexible providing opportunities to explore recent insights with a smaller sized sample. However, the analysis of the result could be more subjective given the low reliability factors of using smaller samples. There are also problems with repeatability. The small selective sample size is related to the in-depth nature of the qualitative approach (Carr, 1994).

Cohen et al. (2007, p. 461) points out that "*qualitative data analysis involves organizing, accounting for and explaining the data; in short, making sense of data in terms of the participants' definitions of the situation, noting patterns, themes, categories and regularities…the analysis will also be influenced by the number of data sets and people* *from whom data have been collected*". The idea is that someone else conducting the same qualitative research at a different time could reveal something quite different. Qualitative methods include, for example, interviews, observation and ethnography. Bjorck (2001) uses a qualitative method to study information security consultants' experiences and insights relating to the implementation and certification of information security management systems (ISMS).

3.2.2 Quantitative Research Methods

Quantitative research methods examine the relationship between variables to support particular questions or hypotheses. This method tests theories and tests deductively from the literature or existing knowledge (Flick, 1998). Quantitative methods produced valid scientific answers and, accordingly, action was taken and changes took place (Carr, 1994).

The results of quantitative methods provide fewer details on behavioural attitudes and motivational issues behind responses or results. The results are often based on larger sample sizes and this can help to generalize the results (Scandura & Williams, 2000).

In the field of information security many researchers use quantitative methods as part of their research. For example, a recent study by Workman (2007) uses a quantitative method to investigate social engineering attacks in the form of questionnaire in a field study of a government-regulated entity that experienced serious security breaches in the past.

Quantitative methods includes questionnaires, lab based user studies and software logging.

3.3 Research Strategy

A "research strategy" offers a general plan for research and ensures that research questions are answered using appropriate methodologies. There are many strategies available to carry out research studies. Creswell (2003, p. 14-15) define some strategies associated to research method, which are:

<u>Quantitative Methods</u>

- **Experimental Research:** The purpose of experimental research is to study cause and affect relationships.

- **Survey research:** contains cross-sectional and longitudinal studies using questionnaires or structured interviews for data collection.

Qualitative Methods

- **Ethnographic:** This strategy will seek to understand the whole cultural group through the nature of their social structures and behaviours over a long period of time.
- **Grounded theory:** This strategy is not determined but derived from a general, abstract theory of a process, action, or interaction grounded in the views of participants in a study (for more details about grounded theory see Appendix C, p. 244).
- **Case studies:** This strategy explores in depth a program, an event, a process, or one or more individuals.
- **Phenomenological research:** This strategy identifies the real meaning of human experiences. Rich & Ginsburg (1999) clarifies that this approach is about understanding humans through the meanings inherent in their experience.
- **Narrative research:** This strategy interprets human motivation, perceptions and behaviour from reported stories about their lives.

3.4 Selected Research Method and Techniques

"*No research approach is complete or flawless; quantitative and qualitative methods have different strengths and limitation*" (Rich & Ginsburg, 1999, p. 371). This supports the need for using a combination of qualitative and quantitative methods in this study to avoid the limitations of one method. This type of approach produces better outcomes in terms of quality and scope (Tashakkori & Teddlie, 1998). The aim in using both qualitative and quantitative approaches is to provide a balance of strengths and to avoid overlapping weaknesses.

Rainer et al. (1991) use a combination of qualitative and quantitative approaches to risk analysis process for IT. Fulford & Doherty (2003) use a questionnaire to explore the application of information security policies in UK-based organizations and identify a need for more qualitative studies to explore and explain the same field. Also Voss (1985) uses an interview followed by a questionnaire to determine success in the development of application software.

This research is divided into three stages to achieve the objectives of the study. For the purpose of this study the researcher will use a semi-structured interview (qualitative method) for the first stage, questionnaire (quantitative method) for the second stage and semi-structured interview (qualitative method) for the third stage to maximise the breadth and depth of detail obtained. Details of the different stages will be described later in the chapter. Using mixed methods (triangulation) is recommended by both Carr (1994) and Bandyopadhyay et al. (1999).

3.4.1 Interviews

Interviews are the most widely used method in social science research. This is because of the flexibility of the technique and the great depth of the outcomes. Interviews will give the opportunity to the researcher to see the research topic from the view point of the participant and to understand how individuals come to have this perspective. The limitations as explained by McIlwraith (2006, p. 125) are that interviews can be "*expensive and slow; personal contact can reduce truthfulness or responses; [there is] no practical way to maintain anonymity; organization logistics [are] time consuming and expensive; [and the] interviewer can introduce bias.*"

According to Patton (2002); Briggs & Coleman (2007); and Bruce (2004) interviews can be categorized as:

- **Structured (standardized)**: use questionnaires based on predetermined and standardized schedules, usually with coded answers also used in quantitative research. The researcher asks the same set of questions in same order to different interviewees. The rationale about this interview is there is no flexibility in wording the questions. This is convenient for comparing different interviews (Di Milia & Gorodecki, 1997). It reduces bias from interviewer but can be inflexible.
- **Semi-structured (semi-standardized)**: also called guided interviews. This type comes between structured and unstructured interviews; the researcher will have a list of themes and questions to be covered and normally data is recorded by note taking or by tape recording. Semi structured interviews use open-ended questions, start with more general questions, for example (tell me about …) and most of the questions are created during the interview, such as (you said before…can you tell me more?).
- **Unstructured**: also called informal conversational interviews, this approach normally allows the researcher to gain additional information about the research

topic because of a free-talking style. This approach is difficult as the researcher generates and develops questions according to what the interviewees say. This approach is useful for narrative methodology (McCance et al., 2001) as it is more likely to produce stories.

There are also different types of interview set-up:

- **Face-to-face:** Answer rates are likely to be high and lead to obtaining some rich data.
- **Telephone:** This might be the relatively cheap and quick approach but there is no control over the interviewee's environment.
- **Group:** This approach is good if it is conducted in one or few locations. Also it gives a good opportunity to observe interactions between interviewees about the research topic.

All types of qualitative interviews have certain characteristics in common. Rubin & Rubin (1995) summarize common interview characteristics by adjustments of ordinary conversations, but with significant features. More interested in the understanding and knowledge of the interviewees than categorizing people or events in terms of academic theories; the content and the flow of the interview goes with what the individual interviewee knows and feels.

Based on this review, this research focused on using a face to face interview for the ‘in depth’ data it can provide. The limitation of the semi-structured method is that it is slightly less reliable because of the difficulty of exactly repeating the interview.

3.4.2 Questionnaires

A questionnaire is a term that includes all techniques of data collection in which a person is asked to respond to the same set of questions in a predetermined order. Questionnaires can be a very useful means of collecting large volumes of data and provide potential anonymity for the respondent, which can lead to more trusted or valid responses. The questionnaire can be filled out at the convenience of respondents without interviewer bias or error. The main difficulty in using a questionnaire is securing high response rate (Punch, 2003). Creswell (2003) suggests a following up approach to avoid such situations, such as sending an email for reminding, or following up by phone calls.

According to Saunders et al. (2000), there are different types of questionnaires, classified as:

- **Self –Administered Questionnaires,** such as:
- **Online questionnaire**: Using electronic mail or other online media.
- **Postal questionnaire**: These are completed by respondents and returned by post.
- **Delivery and collection questionnaire**: Delivered and collected by hand.

- **Interviewer Administered,** such as:
- **Telephone questionnaire**: These are managed using the telephone.
- **Structured interview**: Refers to questionnaires where an interviewer meets the respondents face to face but the interviewer does not move away from the questions.

The area of information security, particularly the process of implementation by the organizations, needs a careful understanding of what is required to achieve good security. Understanding employees' attitudes towards organizational security policy is crucial to avoid potential security breaches. Grounded theory (for more details about grounded theory see Appendix C, p. 244) was chosen for the analysis of the semi-structured interview data. The grounded theory strategy is suitable as it can derive in-depth data concerning the general area of information security. Also, it documents the participants' points of view when they talk freely about events, behaviours and beliefs in the information security area.

The grounded theory approach develops conceptual categories from the qualitative data and then new observations will be made to clarify and elaborate these categories. The data has been categorized by identifying some patterns or themes and organized to bring meanings into categories.

3.5 Selecting Participants

Gorman and Clayton (1990) state that in undertaking research in organizational surroundings, there is good reason to interview a variety of staff stratified within the organization to allow more views to be heard. Reid (2003) suggests that the researcher should select individuals who make positive contributions, display leadership qualities and reveal independent thinking. He also notes, for face to face interviewing, the researcher needs participants who are not hesitant to converse and share ideas and needs to decide a setting in which this is possible. The less articulate, shy interviewee may present the researcher with a challenge and less than adequate information.

Details of selecting participants at each stage of the study will be explained in the following sections.

3.6 Overview of the Research

This study is divided into four stages. A brief description of each stage is given below:

3.6.1 Stage One: Success Factors in Information Security – Semi-Structured Interviews, (Oman)

This research is part of a wider research project for government organizations in Oman implementing information security. The study is based on an exploratory approach using a semi-structured qualitative method for collecting data and using grounded theory to analyze the data. Currently there are approximately fifty-two government organizations in Oman (Omanet, April 2006). Two sets of semi-structured interview questionnaires were developed by the researcher, firstly for the IT & security experts who have not less than 5 years of experience with information security and secondly for the end-users who are familiar with information security and use computers on a daily bases. Due to the sensitive nature of the subject, the information technology authority (ITA, see Appendix A, p. 231) in Oman has been contacted and they provided the researcher with a list of ten experts and ten end-users from different Omani government organizations. A summary of the method is described in the following Figure 3-2.

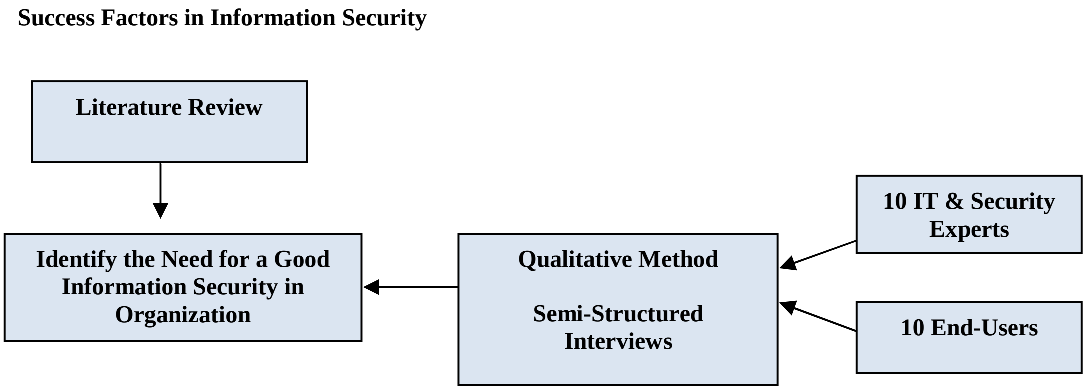

Success Factors in Information Security
Literature Review
Identify the Need for a Good Information Security in Organization
Qualitative Method
Semi-Structured Interviews
10 IT & Security Experts
10 End-Users

Figure 3-2 Stage One Investigation.

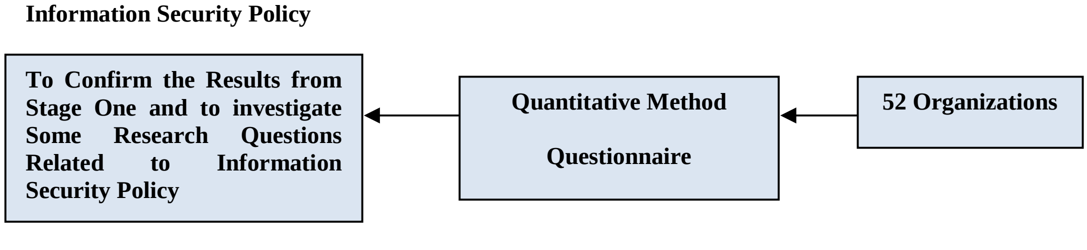
Each interview was required at the convenience of the interviewee and the interviews took place at the interviewees' offices. The ethical points, such as confidentiality of the data, were explained to all participants on a written piece of paper (see Appendix A, p. 232). The objectives of the research study, the choice to participate or not to participate in the interview questionnaire and finally the permission to tape record the interview, were mentioned as well. The interviewees were informed about their right to withdraw from an interview at any time without giving any reason.

One hour was given for each interview for the IT & security experts and thirty minutes for the end-user because their questions are not as in-depth as the IT & security experts' questions. All of the participants refused to tape record their interviews and all of them were thanked personally for their participation. This could be related to cultural issues or because of the sensitive nature of the study.

The purpose of the approach is to explore and identify the important aspects of the implementation of information security in government organizations. Furthermore, the study was intended to identify success factors for the implementation from the experts' perspective. It investigated what concerns end-users have about information security. The semi-structured interview questionnaire was based on five areas which were developed from the literature review in Chapter Two. Details of this investigation are explained in Chapter Four.

3.6.2 Stage Two: Information Security Policy – Questionnaire, (Oman)

After analyzing the outcomes from the semi-structured interviews a questionnaire was developed including some relevant questions from the Doherty & Fulford (2005) survey questionnaire for information security policy and other questions identified from the literature. The questionnaire was distributed to fifty-two Omani governmental organizations in paper form to the IT department of the organization. To give weight to the importance of the questionnaire and to avoid any problems with the sensitivity of the subject, the information technology authority (ITA) in Oman took part. The questionnaire was delivered and collected by hand with the help of the ITA. A month was given to each organization to fill out the questionnaire. A total of forty-two responses were received representing a response rate of 81% which indicates a high level of responding. A summary of the method is described in Figure 3-3 below.


Information Security Policy

To Confirm the Results from Stage One and to investigate Some Research Questions Related to Information Security Policy

Quantitative Method

Questionnaire

52 Organizations

Figure 3-3 Stage Two Investigation.

The research questions of this investigation centres around the effectiveness of the security policy to reduce organization security breaches. It is understood that the limitation of this research and the sensitive nature of information security might make the participants not say what they want to or what they actually believe. The number of security breaches that the organizations are experiencing is not exactly known. Nobody reports security breaches because it makes them look bad so that makes it hard to come up with an accurate estimation. There is no evidence in the literature as to what an effective security policy is or what makes good security policy. Therefore this research is about reported attributes of security policy and reported effectiveness of security policy compared to reported frequency of security breaches. Details of this stage are explained in Chapter Five.

3.6.3 Stage Three: Compliance with Organization's Security Policy – Semi-Structured Interviews, (UK, Glasgow)

The findings from the quantitative analysis in stage two confirm that there is no statistically significant evidence that the adoption of security policy criteria will reduce the reported level of breaches. Also there is no statistically significant evidence that the adoption of success factors of information security will reduce the reported level of breaches in an organization. These results show a need for further investigation of employee behaviour with security in an organization using semi-structured interviews. A summary of the method is described in the following Figure 3-4.

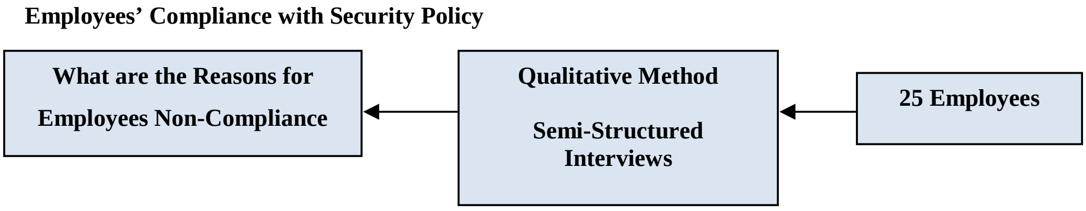

Employees' Compliance with Security Policy
What are the Reasons for Employees Non-Compliance
Qualitative Method
Semi-Structured Interviews
25 Employees

Figure 3-4 Stage Three Investigation.

This study explores the opinions of employees regarding typical activities with security implications within their organizations. Scenario-based questions were used to explore the interviewee's point of view of other activities where a choice had to be made. The interviewees were asked to provide opinions based on different scenarios on employees' behaviour. A scenario based question was used to give employees the freedom to give their opinion with no pressure to explain what they think about the different security activities mentioned. Each of the scenario questions is related to security activities that any employee could be practicing in an organization.

The selected samples for the semi-structured interviews are a mixture representing a cross-section of twenty five employees from different departments from Glasgow University, UK who are familiar with organizations security policy. For such sensitive investigations about employee compliance with security policy it had been decided to conduct the interviews at University of Glasgow for the ease of access and because participants feel comfortable in discussing this matter with someone considered a colleague. More about the reasons for conducting this investigation in the UK is discussed in Chapter Six.

The study was conducted in two parts. The first part was based on an exploratory approach using a semi-structured interview for collecting data and the grounded theory qualitative method to analyze the data. Thirty minutes were given to each employee and the confidentiality, objective of the research, right to withdraw from the interview was mentioned at the interview (see Appendix A, p. 232). The participants in this investigation agreed for the interviews to be tape recorded. Details of this stage are explained in Chapter Six.

3.6.4 Stage Four: Recommendations about how to Formulate a Security Policy

The findings from the literature with the findings from stage one, stage two and stage three about what makes an effective information security policy in an organization were combined. All the findings were tested on real-life examples of existing security policies from different organizations to give recommendations about how to formulate a security policy to encourage employee compliance and therefore reduce security threats.

3.7 Reliability and Validity of the Selected Methods

In order to explore successfully the research questions of each of the research stages it is very important to demonstrate the validity and reliability of the methods used in the research. Straub (1989, p. 160) describes reliability as "*a statement about the stability of individual measures across replications from the same source of information*" which means will the test give similar outcomes if it is tried again in the same way. Oppenhiem (1992, p. 162) lists different kinds of validity:

- **Content validity**: do the items in the measurement or test reflect some kind of balanced coverage of the issues, skills or knowledge to be measured?

- **Concurrent validity**: do the outcomes of the measurement relate to some other well-validated measures of the same topic, theme or skills?
- **Predictive validity**: do the outcomes of the measurement relate to some future criterion such as job performance, recovery from illness or future examination attainment?
- **Construct validity**: do the outcomes of the measurement relate to some set of theoretical assumptions about an abstract construct?

The questions of the semi-structured interviews and the questionnaire for all three investigations of the research have been validated and checked for reliability by doing the following:

- Approval gained for the method by an experienced person in the field of social science research who has been working with PhD researchers for many years;
- Approval of the questions by some experienced person in the field of information security who has worked in the field for more than ten years;
- After some modifications some experienced person critically evaluated the questions focusing on the clarity, question wording and validity, to enhance the outcome of the results.
- Pre-testing of both research methods has been done to check if the questions are being understood in the way intended. This has been done by applying the research method with four to five colleagues or friends before the real investigation started.

3.8 Conclusion

The use of information security is affected by social, cultural, economic and political forces. As described in Chapter Two Section 2.8 human threat is the most fundamental threat in any system. As a result, information security depends on human nature, life experience and the motivation of people. In this chapter the researcher indicated the methodological approach of this study. The methodology employs a combination of quantitative (questionnaire) and qualitative (interview) methods to collect data. Each of the mentioned research methods has different strong points and limitations. Therefore using a combination of qualitative and quantitative research methods as described will facilitate the researcher to get the best of both methods into in this study and avoid the weakness. The underlying principles of empirical research were studied in order to consider the appropriate research methodology for this study.

There are a number of reasons for selecting the qualitative methods described. One is to learn about people's experience in information security and to find out what people think and feel about information security. A further motivation is to understand the human factors and influences in information security. The flexibility that the qualitative method will imbue the research process with, by giving the ability to understand the research topic in depth, should not be forgotten. The quantitative approach will allow generalisation of the results and it also means that it can be replicated. The idea is to simply use qualitative data collected from interviews to support the quantitative data collected from the questionnaire and then use further interviews to answer some emerging issues from the quantitative outcomes.

Combining the qualitative and quantitative methods of research described can produce a final product which can underline the significant contributions of both (Nau, 1995). The flexibility of using different methods provides the researcher with the opportunity to use the best of qualitative and quantitative techniques in research studies which attempt to support and complement findings and gives the research a balanced approach. Due to the sensitive nature of the study the sample size was selected for each of the investigations. According to Goering & Streiner (1996) a precisely selected respondent gives the researcher the chance to learn the most from them. Cohen et al. (2007) explained that a sensitive subject is a reason for using a selected sample size.

The next chapter explains the data analysis of the stage one study. The information security concept in Oman is immature. Therefore, the research is exploring the topic using qualitative techniques to elucidate what makes a successful implementation of information security. In other words, the use of policies and legislation in an organization, as well as other factors.

Chapter Four

Success Factors in Information Security – Semi-Structured Interviews, (Oman)

The previous chapter explained an overview and rationale for the methodology of this research. In addition, the reasons for choosing a specific research method (Qualitative/Quantitative; interview/questionnaire) were presented. This chapter will identify aspects of the implementation of information security in Oman through reviewing governmental organizations' different information security practices, in order to find out the successful factors for implementing information security in Oman. A qualitative analysis (using interview methods) of the organizations' experience formed the basis of the study.

This chapter is organized as follows. The first section 4.1 outlines the introduction. Section 4.2 illustrates the methodology applied in the research study. Section 4.3 presents the results of the analysis. Section 4.4 presents a discussion of these results. Finally, section 4.5 presents the conclusion of this chapter.

4.1 Introduction

In December 2007 in the UK, The Ministry of Defence (MOD) lost the personal data of 600,000 people, when it was stolen from a junior Royal Navy officer's car in Birmingham. According to Defence Secretary Des Browne, "*a probe into the loss of a laptop with details of 600,000 people has uncovered two similar thefts since 2005*" cited by BBC News (BBC, January 2008). The Times online (Timesonline, January 2008) comments that " *the latest theft of personal data will add to the Government's embarrassment over recent serious of losses of sensitive information*". The following serious losses happened last year (source: Timesonline, January 2008):

- November 20, Revenue & Customs admits that the personal details of 25 million child benefit claimants have been lost.
- December 11, Police investigate after details of more than 6,000 Northern Irish drivers disappear.
- December 17, Announcement that information on three million learner drivers is missing.

- December 23, Medical records missing at nine NHS trusts.

Information security is therefore important to organizations (Garg et al., 2003). As von Solms (1999, p. 51) states "*if an organization is found secure enough by others, it will be welcomed to join [the community], if not, it may be excluded and left in the cold*". Organizations are under pressure to demonstrate the effectiveness of their information security programs. Unfortunately, it is not clear yet what is 'good enough security' (Sandhu, 2003). This is related to risk assessment (Hoo, 2000), since when an organization system is secure today it does not mean that it will be secure tomorrow, as new employees are recruited or new breaches appear.

According to Bishop (2003, p. 69), security is related to three elements: requirements, policy and mechanisms. Requirements describe security targets (*what organizations expect security to do for them*) to define what kind of security level the organization needs. Policy defines the meaning of security (*what steps do organizations takes to reach their security target*). Mechanisms enforce policy (*what tools, procedures, and other ways do organization use to ensure that requirements and policy are followed*).

Sandhu (2003, p. 67) suggests the following for organizations in adopting information security: "*Everything should be made as secure as necessary, but not securer*". No organization can achieve perfect security. Moreover, what is required of an organization is to look for an effective information security plan. Fung & Jordan (2002, p. 527) state that, "e*ffective information security has to build on a good technical infrastructure, appropriate information security policy, procedures and an information security culture*". Effective security relies on creating a workplace environment and organizational structure where management recognizes and completely supports security efforts, the policies in place and also encourages employees to implement security.

Fulford & Doherty (2003, p. 106) summarize some key factors that guide effective information security management:

- "The need for senior management commitment and support to information security management;
- The detailed assessment of potential security risks and threats;

- The implementation of appropriate controls to minimize or guard against those risks and threats; and
- The thorough communication of security issues to users of both information and information systems through relevant education and training".

In order for organizations to achieve a stronger protection over their information the recognition of the main threats facing organizational information is urgently required (Whitman, 2003). When an organization neglects the importance of information security they can be open to security breaches (Straub & Welke, 1998). Fung & Jordan (2002) believe that breaches in information security help an organization to find out the weaknesses of their system and provide a good guideline from which to learn lessons; of course this assumes such breaches are manageable and not harmful.

Several recent breaches in government organization around the world have raised the need for a change in the way organizations deal with information security. According to Whitman (2004) these types of threats urge the need for understanding and implementing good quality information security as discussed earlier by Fulford & Doherty (2003). Therefore, organizations need to recognize what possible factors need to be considered when implementing information security. Holistic security that runs to the very top of the organization and through every employee will offer the strongest foundation to secure against future attacks. Information security is much more than a specialized function; it is everyone's responsibility in any organization (Fenton & Wolfe, 2004).

A recent Web-based study by Knapp et al. (2006, p. 53) surveyed 874 certified information system security professionals (CISSPs) from more than 40 nations. It selects and ranks the top ten issues related to information security facing organizations today from a list of twenty-five information security issues. This list came from a previous study conducted with 220 CISSPs carried out by Knapp et al. (2006). These issues illustrate the most difficult aspects with which information security professionals are regularly addressing. Most of these aspects are of a managerial nature to support the organization to address information security. The top ten ranked issues are shown below in Table 4-1.

Table 4-1 Issue Ranking Results (Knapp et al., 2006, p. 53).

Bjorck (2001) presents the findings of an empirical study of information security consultants' experiences and insights relating to the implementation and certification of information security management systems (ISMS). This investigation used open-ended questions such as "*In your opinion, which are the critical success factors for a successful implementation of an information security management system, ISMS? (Please give reasons for your answer)*". In total eighteen information security consultants participated and qualitative analysis of data was conducted using a grounded theory methodology. Some critical success factors for the implementation and certification of ISMS were defined. The information security consultants' suggested six categories:

- **Project management capability**: an efficient project management capability is essential for successful implementation of an ISMS and needs active project members, a suitable project organization and realistic time plan.
- **Commanding capability**: the commanding capability empowers the role of top management by defining and supporting the information security all through management’s awareness and participation in information security.
- **Financial capability**: locating the required resources in order to estimate cost realistically.
- **Analytic capability**: this feature focuses on the importance of analytical capability in order to improve ISMS by balanced policy grounded in reality.
- **Communicative capability**: the communication process is important between those responsible for information security in the project and other parties.

- **Executive capability**: developing information security policy is vital but it will be useless if these policies are not put into practice.

Kankanhalli et al. (2003) develops an integrative model of information system security effectiveness based on deterrent and preventive efforts. Deterrent efforts are to discourage employees from criminal behaviour through fear of sanctions and preventive efforts are to discourage employees from criminal behaviour through control efforts. This study targeted 164 information system managers from various sectors of the economy in Singapore; only 63 of them took part in the survey to determine the ability of these measures to protect against unauthorized or deliberate misuse of information assets by employees. Kankanhalli's model, as explained below in Figure 4-1 integrates three organizational factors: organization size, top management support and industry type. It is suggested that organization size influences the information security system as bigger organizations deploy more deterrent efforts than smaller organizations. Top management support played a crucial role in allocating the resources to deploy advanced security software and encourage positive employee attitude towards the use of security policy. Finally, the industry type determines the level of prevention efforts.

Figure 4-1 Model of Information Security Effectiveness (Kankanhalli et al., 2003, p. 143).

Torres et al. (2006) identify 12 critical success factors from the literature on information security. These success factors have been grouped in the "Swiss cheese" model developed by Reason (1997). This was initially developed in the field of safety. It models the layers of defences to keep incidents from happening. Holes in the cheese denote the equipment failures, policy failures or human errors, which must line up for an accident to occur. The layers of the cheese are not static but change over time. Each slice of the cheese stands for a barrier or resistance to protect the system. The Swiss cheese model illustrates how the holes in the defence layer can cause incidents when these holes line up.

Figure 4-2 Critical Success Factors Arrangement Using Reason’s Swiss Cheese Model

(Torres et al., 2006, p. 533).

Reason's (1997) approach uses the three-dimensional cheese model where the cheese slices are defined as layers of security. Torres, et al. (2006) modifies this approach to use security controls for each dimension of the cheese where each control consists of some critical success factors, as shown above in Figure 4-2. The security controls are the basic elements of security.

Based on the Reason (1997) approach the following Figure 4-3 shows how the holes in the defence layers can sometimes line up to allow threats to pass through and cause accident.

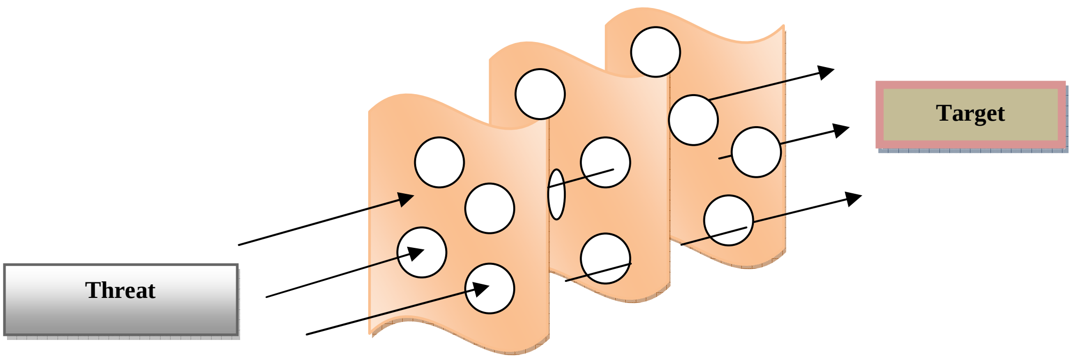


Figure 4-3 How Threats can Cause Accidents.

Bishop (2003) clarifies (as discussed earlier) what the technical components, the formal components and informal components are.

- Technical Component: tools such as hardware and software to prevent the illegitimate access to organization system.
- Formal Controls: the policies, regulations and procedures to explain the need of information security where it describes the roles and responsibilities.
- Informal Component: the mechanisms that are used to enforce the policies.

All of the above discussed models and theories consider information security differently. Some look at information security as a project in organization and investigate the importance of these factors to implement such projects Bjorck (2001). Kankanhalli et al. (2003) develops a model to demonstrate information system security based on deterrent and preventive efforts. Torres et al. (2006) define some success factors based on current information security literature, security experts' perspectives and ongoing projects.

This research study is different because it explores what organizations need to consider when implementing information security. The researcher wants to learn these aspects from people who are inside the organization and who are practicing information security on a daily basis, some as part of their work. This research is looking at the holistic picture of information security and this will help organizations to identify their requirements to implement information security successfully.

The next section will describe the methodology of this research study.

4.2 Methodology

This research is part of a wider research project for government organizations in Oman implementing information security. The study is based on an exploratory approach using a semi-structured qualitative interview method for collecting data and grounded theory to analyze the data. The interview was conducted in English language for the IT & security experts as well as the end-users. The work was conducted from June 2006 until July 2006.

The aim is to explore and identify factors affecting the implementation of information security in government organizations in Oman. Furthermore, the study looked at success factors from the experts’ perspective. It also looked at what concerns end-users have about information security. Due to the sensitive nature of information security, a determined sampling was selected for this study (Cohen et al., 2007; and Kvale, 1996).

Currently there are approximately fifty-two government organizations in Oman (Omanet, April 2006). The selected samples for the semi-structured interviews were a mix representing a cross-section of ten IT & information security experts and ten end-user employees. Almost one-hour was allowed for the IT & information security experts and thirty minutes for the end-user employees. The Information technology authority (ITA) in Oman was contacted and they provided the researcher with a list of ten experts and ten end users from different Omani government organizations. ‘End-user’ here refers to an employee who is using a computer for certain work-related purposes and is familiar with information security policy and guidelines. Experts and end-users selected for the interviews were a mix representing a cross-section of the population of approximately sixteen government organizations. All the experts are at a senior level of information technology or information security in their organization with not less than five years experience in the field of information technology. The end-users are from different departments from different organizations, all of them with a generally high level of education at graduate level and above.

Below are descriptive statistics of experts and end-user job titles and years of experience with information security.

Experts	**End-Users**
Job Title / Years of Experience	**Job Title / Years of Experience**
1. Head of IT / 5	
2. Director of IT /12	**1. Director of expenditure / 2**
3. Director General of Planning and IT / 13	**2. Microbiologist / 2**
4. Information Technology Authority Member / 8	**3. Secretary / 3**
5. Associated Director of IT / 10	**4. Finance employee / 4**
6. System Analyst and IT manager / 7	**5. Engineer / 2**
7. Head of Computer Centre / 12	**6. Head of Information & Media / 3**
8. Head of Section of Operation and Network / 5	**7. Head of Science Department / 2**
9. Information Technology Director / 14	**8. Human Resource Employee / 4**
10. Head of Networking / 9	**9. Lab Technician / 2**
	10. Admin Employee / 2

Table 4-2 Descriptive Details of the Participants.

The problem with this sample could be that it is slightly biased because of the selecting method by the ITA but to meet the aim of the study such selections should be considered in the interpretation of the results. Albrechtsen (2007) carried out two interview studies of users in a service center at a Norwegian IT-company and in a department of customer counselling at a Norwegian bank. A total of eighteen interviews were conducted, nine interviews in each of the studied companies. The aim of his study is to interpret some users' experiences of information security.

This research is an initial investigation, needed to get some initial information on the subject and therefore there is no assurance that employee responses revealed their real views but their responses may have been positively skewed in the direction of trying to please the investigator or reveal positive attitudes.

The interviews were arranged at the convenience of all interviewees and held in their own offices. A written description of the objective of the research study was provided, in which participants were advised of the ethical considerations, such as confidentiality of data. Additionally, they could choose to decline to take part, or to have the interview recorded. All participants requested that neither they, nor their organisation, be named. The decision to ask the researcher not to mention their details was not surprising because of the sensitive nature of information security (Doherty & Fulford, 2005).

Two sets of semi-structured interview questionnaires were developed, one for the experts and one for the end-user employees. A copy of the two sets of interview questions is included in Appendix A (p. 233-237). The questions were of an open-ended type to encourage the respondents to explore their own experiences, success factors and measures undertaken for information security. The questions of the semi-structured interviews were validated as explained in the previously in section 3.6.

The following section will give a detailed description of the findings of the research and a subsequent discussion.

4.3 Research Analysis and Discussion

The semi-structured interview questionnaire was based around the five areas in information security in an organization for the IT & security experts, established from the literature review phase:

- **Organization Security Mechanisms**: focus on the mechanism of security the organization is using to give an idea of how the organization is prepared for information security; how organizations are planning information security; and how organizations manage information security.

- **Information Security Policy**: the information security policy that discussing in this research is at employee-level and known as the acceptable use policy (AUP). This section is concerned with discovering if organizations document security policies or not; whether employees know about these security policy; how organizations develop organization security; if any employees are involved in the development of the security policy; whether the organization give any training in policy to their employees; how organization enforce the policy; and whether organizations review their policies.
- **Types of Threats that Occurs in the Organization**: focused on if an organization is facing any security threats and what types of threats the organization is experiencing.
- **Success Factors of Information Security**: concerning what the aspects are that might help an organization to have an effective information security.
- **Different Practices of Information Security in the Organization**: what are the practices of information security that the organization is applying and what steps the organization are taking to reduce threats.

There are also three areas that concern end-user employees:

- **Organization Security Mechanisms**: this part focuses on employees' familiarity with the organization’s security mechanism; e.g. are they satisfied with their organization's security technology?
- **Information Security Policy**: trying to know if employees are aware of an organization’s security policy; do they understand this policy; do they get any training on the security policy; and are they aware of the purpose of the policy.
- **Different Practices of Information Security in the Organization**: trying to know if employees are taking part in improving their organization's security policy; and what is their concerns about their organization's information security.

Many questions were developed around these themes to explore the above-mentioned areas and all are included in Appendix A. The qualitative responses are supported by verbatim quotes from the interviews. The IT & security experts and the end-user employee responses are presented. The data was saved in text format. It was examined for keywords, themes, categories and issues and then quotes were used to directly illustrate each of these main findings or points.

4.3.1 Organization Security Mechanisms

Findings from the interviews show that all of the experts in IT and security reveal that the information security objectives, i.e. the confidentiality, integrity and availability of the information, are available in their organization. As explained in one quote,

"*We do protection according to the access rights of the users, not everyone sees the data because the director of each department specifies, in writing, what kind of the privileges his staff get*".

Also another expert said:

"*We use a solid security system, the hashing technology that helps the integrity of the data, we limit access to sensitive data to few people, and we also do a daily backup*".

The interviews also show that the principles applied to each organization differ depending on the perception of the needs of the organization, as well as its type. In other words the level of security needed to achieve confidentiality, integrity and availability of the information will vary from one organization to another, because each organization has its own security goals and requirements (Bishop, 2003).

All the organizations use access control mechanisms with identification, authentication and authorization processes applied to the entire organization's employees. This was described from the experts as well as the end-users. One expert commented,

"*Nobody can log into our system without permission, employees have a user name and password and if there is a new employee we get a request letter from his or her head of department for a user name and password, also with what rights they require*".

This shows that employees can not use an organization's system unless they are authorized. Even if there is a visitor they have to be authorized to use the organization's system as described,

"*…based on our organization setup every employee must be authorized and authenticated, even visitors can not use computers without authentication*".

Also from the interviews, it was observed that most of the end-users feel some doubt as to whether someone can access their work information or even their personal information. For example, one respondent commented, "*I am not sure about it but from what I see there is a chance for the information to be seen either as a printed copy or through the network*".

At the same time some of them do understand that they have to be careful and apply some protection while they are working on something private or sensitive, as explained by another end-user employee:

"*I use the minimum precautions, like when I am working on something private for work and see someone is coming, I minimize the screen, also we have to lock the PC when we are not around the workstation*" or *"… saving all the data that is not supposed to be accessed by colleagues in my personal computer or private memory space and not storing such data in any public space or shared drive*".

These employees are behaving in the above ways perhaps because of the job type they are handling, but what about other employees? One of the end-users said,

"*I do understand what the purpose of information security is but there are many employees who do not understand and I can not blame them because of their limited knowledge of technology and related problems to information security*".

Another user described commented that,

"*I wish that my organization worked on teaching us how we should use the technology in a proper way so no-one can misuse or damage the system. For example, we do have good software but sometimes it is not working and this software is required by me to do my work. We do not have anyone trained and they bring people from outside to come and fix it and sometimes we wait for weeks to work again and use it*".

4.3.2 Information Security Policy

The information security policy that discussed in this research is at the employee-level, known as the acceptable use policy (AUP). The results show that only one organization in the sample has a documented information security policy. This organization implemented information security more than ten years previously. The remaining organizations have informal information security policies but they are not documented or written. As described by some experts,

"*We have a policy and we are working to produce a documented policy for users, IT and networking for all of the organization*" and "*Yes we have an internal security policy, but* *we are aiming to implement the international standards but we do not have a written one*".

Because the policy is not documented the employees of their organization do not have a copy of it, as explained by some end-users:

"*… we do not have a printed copy and they are working on having a printed one soon*".

Most of the experts explained that when they said they have an information security policy in their organization, although undocumented, what they mean is that they have a form of orders and instructions issued from time to time for the employees to follow.

"*What we do is issue orders to staff but none of these orders are documented…*" says one of the experts.

However a question still remains as to why they do not currently have their security policy documented.

One of the end-users explained that the reason for not having a documented policy is that the management does not feel it is important if they know how to properly use the computers and networks of the organization and commented

"*…unfortunately they do not provide us with a copy, that's why it is an ambiguous situation. Until now we did not hear of any serious problems which might damage the reputation of the organization and maybe that is the reason the organization does not feel that we need to know how to make proper use of the computer and the network*".

On the other hand many of the end-users think the effort that the organization makes is not enough in terms of using their systems properly and knowing their responsibilities regarding their work. One commented,

"*… it is a small effort [but] I think they need to make more effort in enforcing the policy. In a way they should have a written policy [for] every one, to know how to use the network and to tell us who is responsible for what*".

Employees feel their organizations are not serious in enforcing policies by having a documented policy, moreover the may seem not serious because of the gap between management and information security concerns (Siponen, 2001).

Other reasons may be related to a regulatory source; one expert described that there was a need for one:

"In Oman we should have a governance body and this accord now with the decree of His Majesty to have an Information Technology Authority in the country. This will help to have a regulatory source".

Another expert feels that information security importance is not yet measurable in Oman, they commented:

"*I wish if there was a case that an organization closed because of an information security problem, this would help to give weight to information security and would help to support our work when crises happen... we try to prevent*".

The reason could be the lack of legislation in the country and also organizations will not show any security problem to the public because, in the end, it is the reputation of the organization that they care about (Cooper, 1984).

One of the experts who has been working with information security for more that ten years believes that having a security department separate from the IT department is helpful for the organization to implement information security, they comment:

"*Information security is an important area and* I *believe an organization should ensure that there is a policy drafted, studied, endured and enforced; also information security should always be independent from IT and must report to the highest level of the organization*".

However, the end-users were divided in opinion. Some did not feel that the current security policy is sufficient for protecting the information they deal with as part of their work or their personal information held by the organization; others disagree with this opinion. One of end-users linked the sufficiency of the policy to the number of problems they have in the organization,

"*The current policy is quite sufficient because so far we have not found any problem regarding our personal information in the system* ".

Among all the selected samples only one organization reviewed its information security policy regularly. When updating organization security policy activity is not advisable, according to Briney (2000), reviewing organization security policy regularly may help the organization to strength its controls in protecting their assets.

4.3.2.1 Advantages of Information Security Policy

The interviews showed some advantages for using an information security policy in organizations. Figure 4-4 summarized the findings.

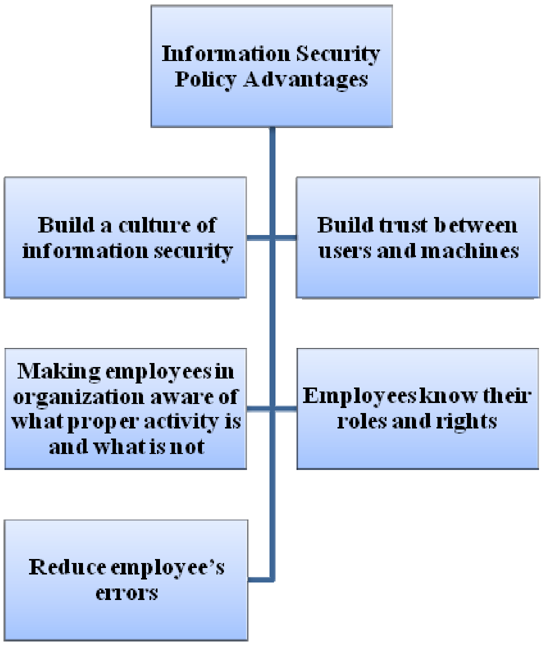

Information Security Policy Advantages
Build a culture of information security
Build trust between users and machines
Making employees in organization aware of what proper activity is and what is not
Employees know their roles and rights
Reduce employee's errors

Figure 4-4 The Advantages of Information Security Policy.

The results show that having an information security policy will create a security culture in the organization. As one of the experts stressed,

"*To create a system, not the people, and what I mean by the system is the general system of the organization*".

Other experts said

"*... people come and go that's why having a system is important*".

This point of view was also pointed out by one of the end-users,

"*Of course by having such a policy it will remain in the organization regardless of the users of that system*".

This issue is also discussed by Martins & Eloff (2001) in that the benefit of an information security policy is to build a culture of information security in the organization.

Most of the experts disclosed that their organizations are working on having a documented policy. As explained by one of the experts,

"… all these policies are scattered around, not documented, but we are in the process of having it as an official document. This way will make the users and IT people aware of what kind of practices they make in the organization".

Another expert referred to having a written policy in order to make policy clear to the employee so that they will know their roles and rights:

"*When we have an official policy, everybody will know their roles and parts as well as the consequences of not following the rules*".

Hone & Eloff, (2002) argue that formal information security policy will make employees aware of what practices are acceptable or not. The end-users share the experts' opinion that the policy will make them aware of the rules and regulations, one explains,

"*Indeed if things are clear to us we know our rights and we know what to do and what not to do and this will make us follow the rules and the policy*".

All of the experts commented that having a policy in the organization will minimize the employees' errors and will create a good immunity to the organization from inside:

"… security policy will help to reduce human mistakes and if we are ready from inside it is a great defense for any organization". Another expert believed that the policy would, "*build trust between users because users feel there is no privacy with IT department*".

Also,

"*to improve security to make users responsible for the use of the system*" as well as *"… protect the data from being exposed to the wrong people*".

Another said that their is,

"*…trust between user and the machine; no one can take us hostage. At the end I want the user to be happy to use the system, I do not want him to go back to using pen and paper*".

4.3.2.2 Process of Designing Information Security Policy

The interviews reveal that only two organizations did a study aimed at having the implementation of information security ready in their organization. The study covered the implementation of information security around the world as well as in the local environment as outlined below:

"*We told our staff that a study is going on in the organization and then a questionnaire was distributed and there was discussion with some key people in the department. We found what we want and where we want to go. Based on that information we started to work with the policy*".

This organization is in the process of having a documented policy.

An expert from the same organization said, "*The results opened our eyes*" and another expert described it as a "*road map*".

At the same time one of the experts emphasized that the organization should adapt the results of the study to its needs, saying,

"*We never do things without a study but we can not implement the whole recommendations in our organization because their services are different, but we learn from them and from their experiences and try to modify according to our need*".

This organization already has a documented policy.

The interviews show that some of the organizations have an internal audit department and usually the function of this department is, as explained by one of the experts

"*…to make sure the employees understand the good practices of using the computers, internet and the network of the organization*".

But this contradicts what the end users explained earlier in section 4.3.1 about the problem with not understanding and using technology properly and not harming the organization's system.

The experts described the situation as being that each organization consists of a group of employees from different departments performing in a team, depending on the organization's views and beliefs as to who should be involved on that team. Some see the team involving the IT department and security department or some depend totally on consultants or involvement of different departments for the benefit of the organization. This is described by one of the experts:

"*We have three types of people involved in the information security policy, these are: visionaries who see security in the future, designers (IT and security) of this vision, [answering]how can this vision happen, and implementers (network department, service department and development department and then security and standards department), [they] will check and make sure they implement the policy*".

Many of the experts agreed that formulating the security policy should be handled by the same team which is handling the development of the security policy. One of the experts explained that it was not advisable to include employees from different departments; he referred to the reasons as "*… a lot of employees do not understand information security.*"

However, some of the end-users do see it as important to have different departments involved in setting up the information security policy, as described by one of the end-users:

"*Different sections such as administration, IT, finance etc... All of them will come up with an accurate security policy which helps the organization as a whole or they may add some procedures in the security system itself which can be used to perfect security policy rather than having one single perspective which might not be knowledgeable*".

Experts believed that working with a consultant on developing the information security policy in the organization is helpful but at the same time it has to be teamwork, as one describes:

" *...we are planning to have a consultant to do it for us, but in my opinion who has to run our security policy in the organization is us, that's why I do not like to depend totally on the consultant, it should be teamwork*".

But one of the experts (whose organization is in the process to have a documented security policy) who has experienced the use of a consultant described his experience as:

"*I realize that a consultant is not better than us because he has standards but not experience*".

4.3.3 Types of Threats that Occur in the Organization

The interviews revealed that the type of incidents that all the organizations are facing involve their own users, known as insider threat damage. They did not mention any incidents arising from outsider threats. As described by one expert:

"*yes we faced some incidents, there have been attempts at sabotage by our users, our employees sabotage us*" .

Katz (2005) clarifies that employees are the biggest threat to information security. The reason for not having any serious outsider threats is not that organisations ignore outsider threats; it is primarily that they do not feel it is so important. As one of the users said,

"*…[there is] no outsider threats because of the VPN, our organization is not linked to the internet and hardly anyone can have access from outside.”* Another expert said, "*From* o*utsiders we [have] not faced any hacking attacks, the only thing we face is viruses and spam*".

The viruses and spam may occur when employees open spam emails or attached files that have viruses that affect the organization's system.

Some experts shared stories of various incidents:

"*One user wanted a promotion and when he did not get it, he deleted the data-base of the organization and said that the system crashed but we found that he had made it happen. He made mistakes and he was not that smart so it was easy to know [he had done it]*".

"*…others used to write nasty letters to certain people but we could not find the user because people save their password and others use it*".

"*…we had some group of students who hacked our system, by using some software that was available from the net. They were practicing through our system, what they were capable to do is only changing users ID by adding or deleting. Fortunately we noticed the problem before it got bigger*".

Many of the experts explained that the way to handle any vulnerability or threat in their organization is to fix problems as they arise. As one experts explained,

"*if we notice a problem in our system we raise it in our regular meeting and then we take permission from our boss for implementation*".

Another said:

"*We are reviewing incidents ad hoc, it is not procedural…*" and "*… when we notice an incident we discuss it in our meeting then take some action and then incorporate it into policy*".

Siponen (2001) indicates that in terms of security, organizations usually do nothing as long as nothing goes wrong, but when things do go wrong, they suddenly pay attention and a lot of effort is required to recover from the situation, where sometimes the recovery is not useful.

Experts mentioned that their employees showed some resistance when applying some policies (in the form or orders, not a documented policy) commenting,

"*when you do something to reduce the freedom of employees they won't like it…*"

It can be argued here this could be normal with most of the organizations in this research who do not have a formal security policy. At the same time all of the end-users show concerns that they must conform to the organization security policy and obey all the instructions, if they exist.

To avoid this resistance, some efforts must be made. The experts explained some ways to handle this matter:

"*…we are working to make them understand the purpose of the policy.*" In addition, "*after awareness comes employees will understand the purpose of the policy and apply it, but we always have to remember that in order to keep the implementation successful we should have a non-stop awareness program*".

This agrees with Siponen (2001, p. 26), that without a proper awareness programme employees may misuse or misunderstand many security issues in the organization: “without an adequate level of awareness, many security techniques are liable to be misused or misinterpreted by their users”.

Sometimes there is a breakdown of rules and this happens because users trust their colleagues, as one of the end-users explains:

"*… we are human beings, we have something called trust so sometimes we break the rules because we trust a colleague or a friend.*”

But according to Furnell & Dowland (2000) this is described as an abuse of privileges where the misuse is the consequence of actions by the employees. To understand why rules are broken is required. There are some well known research issues with rules, such as: the no applicable rule where employees do not know what rules apply (Lawton, 1998); rules are applied but do not seem a good idea (Mascini, 2005); and rules contradict each other Ortalo (1998). Further details about this matter are explained in detail in Chapter Six.

4.3.4 Different Practices of Information Security in the Organization

In the interviews, all the experts explained some ways of handling security threats and also making sure that they will not happen again, or at least are reduced:

"*we always try to educate them and all employees must be sent to security awareness training*" (this comment is from the organization which has a documented security policy)

Another comment was that,

"*There is sharing of passwords but we always restrict it in a way that you can not log in from any machine except your machine and we do this by having applications to monitor [this]*."

Moreover, another response was,

"*We are trying to change the habits of the employees here especially in the security issue*".

Also, some experts shared some of the ways that they use in their organization in order to reduce or stop the threats. For example, if employees do not follow policies they deactivate some of the services such as using the internet or the email service. Some others put personal information about the user in his or her outlook mail service and this will stop the sharing of passwords. Such practice from the organization is described as the deterrent effort that Kankanhalli et al. (2003) explain, i.e. that organizations discourage employee’s bad security behavior through fear of sanctions.

Many of the experts believe that the feedback on security in the organizations is a helpful procedure and if used will be a good practice in the organization for the implementation of information security, as one of the experts described:

"*We are in a process to have a feedback system; this will define a continuous feedback [and] will support our monitoring and implementation and then for the good feedback [there] will be an immediate response. And this also will be used to enhance standards and policies and measuring procedures... this feedback should be given to the security management to apply*".

The interviews show some benefits from having the feedback process in an organization. Figure 4-5 summarizes the findings below.

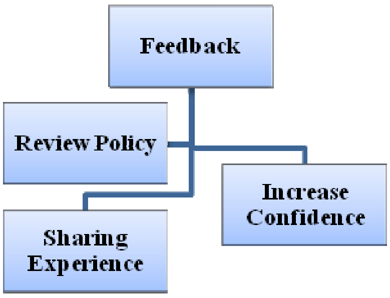


Figure 4-5 Benefits of Feedback in Organization.

Feedback is a way of helping the organization in reviewing policy, as explained by one of the experts:

"*it will be nice to get feedback, but the feedback sometimes becomes an obstacle when employees give ineffective feedback because they want everything easy for them. We check it first and if it is good feedback we will consider it for reviewing the current policy but, if not, employees must understand they have to follow the policy*".

Feedback availability may help to increase the confidence between the employees of the organization and the people who are in charge of security, as well as the IT employees, as illustrated by one of the experts:

"*… continuous interaction between [the] information security department and [the] IT department and also between information security and users, will increase confidence, so they feel free to talk to them*".

The interviews show that the majority of the end-users never provide feedback about security matters in the organization. Another end-user believe it is good for the user to be involved and share his experiences, commenting

"*By sharing my own experience in terms of the difficulties I am facing with the current security and giving my suggestions to improve the security within the organization*".

There is more about how organizations encourage their employees to provide feedback about information security in Chapter Six.

Many of the experts described that the feedback they get from their users is usually in the form of complaining about why they cannot get a certain service or why they have a restriction on using the internet, and so forth. One of the experts explained the reason for ineffective feedback as being that,

"*Some of the employees do not have a clear concept of the importance of such policies and [that] is clear from the type of complaint we receive*".

This may reveal problems in the way management communicate with their employees and also the difficulty of not having a documented security policy.

The next section covers the aspects that the experts believe are important to address information security successfully.

4.3.5 Success Factors of Information Security

From the answers of the experts, different success factors were distinguished. These success factors are presented below in the following Figure 4-6.

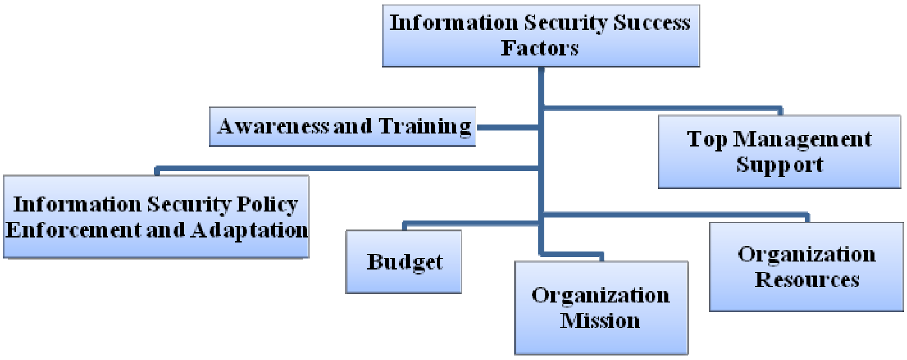


Figure 4-6 Information Security Success Factors.

Each of these factors is explained below.

4.3.5.1 Awareness and Training

The interviews show that organizations wished to secure their information. However, they believed that information security would be achieved simply by increasing awareness and providing training. One of the experts commented:

"*The problem that we faced seven years ago was IT awareness, the awareness of security was zero, a lot of people thought that all they needed to be protected was to have a login name and password, and then we worked on training our employees to raise the awareness to make the implementation of security easy".*

Furthermore, they stressed that information security would need a continuous and ongoing awareness and training programme for employees to deal with the ever-changing security arena. Dhillon (1999) argues that organizations must have ongoing education and training programs to achieve the required outcome from the implementation of an information security policy. However, there is no evidence in the literature that awareness programs play any decisive role in reducing insecure behaviour or that it makes a difference in ensuring information security and in increasing compliance to information security policies.

When there is no documented information security policy it may have an effect on the awareness of the employees and this was clear from one of the expert's point of view:

"In t*echnology we do not have problem, we are suffering from our employees and we are working on it through increasing their level of awareness. Also, if there is a clear and written policy employees will know of course what is proper and what is not proper*".

For example, common practices are employees leaving machines logged on while out for breaks; recording passwords on sticky notes on the computer's monitor; or revealing confidential information to unauthorized people. The accepted wisdom is that there is a need to put effort into training and educating the employees because they are the ones who are going to need to comply with the information security mechanisms and norms. No matter how powerful the technical security underpinning of the system is, or how strong the regulations, or policies, there is still the possibility that they will be broken simply because someone subverts them. As it was explained before there could be many reasons for such problems, Chapter Six will give a broad picture of the reasons behind breaking organization rules.

One of the experts explained that the culture of the organization is an obstacle to an awareness program and to harvest the result of the awareness program will take time. They commented:

"*the obstacle is our culture, the environment, what is happening is a huge change. On one side we put procedures and regulations [but] at the same time people are not ready. But compared with four years back the situation is getting better and employees are understanding more*".

Another end-user explained the importance of training:

"*In security we face new things regularly, therefore training should be in parallel to any changes in the security field and I believe it is better to be prepared before any problems happen, to know how to solve it, and not wait to find out later how*".

4.3.5.2 Top Management Support

In all organizations, understanding and identifying the need for security comes from the IT department or the person in charge of information security. One of the experts said

"*the top management does not know everything, we have to explain to them and make them understand the need of security*".

This confirms what Fung & Jordan (2002) claimed - that management tends not to initiate measures to ensure the security of organizational information because generally they feel that the IT department is responsible for choosing the proper technologies, installing the required software, maintaining the technology in the organization and keeping the organization’s information secure.

The results show that all the experts agreed that in order to have a policy or any instruction regarding security, top management must take decisions and approve the policy before it is implemented in the organization. One expert stated

"*…when we notice any problem in our system, we try to issue some rules but before they are issued officially we submit them to management for approval and final decision*".

After senior management understands the need for the information security in the organization they approve the policy and then it is enforced throughout the organization by the relevant department of information security (which is the IT department, the security and audit department or the information security department). This was also clear from the end-users’ responses, who say that the

"*IT department circulate the rules through our Heads of Sections and then they distribute it to us*".

Experts explained the management effect in the implementation of information security. One of them commented that,

"*Top management? We can not do any thing without their authorization, they have to support us in implementing information security in the organization*". One expert stressed that "*…we have to understand [that] if the top management do not support or understand the need of information security, the implementation of information security will fail*". Also, another expert said "*… it is an important issue because if they believe in the importance of information security for the organization they will work on enforcing it and also the employees will take it serious*".

Top management must be convinced of the importance of information security in order to get a proper budget and enforcement. According to Hone & Eloff (2002), the behaviour and attitudes of employees towards information security starts correctly if their top management shows concern for it. Von Solms (1999) believes that the top management must be convinced of how important information security is in the organization in order to provide the sufficient budget, enforce the information security and for the employees to take it seriously. Also, one of the end-users commented

"*The management plays a major part in addressing and implementing the security policy and they need good people around them to advise them. There is no use having the latest technology if we do not know how to deal with it, therefore all of us need to be aware soon that we will be under the e-government umbrella to use it and to work with it correctly we need to be educated in a proper understanding of the needs of security"*.

4.3.5.3 Budget

The interviews revealed that all the experts identified budget as an important aspect of implementing information security in their organization. One expert commented on the budget that, "*One day my boss asked me 'are we protected?', I told him if you have a house and you want to protect it you will need money to do so… so the level of security or the protection you will get depends on how much money you will spend. According to the budget we plan for information security*".

The budget needs to be adequate as explained by another expert:

"*Without enough money, we can not have security in the organization; money will bring software, hardware, and consultants*".

Without a proper budget, organizations will not be equipped with sufficient resources to ensure information security. Bjorck (2001) describes budget as the financial facility which firstly rationally estimates the costs and secondly assesses the access required to the resources to achieve successful implementation of information security. Usually organizations do not have specific budgets directly for information security as explained by one of the experts:

"*we do not have a budget for security, but we have it for IT, whatever we implement we make sure security is part of it*".

More future work is needed on how budget is determined for information security.

4.3.5.4 Information Security Policy Enforcement and Adaption

One of the experts explained,

"*The performance of the organization will be successful when we create a policy, get right implementation of the policy, acceptance from employees, and [then] stick to our rules and do not manipulate them*".

Many experts in the interviews agree that the policy should be straightforward, easy and clear, as commented:

"*it should be a straightforward policy and you should exclude any process not required, they should exclude any non-sequential reading of the policy*",

It is also important that the policy should be reviewed and updated frequently. One of the experts commented that

"*If we [can] not achieve the goals, [then] go back and review the policy again*".

Therefore reviewing and updating organization policy is advisable. Hone & Eloff (2002, p. 15) state that, "at the end of the day, an effective information security policy will directly result in effective information security". Canavan (2003) explains that enforcement of the information security policy is by putting it into practice. So when an organization puts an information security policy into practice, employees can follow the rules and know their rights and responsibilities (Hone & Eloff, 2002).

Policy effectiveness is relevant to everyone's job in the organization because everyone is affected by information security to some extent, as described by another expert:

"If you do not have rules and regulations [then] the misuse concept will vary and have different meanings. For example, if someone got an email and he forwarded this email and when you ask him why you did this he will say well no one told me that it is not proper behaviour. The success [is] that we all work together. We have to update and monitor, it is a continuous job, it is like a battle you have to be ready for it, you do not know when it [will] strike you".

Many of the experts mentioned that adaptation of the information security policy to the needs of the organization is important. One of the experts commented that

"*The information security required a lot of customization to fit our organization's culture*".

Each organization provides a different service, that is why they require an adaptation of the security policy, but the underlying principles should be the same:

"*In general terms the information security policy should be the same but the rest varies from place to place in terms of implementation. For example security differs from a tent to a house*".

A customized information security policy can reflect the culture of the organization. Barman (2001) argues that the content of the information security policies may vary from one organization to another but that all policies have some topics in common. The policy should be developed based on the security needs and business goals of the organization (McKay, 2003).

4.3.5.5 Organization Mission

Some of the experts said that clear goals and objectives are essential in implementing information security policies and that having a culture of secure information in the organization will affect its success. A statement from one of the experts illustrates this:

"*It is successful when understanding what we want to achieve [and] defining what we want to achieve by setting goals and objectives will support the information security implementation*". Also, "*what makes it not successful is when the users do not understand and believe the need for information security. In other words, incomplete culture change will reflect on the success on information security*".

McKay (2003) clarifies that if the organization's mission is not addressed, the organization will continue to struggle to secure its information. Employees will not take responsibility seriously and will not follow and respect the guidelines in the information security policy.

4.3.5.6 Organization Resources

One expert in the interview mentioned the organization’s resources as the base of information security in the organization:

"*Security software or IT technology within the organization is a part of the requirement to conduct information security which is a mandatory need...*”.

There are essential operating systems, applications and other technologies which are required to support the implementation of information security in the organization (Canavan, 2003). This factor is different from the budget factor because you need money to equip organization with the proper resources to defend organizational assets.

The next section will summarise the findings then follow-up with a discussion of the results.

4.4 Discussion

As it was discussed earlier in the introduction, information security effectiveness centred on three things as Bishop (2003) illustrates: requirements, policy and mechanisms to enforce policy. The results suggest that organizations are using security mechanisms to prevent any unauthorized access to their assets. The results showed that only one organization in the entire selected sample had a documented information security policy.

Therefore the findings also suggest that organizations need to be more proactive in producing a documented policy, available to all the staff in one document, not in the form of scattered orders distributed from time to time. The results suggest that organizations are facing a lack of proper interventions related to deploying information security through employees, as David (2002) highlights, having a policy is one thing and enforcing the policy and putting it into practice is another.

The interviews revealed that there is no legislation in Oman for information security and findings suggest that legislation for information security in Oman would enhance the implementation of information security in their organizations. Hare (2007) stresses that legislation has an impact on the organization in terms of forcing the organization to implement information security. This was clear from the end-users views that their organizations are not putting enough effort into making their employees implement information security properly through knowing their responsibilities about their organization’s assets. Most of the organizations in the interview never did any study before implementing information security.

The results also suggest that organizations are experiencing threats from their employees. This is in line with many other authors who argue that the biggest threat in an organization is the insider threat. Organizations' employees can cause information security delays through breaches to information security or errors that influence the organization's response to threats (Kotulic & Clark, 2004). Employee errors are sometimes related to the breakdown of their organization rules. This could be related to different reasons as was explained earlier. For example, they feel that these rules contradict each other, rules are hard to apply, or they are not aware of what rule applies (more about such reasons are explained in Chapter Six).

The results suggest there should be feedback mechanisms in the organization and also increased confidence between the employees and the IT department (or the department responsible for the security). However, the organizations do not appear to be implementing such practices. Feedback will help to review security policy and make employees share their experience regarding information security. As argued by Siponen (2000), feedback is a source of ongoing evaluation and improvement in the organization. McKay (2003) describes feedback as a facility where employees can share their concerns and feel comfortable in discussing security issues. Experts in the interview understood that the feedback mechanism was important in engaging employees in information security, while, on the contrary, employees never practiced feedback about security matters.

End-users from the interviews feel that setting up an organizational security policy needs different sections’ or departments’ involvement. They believe that each of them know what kind of security they require. The interviews suggest that having a security department separate from the IT department is helpful for the implementation of information security in organizations. End-users explained the reason for not having a documented policy in their organization was that the management did not feel it was important. There were concerns about their level of awareness about how to implement information security properly.

Among the findings, the results suggest many factors organizations should consider to implement information security successfully. The following are the most sensible aspects that promote good implementation of information security. These success factors were derived from the opinions of the experts in IT and information security. There is a chance that in giving these answers they do not want to be seen as complacent.

Awareness and Training

The results suggest that organizations need to apply training and awareness programs. According to the interviews, training and awareness programs will enhance the implementation of information security and make the implementation of security easier. This might help employees to practice information security properly and reduce the number of errors they make (Siponen, 2000). As a result when an organization institutes awareness programs employees might help to change their behaviour from security vulnerable to a more defensive element against security breaches. Organizations should therefore not underestimate the importance of information security awareness training (McCoy & Fowler, 2004).

Training and awareness programs can be employed for employees at all levels in the organization with the consideration of the job type or the environment they work or deal with. For example, awareness training for managers will vary from other employees in the IT department and so forth. There is no evidence in the literature that training and awareness programs will help to reduce employees' errors, but at the current time it is the only tool in our arsenal and it is possible that it will do some good.

Top Management Support

The interviews suggest that top management support is important for the implementation of information security. The results reveal that when the top management believe that information security is important they will approve the proper budget for information security and enforce information security where employees will take security in an organization seriously. Hone & Eloff (2002) explain that the behaviour and attitudes of employees towards information security will be more in line with secure behaviour if top management demonstrates concern, therefore it is suggested that the tone of security is set by the attitudes of those at the top of the organization (Hinde, 2002).

According to Posthumus & von Solms (2004, p. 639), "*the support of top management is paramount to the success of an organization's information security efforts*". Management will not act to support the information security unless they can see that it supports the organization's core business function (Blake, 2000). Hence, they must be convinced of the importance of information security before they are willing to provide sufficient budget, and act to enforce the information security policy (von Solms, 1999). Fung & Jordan (2002) argue that the middle-up-top-down approach has the potential to be more effective than the top-down approach since they sell information security to top management. According to them top management work with information security on a project basis which requires a certain period of time and once it is finished they work on another project. The researcher recommends that both parties need to communicate properly to address and implement information security in an organization.

Budget

The results show organizations allocate budget to IT in general rather than specifically to information security. Budgets, as the interview reveals, buy software and hardware, allocate training and awareness programs, and set up policies in organizations. Organizations require adequate funding to achieve effective information security. "*Budgets generally depend on the manner in which individuals' investments translate to outcomes, but the impact of security investment often depends not only on the investor's own decisions but also on the decisions of others*" (Anderson & Moore, 2006, p. 612).

Lack of information about security budgeting in organizations leads to under-investment in appropriate controls (Dinnie, 1999). When it comes to technology, new products appear frequently and are sold as the security "silver bullet". This happens because the information security vendors and consultants naturally sell their latest products and services. What they do not mention is that the software often needs to be updated frequently in order to address the continuously changing and emerging threats. It is therefore challenging to meet Gordon and Loeb's maxim: "*From an economics perspective, firms should invest up to the point where the last dollar of information security investment yields a dollar of savings*" (Gordon & Loeb, 2006, p. 121). Organizations do not need to invest in expensive software or hardware to achieve an effective level of information security. What is required is a careful plan that ensures that the user behaves securely, and this cannot be achieved by the means of any new technology or software product. However, such training is expensive and, in turn, it is hard to demonstrate the efficacy, which makes it difficult, if not impossible, to demonstrate the return on investment that management needs in order to justify expenditure. Future work is needed on how budget is determined for information security.

Information Security Policy Enforcement and Adaptation

The interviews suggest that the benefit of an information security policy is to build a culture of information security; build trust between users and machines; make employees in an organization aware of what proper activity is and what is not; let employees know their roles and rights and help to reduce employee errors. Top management take decisions to approve the policy before it is implemented in the organization. The results reveal that adoption of the information security policy is needed for the organization to fit the organizational culture. The results suggest that information security policy should be reviewed and updated frequently and that the policy needs to be straight forward, easy to use; and clear to understand.

The benefit of information security policy is to make employees aware of whether practices are acceptable or not (Hone & Eloff, 2002). Madigan, et al. (2004, p. 48), clarifies that policy enforcement involves "*assuring that the policies are understood by all interested parties, regularly checking to see if the policies are being violated, and having well-defined procedure guidelines to deal with incidents of policy violation*". A security policy can mitigate some threats, such as viruses, and work towards preventing incidents caused by these threats from re-occurring (Hinde, 2003). The aim is to change the habits of employees in the organization.

The policy features are explained in Chapter 2, section 2.4.3. For example, when employees understand the policy and they can apply it with no problems, this sounds a clear policy and easy to use. There could be a subjective element that changes from one person to another. More about such matters are explained in Chapter Six.

Organization Mission

The results suggest information security objectives and goals need to be addressed properly and clearly in order to work in a stable environment, and one should not wait for crises to occur. This will happen when organizations put information security high on the agenda. Organizational missions need to be stated in organization security policy to help management take decisions related to information security (Barman, 2001). Moreover, the problems will increase when organizations do not recognize the danger to their information (Stocker, 2000) in cases when it could bring risk to organizational assets.

Organization Resources

The results suggest organizations need adequate hardware and software to enforce information security. Organization resources are the fundamental requirement to enforce and monitor the implementation of information security. Organizations that lack software or hardware will face difficulties in handling some security issues such as access control mechanisms or helping employees to apply good security practice, like automatic logoff or regular password changes. The budget brings resources into an organization.

From what has been discussed about the success factors the results reveal that the adoption of these factors is not high. The experts feel they are important but from employees concerns about awareness, management, and information security policy, it seems that organizations are not addressing these factors properly.

Finally, the literature suggests another factor related directly to employees of an organization, which is employee acceptance (Nijhof et al., 2003). When employees appreciate the need for information security they will aid good implementation. The interviews suggest many aspects to help achieve employee acceptance, such as the support of management through providing the appropriate training and awareness programs. Also, clear organization security policy could help employees to understand what is an acceptable activity and what is not. This all might lead to reduce employees' errors. More about this aspect is discussed in Chapter Six.

4.5 Conclusion

The results of the study cannot be generalized facts given the sample size, but shed light on the requirements for good information security implementation. What has been discovered from the study is that there are a number of factors which information security experts have identified as being essential if an organization wants to achieve an adequate level of information security. The results suggest that organizations must institute information security policies to prevent unauthorized access to their resources. Steps must be taken to ensure that employees get the required awareness and security training to make them aware of the security issues and the consequences of insecure behavior. Moreover, the results suggest the ethos of information security must come from the top of the organization to encourage a serious attitude from employees and an expectation that they will comply with the organization's security policy rules and regulations. Implementation of information security will not be possible if a sufficient budget is not allocated. Furthermore, it is recommended that clear organizational mission statements and goals result in positive employee behaviour and positive attitudes towards securing the organization’s information assets. The results suggest that the identified factors are connected and linked to each other and therefore it is difficult to prioritize one factor over another.

The study highlighted the requirements for good information security practices. At the same time the study raised an important question - do all employees know what information security policy is? Therefore, there is a need for follow-up studies using different methods or different tools to help organizations to understand what is required to improve the effectiveness of their information security policy.

While the whole issue of information security is under-developed in Oman, the outcome of this research will contribute to both governmental organizations and non-governmental organizations in terms of best practice in enhancing information security. As the research unfolds, it is expected that the findings will help organizations better understand and determine the steps that are needed to improve the organization’s information security.

The next chapter will present the results of a quantitative investigation conducted as a follow up to the work discussed in this chapter. This work will use organizational questionnaires to test some research question related to some of the interview results. The main research question this current study proposes is as follows:

- Do organizations with a documented security policy report fewer breaches than organizations with a non-documented policy? This suggests that a documented security policy in an organization helps to reduce threats. Therefore, it is reasonable to propose that organizations' having a documented policy may experience fewer reported levels of security breaches.
- Do organizations with greater adoption of ‘success factors’ also report fewer security breaches in their organization. The findings from the interviews identified possible success factors for information security (e.g. training and awareness program, top management, budget, etc…). Therefore, it seems reasonable to propose a relationship between the adoptions of success factors by organization and security breaches.
- Do organizations that report a greater adoption of success factors report a more effective security policy? This research interview identified success factors (e.g. training and awareness program, top management, budget, etc…) for information security. Therefore it seems reasonable to propose a relationship between the adoption of success factors by organizations and the reported effectiveness of the policy as described above. More adoption of success factors means the organization is practicing more successfully.

Chapter Five

Information Security Policy- Questionnaire, (Oman)

This chapter builds on the qualitative results of the previous chapters using a different research method. As explained in Chapter Two, the type of information security policy this research will focus on is at the employee-level, known as the acceptable use policy (AUP). The findings from Chapter Four suggest that organizations must institute information security policies to prevent unauthorized access to their resources. The findings also suggest that organizations need to be more proactive in producing a documented policy, where it is available to all the staff in one document and not in the form of scattered orders distributed from time to time. These findings suggest that it would be valuable to investigate information security policy within organizations in terms of its effectiveness in reducing security breaches. This was done using a questionnaire informed by the researcher and distributed by the ITA in Oman. The questionnaire was in English language and the ITA distributed these questionnaires to the IT department of all the governmental organizations in Oman. The work was conducted from mid-October 2006 until mid-November 2006.

This chapter is organized as follows. The following section presents the methodology for the research study. Section 5.2 presents the results of the analysis. Section 5.3 articulates a discussion of the results. Finally, section 5.4 presents the conclusion of this chapter.

5.1 Research Methodology

Based on the literature review and the findings from Chapter Four, some aspects related to information security policy (AUP) need further investigation.

The objective of this study is to

- Investigate what makes an effective security policy.
- Investigate the effect of security policy in reducing security threats.

5.1.1 Questionnaire

After analyzing the outcomes from the semi-structured interviews in Chapter Four, a questionnaire was developed including some relevant questions from the Doherty & Fulford (2005) survey questionnaire and other questions identified from literature. The questionnaire is presented in full in Appendix B (p. 238-243). The motivation of the questionnaire was to determine:

- How many organizations have a documented information security policy?
- If not, why is the policy not documented?
- What is an effective security policy?
- What are the different types of threats faced by an organization?
- Have the fundamental success factors (top management support, budget, information security policy enforcement and adaptation, organization mission and organization resources) been adopted by the organization?
- How successful does the organization believe that their information security policy has been in adopting each of these criteria? (e.g. explain what is an acceptable activity and what is not, state the purpose of the policy and the scope of the organization, etc…).
- What are the different issues (e.g. user login responsibilities, use of organization system & network, internet access …etc) the organization faces in implementing their security policy?

The quantitative questionnaire was divided into five sections and included a total of 22 questions. These required tick boxes and, in some cases, brief written answers.

Section A: Question 1 and 2 request a description of the organization

Section B: Question 3 asks the respondents to report on any breach and the severity of each breach that their organization has experienced in the past two years. The number of breaches were requested as a six-point ordinal scale (0; <5; 5-10; >10; >100; >1000). The severity of breaches was measured using a five–point Likert scale.

Section C: Questions 4 to 20 ask for information about the security policy in the organization; if the organization has a documented security policy and, if not, requests the reasons for not having a documented policy. Questions concern the issues that the policy covers in each organization. Also, it is asked how the organization checks the compliance of their employees with security policies.

Section D: Question 21 evaluates the importance of the derived success factors to information security from the semi-structured interview and how successful the respondents believe their organization has been in adopting each of these factors. Both issues were measured using a five –point Likert scale.

Section E: Question 22 is aimed at organizations that have a documented information security policy. Respondents were asked to evaluate the importance of security policy criteria derived from the literature and the semi-structured interview and how successful they believe that their security policy is in meeting each of these criteria. Both issues were measured using a five –point Likert scale.

5.1.2 Research Question

Based on the literature review and the findings from Chapter Four, it is possible to propose that a number of aspects of information security policy could have some impact on the effectiveness of the policy as well as the level of security breaches.

The researcher understand the limitation of this research in that the sensitive nature of information security might make the participants reluctant to say what they do or what they believe in this context. The number of security breaches that the organizations are experiencing is not exactly known. There is no evidence in the literature as to what an effective security policy is or what makes good security policy. Therefore this research is about *reported* attributes of security policy and *reported* effectiveness of security policy compared to *reported* frequency of security breaches.

Before the data was subjected to a rigorous statistical analysis some research questions were developed. These are described in the following sections.

Section A: Security Breaches

Figure 5-1 and Figure 5-2 show the different proposed research questions that the study will investigate with regards to reducing security breaches.

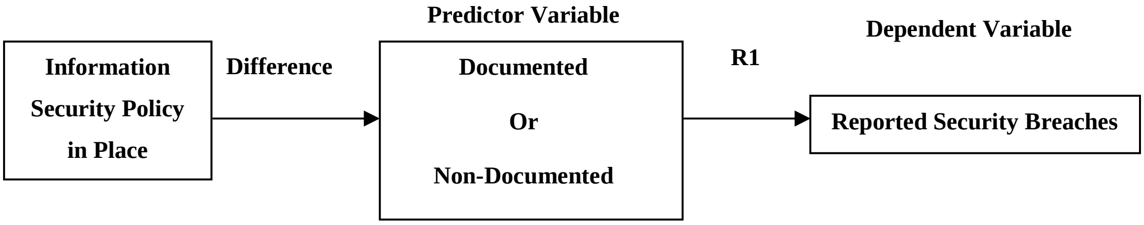


Figure 5-1 Is there any Difference between a Documented and Non-Documented Security Policy and the Reported Level of Security Breaches?

R1: Do organizations with a security policy report fewer breaches than organizations without security policy?

Authors such as Doherty & Fulford (2005); and von Solms & von Solms, (2004) highlight the strength of written policy in an organization in the protection of organizational assets and in reducing threats. Section 4.3.2.1 suggests that a documented security policy in an organization will help to reduce threats. Therefore it is reasonable to propose that organizations that have a documented policy (or not) may differ in their reported level of breaches.

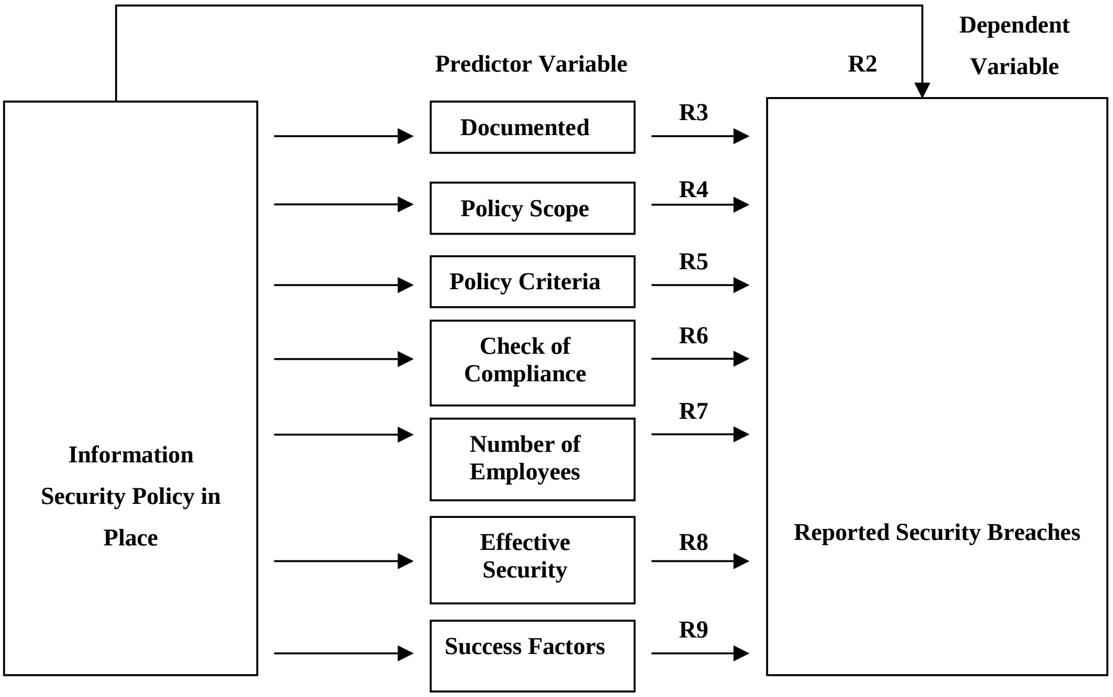


Figure 5-2 The Proposed Research Question with Regards to Reported Level of Security Breaches.

R2: Do organizations with a security policy report fewer security breaches?

The literature stressed (e.g. von Solms & von Solms, 2004; Adams et al., 1997) the importance of an information security policy in reducing security breaches as was discussed in Section 2.4. Therefore it is reasonable to propose the above relationship between security policy in an organization and the reported level of security breaches.

R3: Do organizations with a documented security policy experience fewer reported security breaches?

As explained in R1, on the importance of a documented security policy in an organization, it is reasonable to propose the above relationship between the documented security policy and the reported level of security breaches.

R4: Do organizations with a policy with a broader scope experience fewer reported security breaches?

Literature stresses what elements should be in a security policy. As described earlier in Chapter Two in section 2.5.4, Doherty & Fulford (2005) state that there is not much information in literature which can explain clearly how a policy with a broad scope (e.g. user login responsibilities, use of organization system & network, etc…) could reduce threats. Therefore, it sounds reasonable to propose the above relationship between the wide scope of organization security policy and the experience of reported security breaches.

R5: Do organizations with more adoption of security policy criteria experience fewer reported security breaches in their organization?

Chapter Four indicated that organizations need security policies to illustrate to staff what they are allowed to use the systems for, what is good behavior or not, and what will happen if they did not comply with the policy. It is reasonable to propose the above relation between the adoptions of different criteria (e.g. explain what is acceptable activity and what is not, state the purpose of the policy and the scope of the organization, etc…) and security breaches.

R6: Is there any difference in the number of reported security breaches between organizations reporting different levels of compliance from employees to the organization security policy?

It has been suggested that the number of breaches is related to non-compliance with security policies (Madigan et al., 2004). The consequence of this, as presented in the above research question, is that frequent checks of employee compliance to security policy will lead to a reported reduction in security breaches.

R7: Is there any difference in reported security breaches across a range of employee numbers?

Employees are often perceived to pose the greatest ‘wider threat’ for security. It sounds reasonable to propose the above relationship between the number of employees and reported security breaches in organization.

R8: Do organizations that report an effective security policy also report fewer security breaches?

As described in R1, the literature suggests that there is a link between security policy and security breaches. Also, it is not clear yet how to assess the effectiveness of the security policy. Findings from Chapter Four suggest that the effectiveness of the policy is related to the level of breaches. It is reasonable to propose the above research question that there is a relationship between the reported effectiveness of the policy and reported security breaches.

R9: Do organizations with greater adoption of ‘success factors’ also report fewer security breaches in their organization?

The findings in Chapter Four identified possible success factors for information security. Therefore it seems reasonable to propose a relationship between the adoption of success factors (e.g. organization setting clear goals and objectives of information security, implementation of information security with a consideration of organizational culture, etc…) by an organization and security breaches.

Section B: Effectiveness of the Security Policy.

Figure 5-3 and Figure 5-4 show the different proposed research questions that this study will investigate with regards to the reported effectiveness of security policy. Effectiveness of the policy is related to a good implementation of the guidelines of the policy. Other important factors include what should be protected and what restrictions should be put upon organizations using assets, which in the end leads to a more secure system (Barman, 2001). There is no evidence in the literature on how the effectiveness of a security policy is assessed. Therefore this study will propose the following research question to highlight what makes information security policy effective.

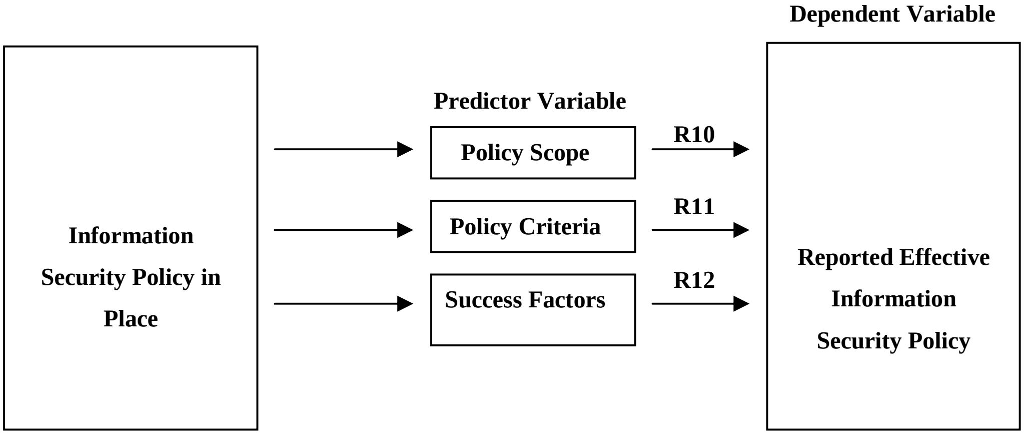


Figure 5-3 The Proposed Research Question with Regards to Reported Effective Information Security Policy.

R10: Do organizations with a broader security policy report a more effective information security policy?

Research question R2 proposes the relationship between the wide scope of factors (e.g. user login responsibilities, use of organization system & network, internet access, etc…) affecting organization security policy and the reported security breaches. It is reasonable to propose the above relationship between a wide scope of organization security policy and the reported effectiveness of the policy.

R11: Do organizations that report greater adoption of security policy criteria also report more effective security policy?

As it is described in R5, there is a proposed relationship between the criteria of security policy earlier (e.g. explain what is acceptable activity and what is not, state the purpose of the policy and the scope of the organization, etc…) and the reported security breaches. It is reasonable to propose the above relationship between adoptions of different criteria and the reported effectiveness of the policy.

R12: Do organizations that report a greater adoption of success factors report a more effective security policy?

As described in R9, there is a proposed relationship between the identified success factors (e.g. organization setting clear goals and objectives of information security, implementation of information security with a consideration of organizational culture, etc…) for information security and the reported security breaches. Therefore it seems reasonable to propose a relationship between the adoptions of success factors by organizations and the reported effectiveness of the policy as described above. More adoption of success factors means the more success factors the organizations are practicing.

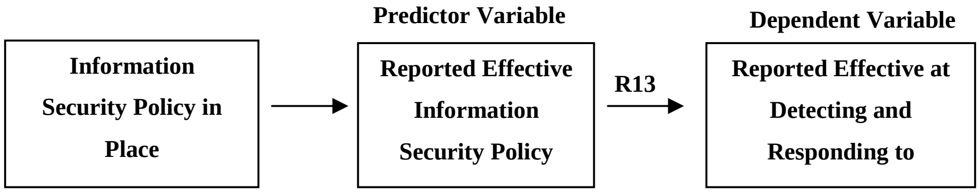

Predictor Variable
Dependent Variable
Information Security Policy in Place
Reported Effective Information Security Policy
R13
Reported Effective at Detecting and Responding to

Figure 5-4 The Proposed Research Question with Regards to Reported Effective at Detecting and Responding to Security Breaches.

R13: Is there any relationship between the reported effectiveness of the information security policy and the reported effectiveness at detecting and responding to information security breaches?

When organizations report that their security policy is effective the researcher assume that the organization will be effective in detecting and responding to security breaches. From all the above proposed research questions, it is reasonable to propose the above research question and to measure the relationship between the reported effectiveness of the policy and the reported effectiveness at detecting and responding to security breaches.

5.2 Research Findings

This section presents a detailed, descriptive analysis of the data concerning the application of information security policy in a number of government organizations. The findings will be presented according to each section of the questionnaire.

The questionnaire was distributed to 52 Omani governmental organizations in paper form to the IT department of the organization. The decision for choosing the IT department and not senior management is that the IT department, as shown in the findings of Chapter Four section 4.3.5.2, are responsible for security in their organization. The questionnaire was delivered and collected by hand. A month was given to complete the questionnaire. A total of 42 were received representing a response rate of 81%. This is a high response rate.

5.2.1 Background Information

Figure 5-5 below describes the number of employees in participant organizations. It can be observed that the biggest group in the sample has 1001-1500 employees, this is 26 percent of the whole sample (N=11). The two smallest groups in the sample are the organizations that have less than 500 employees and over 10000 employees which both represent 5 percent (N=2) of the sample size.

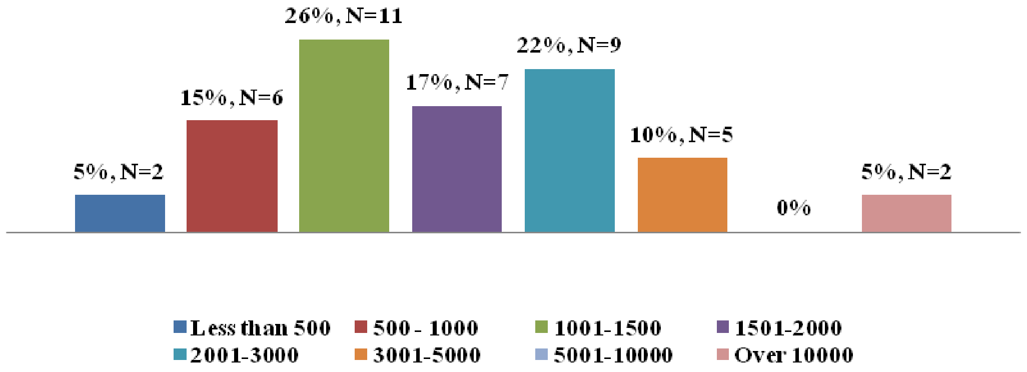


Figure 5-5 Approximately how Many People are Employed in you Organization.

5.2.2 Security Breaches to your Organization

In response to the question "Please record in the table below the approximate number of IT security breaches that your organization has experienced in the past two years, and indicate the severity of the worst breach of each type", all of the organizations recorded different types of reported security breach and severity.

Figure 5-6 and Figure 5-7 below describe the percentage occurrence and severity of 12 different types of security breaches. Figure 5-6 explores the frequency of occurrence and is divided into six options, starting from no occurrence (0), followed by greater than five times (>5), five to ten times (5-10), greater than ten times (>10), greater than a hundred (>100) and greater than a thousand (>1000) times. The percentage occurrences and severity are available in detail in Appendix D (p. 246).

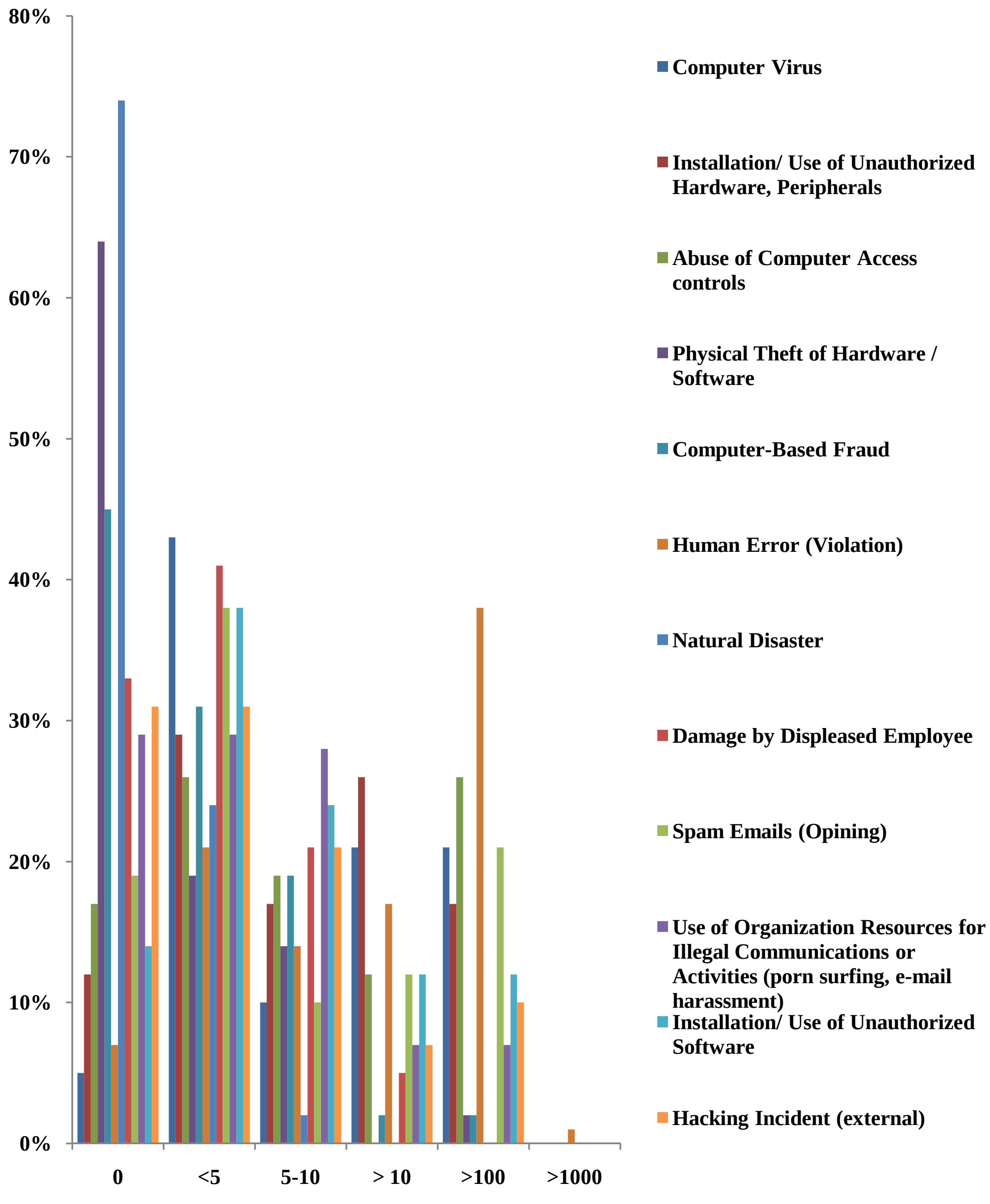


Figure 5-6 The Percentages of Occurrences of 12 Different Types of Security Breaches.

Figure 5-6 above highlights the diversity of security breaches that the organizations experienced in the last two years. The greatest occurrence, at 38 percent (N=16), is

“Human Error” followed by “Abuse of Computer Access Controls” at 26 percent (N=11) and thirdly, at 21 percent (N=9), “Computer Viruses” and “Spam Emails”.

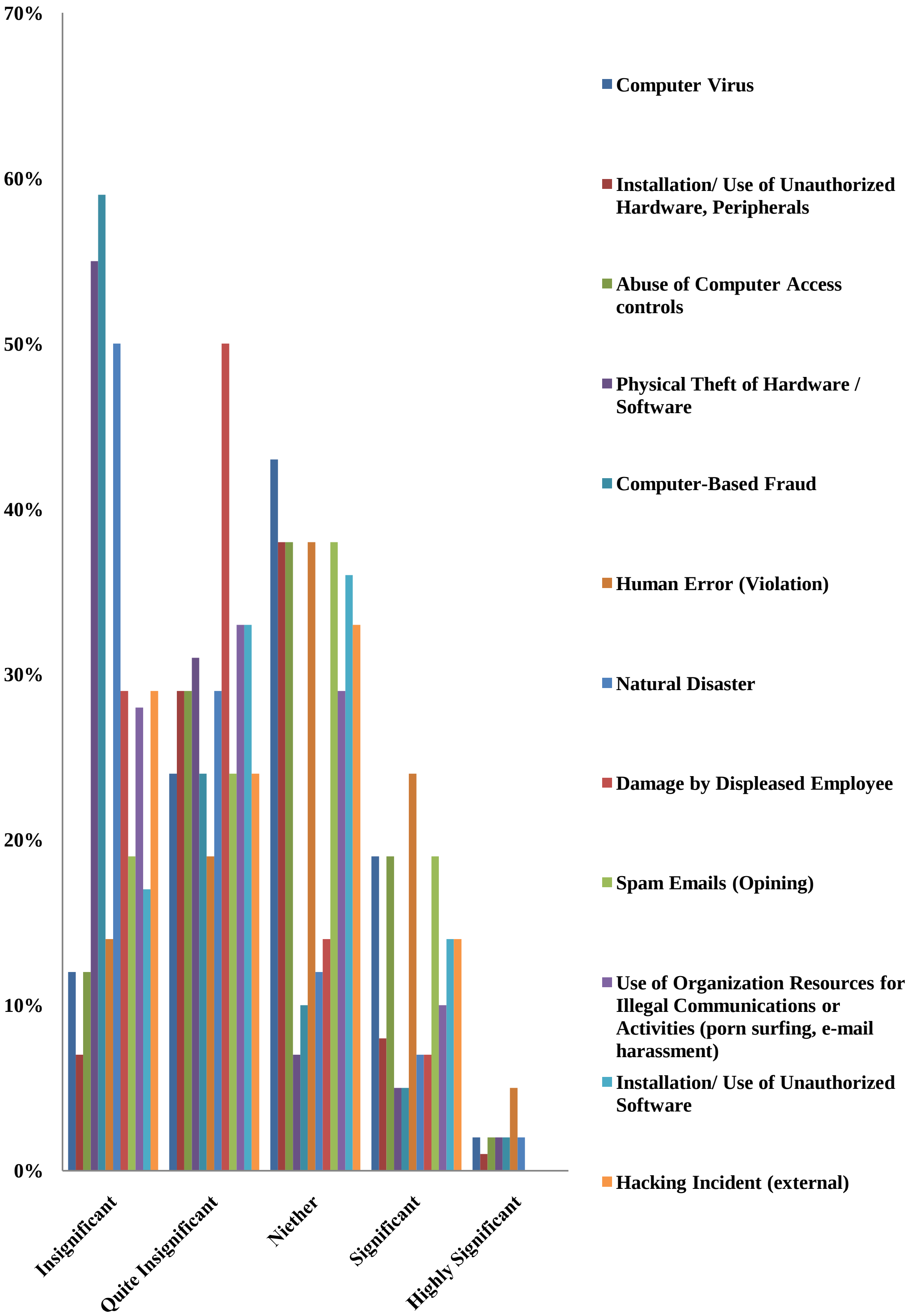


Figure 5-7 The Percentages of Severity of 12 Different Types of Security Breaches.

Figure 5-7 above describes the severity of the 12 security breaches within the organizations. Severity of the 12 security breaches is measured on a scale from 1 to 5 from quite insignificant to highly significant using a Likert scale. Organizations described "Human Error" as a significantly severe security breach with 24 percent (N=10). "Spam Emails" and "Abuse of Computer Access Controls" and "Computer Viruses" are the second most severe group with 19 percent (N=8).

5.2.3 Information Security Policy

The section that follows describes different aspects related to information security policy.

5.2.3.1 The Existence of Information Security Policy

In response to the question, "Does your organization have an Information security policy?" 81 percent of the respondents answered "yes" (N=34), whilst the remaining 19 percent of the sample answered "no" (N=8). No reasons were given why organizations did not have an information security policy. Details are presented in the following Figure 5-8.

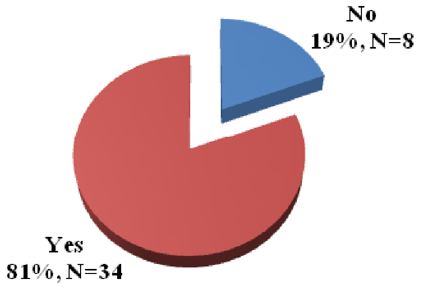


Figure 5-8 Does your Organization have an Information Security Policy?

Those organizations who have an information security policy (N= 34) were asked "Is the information security policy documented?" Almost half of the organizations (47%, N=16) answered "no". Details are presented in the following Figure 5-9. For the organizations who did not have a documented security policy, only 56 percent (N=9) stated a reason for not having *a documented* information security policy in their organizations; 37 percent (N=6) stated that they are in the process of documenting their policy and 19 percent (N=3) are of the opinion that there is not enough effort from the organization to do so.

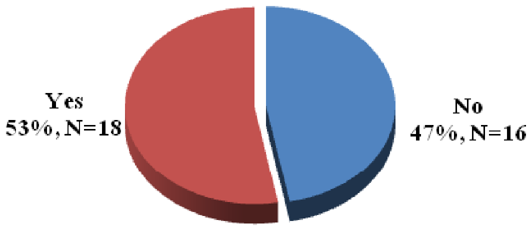


Figure 5-9 Is the Information Security Policy Documented?

5.2.3.2 The Age of Documented Information Security Policy

Respondents from organizations that have an information security policy were asked “how long has your organization been actively using a documented information security policy?” Of the 18 organizations that had a documented information security policy, 27 percent of (N=5) the sample had been practicing a documented security policy for 5 years and 22 percent (N=4) for 6 years. Details are presented in the following Figure 5-10.

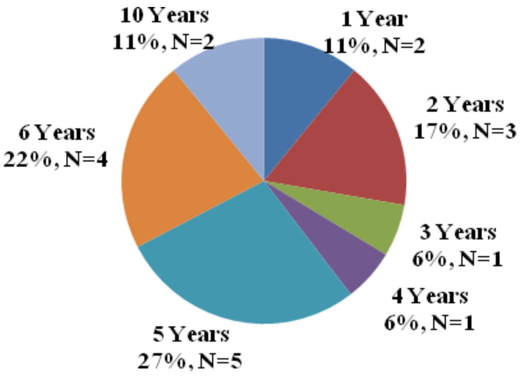


Figure 5-10 How Long your Organization been Actively Using a Documented Information Security Policy?

The following description is based on the 34 organizations that had an information security policy documented or not documented.

5.2.3.3 Methods for Distribution of Information Security Policy

Respondents from organizations that had an information security policy were asked, “How is the policy distributed to employees?”. 15 percent (N=5) of them distribute it through their “organization’s intranet”, whilst 35 percent (N=12) make the policy available via a “staff book”, and 50 percent (N=17) adopt “other” methods. An analysis of the “other” methods reveal that 59 percent (N=10) of those organizations did not specify what other ways were used to distribute their security policy to their employees. 29 percent (N=5) use ‘memo circulation’ to their staff, 6 percent (N=1) use ‘awareness classes’ to explain the security policy and the remaining 6 percent (N=1) use ‘verbal briefings’.

5.2.3.4 Effectiveness of Information Security Policy

In response to the question “How would you rate the overall effectiveness of your policy?” almost half of organizations, 50 percent (N=17), believe their policy is effective, whilst 41 percent (N=14) chose ‘neither’, as described below in Figure 5-11.

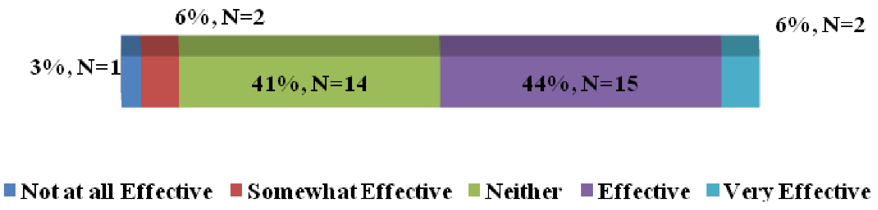


Figure 5-11 How would you Rate the Overall Effectiveness of your Policy?

In response to the question “How would you rate your organization's effectiveness at detecting and responding to attempted information security breaches from your own employees?”, 32 percent (N=11) believe their organizations are responding to security breaches effectively. 38 percent (N=13) chose ‘neither’, as shown in Figure 5-12.

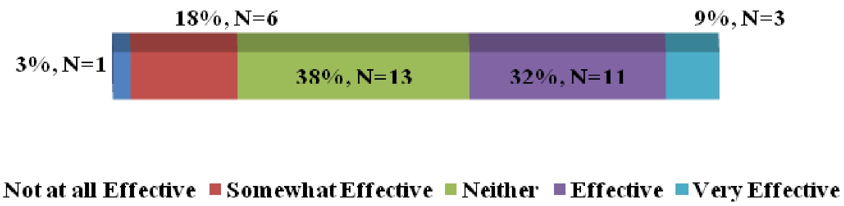


Figure 5-12 How would you Rate your Organization’s Effectiveness at Detecting and Responding to Attempted Information Security Breaches from your Own Employees?

5.2.3.5 Legislation of Information Security in the Country

In response to the question "Do you think legislation for information security is required in this country?", 74 percent (N=25) of organizations answered "yes". When asked, "How would you rate the success of implementing information security in your organization when there is legislation for information security in the country?", 62 percent (N=21) believe that legislation for information security in Oman would enhance the implementation of information security in their organizations as illustrated in Figure 5-13.

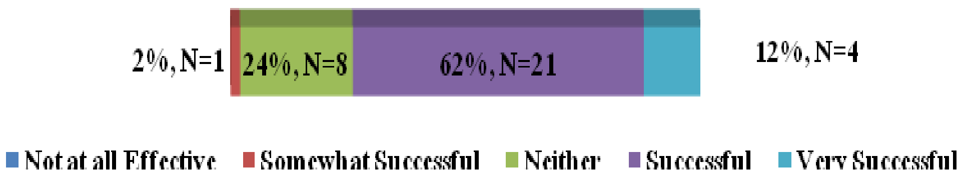


Figure 5-13 How would you Rate the Success of Implementing Information Security in your Organization when there is Legislation for Information security in the country?

5.2.3.6 Compliance in Organization and Recording Security Breaches

In response to the question "How do you check the compliance of employees to your security policy?", 44 percent (N=15) of organisations check compliance on a "monthly" basis, whilst 6 percent (N=2) do it "quarterly", 3 percent (N=1) do it "annually" and 3 percent (N=1) "less often than annually". 44 percent (N=15) are either not sure of such compliance with security policy or they do not practice it as they selected the "unknown" box. When asked about what method they use to check their employees' compliance 26 percent (N=9) selected "none", 56 percent (N=19) "Audit", 12 percent (N=4) apply "random visits", and 6 percent (N=2) apply "remote checks". These details are described in Figure 5-14.

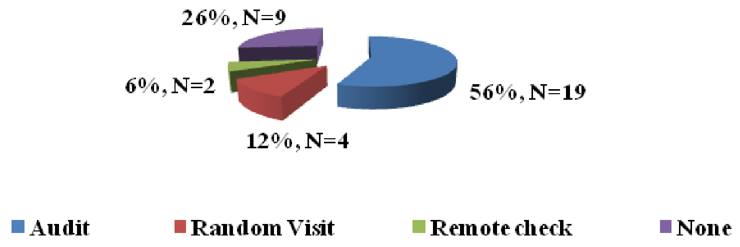


Figure 5-14 How do you Check the Compliance of Employees to your Security Policy?

Respondents were asked if they record the number of security breaches that occur in their organization. 71 percent (N=24) answered “yes”, whilst the remaining 29 percent (N=10) answered ‘no’. In response to the question, “Are the organization’s computers and network devices (e.g. routers, and switches) regularly tested for vulnerabilities?”, 82 percent (N=28) of organizations regularly test their computer and network devices, 18 percent (N=6) do not. In response to the question “Are all computer systems protected with up-to-date anti-virus software and other defences against malicious software attacks?”, 88 percent (N=30) of organizations do protect their computer systems in this way, while 12 percent (N=4) do not.

5.2.3.7 Issues Covered in Information Security Policy

Security policy covers many different aspects including internet usage, user login responsibilities and more. The findings presented in Table 5-1 indicate that these issues are covered differently by the sampled organizations. The results show that 91 percent (N=31) have user login responsibilities, 88 percent (N=30) include Viruses, Worms & Trojans. 76 percent (N=26) of organizations have policies about personal usage of organization resources. 50 percent (N=17) of organizations explain the consequences of violations and breaches in their security policy. In addition, 24 percent (N=8) of organizations have a feedback system for suggesting policy improvements in their policy security.

Issue Covered in Information Security Policy	Yes	Number of Responses
User Login Responsibilities	**91%**	**31**
Viruses, Worms & Trojans	**88%**	**30**
Use of Organization System & Network	**85%**	**29**
Personal usage of Organization Resources	**76%**	**26**
Internet Access	**74%**	**25**
Email Usage	**74%**	**25**
Disclosure of information	**65%**	**22**
Define Responsibilities	**53%**	**18**
Explain the Consequences of Violations and Breaches	**50%**	**17**
Adoption of some Laws, for example: Data Protection Law, International standards (ISO 17799), Privacy Law...etc.	**35%**	**18**
Feedback system for suggesting policy improvements	**24%**	**8**

Table 5-1 Percentages of Organization Practicing Different Issues Covering their Security Policy.

5.2.4 The Success Factors of Information Security

This sample is drawn up from government organizations in Oman. This section of the questionnaire addresses the success factors for information security. Some key factors were found in the previous interviews (awareness and training, top management support, budget, information security policy enforcement and adaptation, organization mission and organization resources). These success factors were derived from the opinions of the experts of IT and information security.

The questionnaire results suggest that all organizations believe that it is very important that all the mentioned factors should be implemented for successful information security. Surprisingly, when it came to the adoption of these factors many organizations felt they were unsuccessful as described in Figure 5-15 and Figure 5-16. For example, regarding the statement, “organization setting clear goals and objectives of information security”, 53 percent (N=18) of organizations believe this factor is very important but 38 (N=13) percent of all organizations cannot be sure if this factor is successfully adopted or not. 82 (N=28) percent of organizations believe that “effective and ongoing awareness program of security for all employees” is very important but only 9 percent (N=3) felt they were very successful and 12 percent (N=4) successful. 68 percent (N=23) of organizations believe that the factor “sufficient budget for information security” is very important but only 18 percent (N=6) adopted this factor successfully. 6 percent (N=2) of organizations are adopting this factor very successfully. Details of the percentages of the importance of each success factor and adoption of these factors in the organizations are available in Appendix D (p. 247).

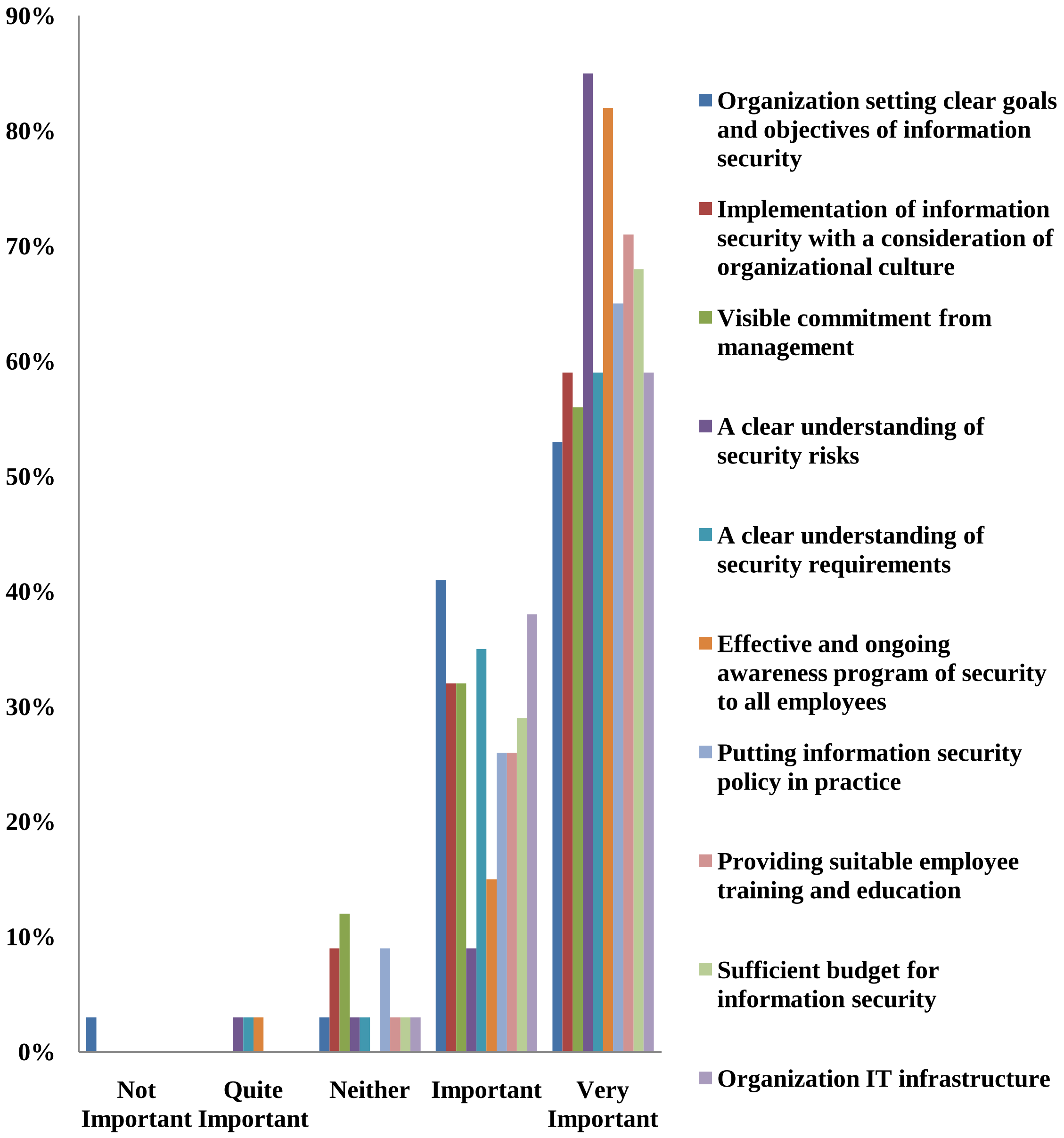


Figure 5-15 How Important do you believe the Following Factors to be for the Successful implementation of Information Security in your Organization?

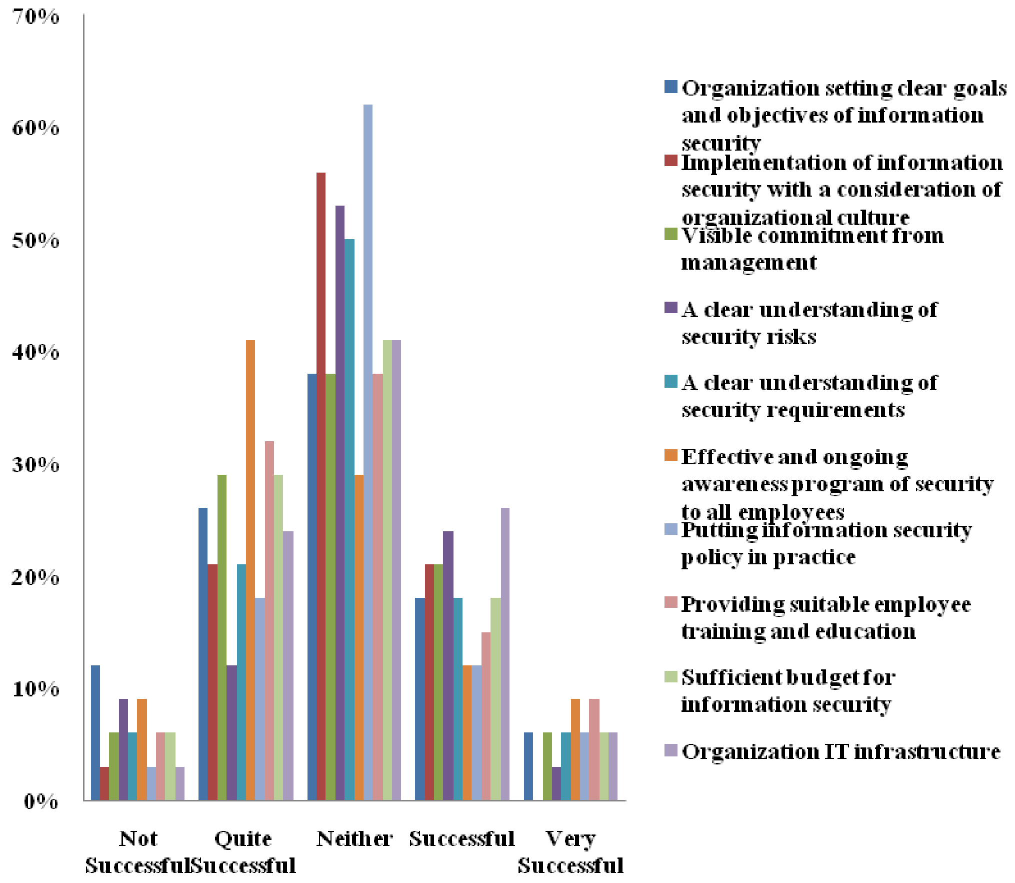


Figure 5-16 How Successful do you Believe your Organization has been in adopting each of these Factors?

5.2.5 The Criteria of Information Security Policy

This section of the questionnaire is only for organizations that have a documented information security policy (18 out of 42 organizations). Figure 5-17 and Figure 5-18 below present criteria for information security policy. The result shows that all the organizations believe in the importance of each criterion. However, these criteria are not well implemented by all organizations. These criteria are important in security policy for employees to understand the purpose of the policy, what is acceptable activity and what is not. For example, 61 percent (N=11) felt that it was 'important' for the policy to “explain what acceptable activity is and what is not”. 17 percent (N=3) said they adopt this criteria successfully. The criteria of security policy being “dynamic in order to cover the changes in the environment of information security” has been considered very important by 50 percent (N= 9) of the organizations, however only 17 percent (N=3) considered its implementation successful. All the details are explained in Appendix D (p. 248).

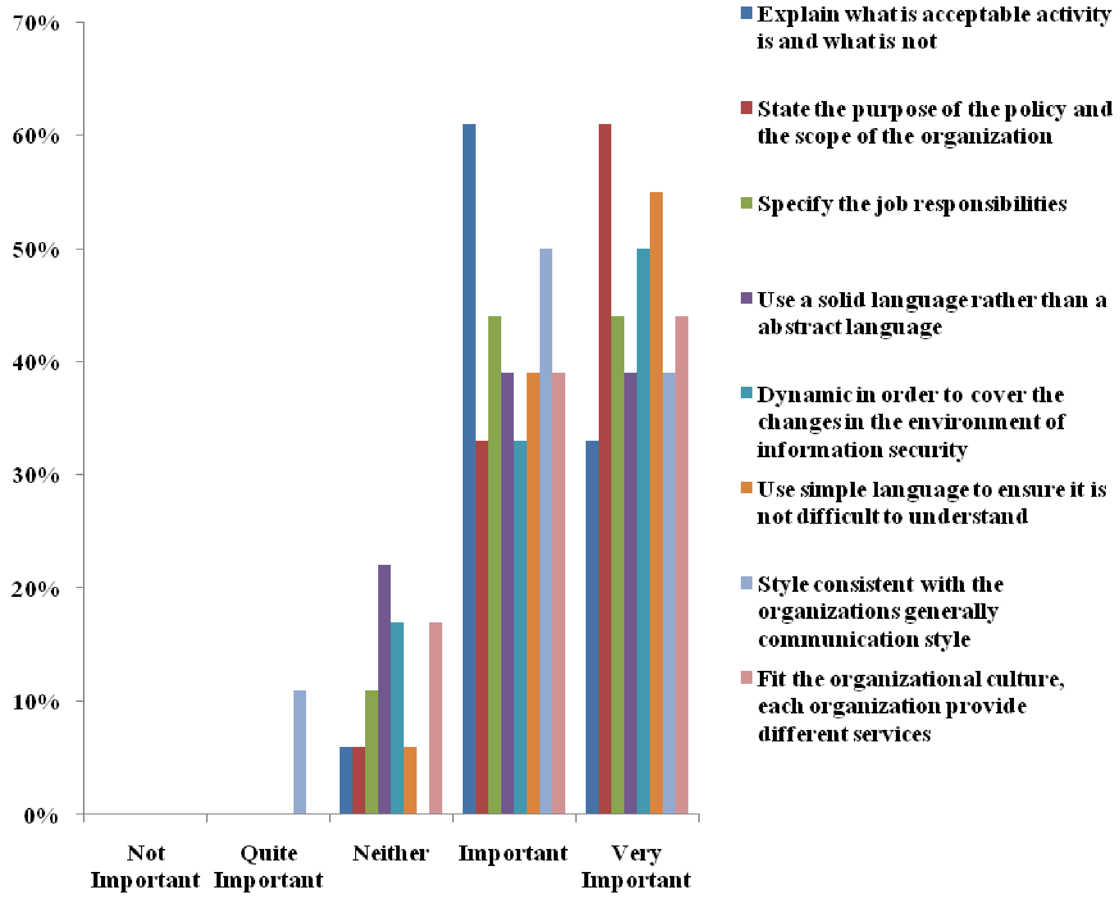


Figure 5-17 How Important do you believe the Following Criteria to be for the Successful implementation of Information Security in your Organization?

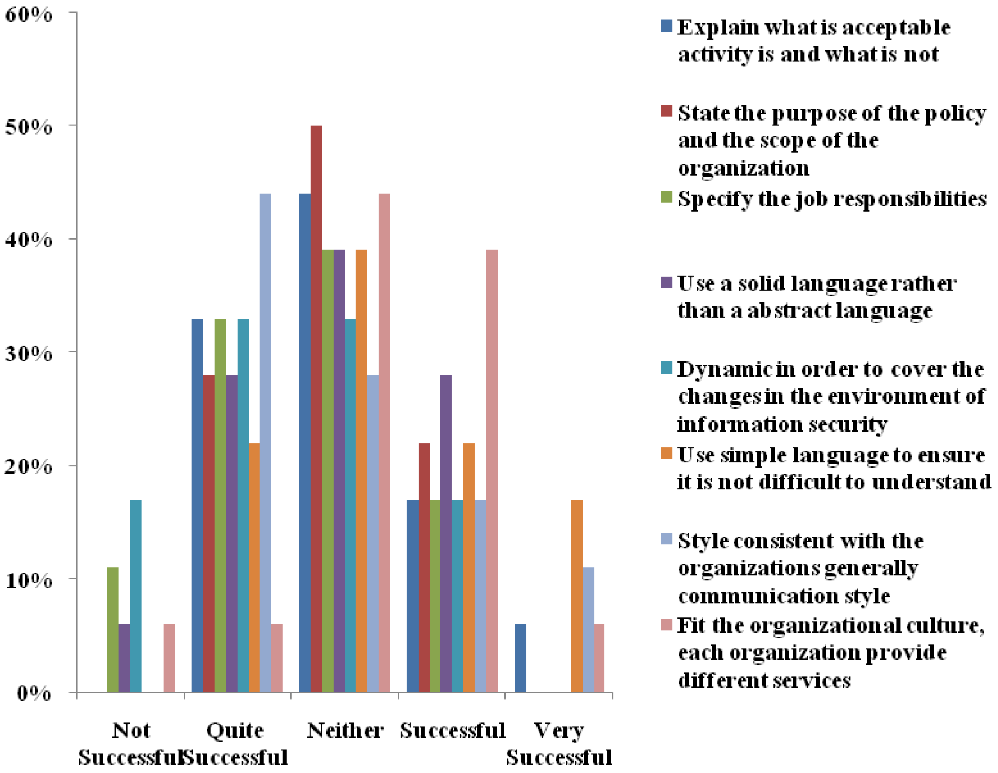


Figure 5-18 How Successful do you Believe your Organization has been in adopting each of these Factors?

5.2.6 Analysis of the Research Questions

The data for this study is non-parametric. Answers were measured on nominal (categorical) and ordinal (ranked) scales. Therefore non-parametric tests can be used to analyze the data for this study including the Mann-Whitney U Test, Kruskal-Wallis Test and Kendal tau_b.

To start analysis a new variable has been calculated from the frequencies of reported security breaches which organizations are experiencing (see question 3 in Appendix B, p. 239). This new variable represents the total reported security breaches in each organization. For example, if an organization selected that the number of breaches they are experiencing is <5 it has been calculated as 5 and divided by 2 to get a continuous dependent variable. If they selected >100 it has been calculated as 100 and divided by 2 and so on for all the other options. For 5-10 the mean (7.5) was calculated and then divided it by 2. This variable and all the data variables are presented in round numbers in Appendix D (p. 249-270). The total reported security breaches has been used as a dependent variable on almost all proposed research question. The detail of the test output of each research question is provided in Appendix D (p. 250-252).

R1: Do organizations with a security policy report fewer breaches than organizations without a security policy?

A Mann-Whitney U test was used to test the differences between two independent groups on a continuous measure. This test is the alternative to the t-test for independent samples. It compares the medians rather than the means of two groups as in the t-test. For this research question is question 4 (See Appendix B, p. 240): “Does your organization have an information security policy?” with “yes” or “no” answers, and the total security breaches variable.

The test output of the probability value (p) is 0.01, which is less than 0.05, and so the result is significant. Therefore there is a difference in the reported security breaches of organizations when the information security policy is documented or not documented. The result suggests that organizations that have a documented security policy will report fewer breaches than organizations that do not have a documented security policy.

R2: Do organizations with a security policy report fewer security breaches?

Here Kendall's tau_b correlation test was used to look at the correlation between the two variables, Question 4 “Does your organization have an Information security policy?” and total reported security breaches.

The result shows that (r = -.112, p =.387 >.05), the probability value (p) is not less than or equal to .05 which indicates the result is not significant, therefore it cannot conclude that there is a relationship between the existence of a security policy and the number of reported security breaches.

R3: Do organizations with a documented security policy experience fewer reported security breaches?

Here Kendall's tau_b correlation test was used. The correlation between two variables was looking at, Question 6 “Is the information security policy documented?” with “yes” or “no” answers, and total reported security breaches.

The result shows that (r = -.374, p =.010 <.05); the probability value (p) is less than .05 which indicates the result is significant. Therefore, there is a relationship between the documented security policy in organizations and the number of reported security breaches.

R4: Do organizations with a policy with a broader scope experience fewer reported security breaches?

Here Kendall's tau_b correlation test was used to look at the correlation between the two variables: Question 20 “Indicate the issues covered in your Information security policy?”, and the total reported security breaches variable. A broader scope of the policy was measured, by adding the number of responses to question 20.

The result shows that (r = -.207, p =.067 >.05), the probability value (p) is not less than or equal to .05 which indicates the result is not significant. Therefore it cannot be concluded that there is a relationship between a broader scope of issues in the policy and the number of reported security breaches.

R5: Do organizations with more adoption of security policy criteria experience fewer reported security breaches in their organization?

Here Kendall's tau_b correlation test was used to look at the correlation between: Question 22,“please indicate the importance of each of the following criteria and the extent to which your information security policy is successful in adopting them” and total reported security breaches.

Adopted Criteria of Information Security Policy vs. Total Security Breaches	Correlation	Probability Value (p)
Explain what is acceptable activity is and what is not	-.178	.203
State the purpose of the policy and the scope of the organization	-.132	.352
Specify the job responsibilities	-.067	.630
Use a solid language rather than an abstract language	-.166	.235
Dynamic in order to cover the changes in the environment of information security	-.040	.776
Use simple language to ensure it is not difficult to understand	-.123	.370
Style consistent with the organizations generally communication style	-.032	.817
Fit the organizational culture, each organization provide different services	-.307	.028

Table 5-2 The Correlation between the Level of Adoption of Information Security Criteria in the Organization and the Organizations' Level of Security Breaches, (Kendall's tau_b correlation test).

The correlation in the above Table 5-2 illustrates a modest negative relationship between the level of adoption of different criteria in the security policy and the number of reported breaches in the organization. The probability value (p) for the all criteria of security policy to the level of breaches is not less than or equal to 0.001, 0.01 or 0.05, except the factor “Fit the organizational culture, each organization provides different services”. This indicates that the result is not significant; therefore it cannot conclude that there is a relationship between the adoption of security policy criteria and the number of reported security breaches.

R6: Is there any difference in the number of reported security breaches between organizations reporting different levels of compliance of employees to the organization security policy?

In this research question the Kruskal-Wallis Test is used to compare more than two groups. In parametric data the alternative test is a one-way analysis of variance between groups. In this case scores are converted to ranks and mean rank is compared for each group. For this research question the study considered: Question 15 “How often do you check compliance to your security policy?” with 6 groups of answers (e.g. weekly, monthly, quarterly, annually, less often than annually, and unknown), with the total number of reported security breaches variable.

The results show that the probability value (p) is 0.044, which is less than 0.05. It can conclude that the result is significant. This means that there is a concurrence in the period of time the organization checks their employee compliance, with the total breaches in the organization. Therefore, when organizations check compliance with their policy on a monthly basis, it is likely there will be a difference in the reported level of breaches, compared with if they check annually or more.

R7: Is there any difference in reported security breaches across number of employees?

Here the Kruskal-Wallis Test was used. For this research question the study considered: Question 2 “Approximately how many people are employed in your organization?” with 8 groups (e.g. less than 500, 500-1000, 1001-1500, to …over 10000). This is compared to the total reported security breaches variable.

The test output of the probability value (p) is 0.003 which is less than 0.01; so the results suggest that there is a statistically significant correlation in the number of reported security breaches compared with the number of employees in the organization. Therefore it can conclude that the more employees an organisation has, the more security breaches it will be likely to report.

R8: Do organizations that report an effective security policy also report fewer security breaches?

Here Kendall's tau_b correlation test was used. This research question correlates two variables: question 10 (see Appendix B, p. 240) “How would you rate the overall effectiveness of your policy?”, and the frequency of reported security breaches variable.

The result shows that ($r = -.340$, $p = .013 < .05$), the probability value (p) is less than .05 which indicates the result is significant, therefore there is a relationship between the reported effectiveness of security policy and the reported number of security breaches.

R9: Do organizations with greater adoption of ‘success factors’ also report fewer security breaches in their organization?

Here Kendall's tau_b correlation test was used. This research question correlates two variables: Question 21, “Please indicate the importance of each of the following factors and the extent to which your organization is successful in adopting them,” and the reported security breaches variable.

Table 5-3 indicates a modest negative relationship between the reported adoption of success factors and reported level of security breaches. The probability value for only two success factors which are “Organization has clear goals and objectives of information security” and “Sufficient budget for information security” is less than 0.05. The rest of the success factors are not less than or equal to 0.05. This indicates that there is no correlation between the reported adoption of success factors and reported level of security breaches.

Organization Success Factor Adopted vs. Total Security Breaches	Correlation	Probability Value (p)
Organization clear goals and objectives of information security	-.269	.042
Implementation of information security with a consideration of organizational culture	-.093	.497
Visible commitment from management	-.008	.950
A clear understanding of security risks	-.097	.474
A clear understanding of security requirements	-.138	.305
Effective and ongoing awareness program of security to all employees	-.054	.684
Putting information security policy in practice	-.201	.141
Providing suitable employee training and education	-.029	.827
Sufficient budget for information security	-.264	.048
Organization IT infrastructure	-.223	.096

Table 5-3 The Correlation between the Adoption of Success Factors of Information Security in Organizations and the Organizations' Level of Security Breaches, (Kendall's tau_b correlation test).

R10: Do organizations with a broader security policy report a more effective information security policy?

Here Kendall's tau_b correlation test was used. Here the correlation is between: Question 20, “Indicate the issues covered in your Information security policy?”, and Question 10 “How would you rate the overall effectiveness of your policy?”.

The result ($r = .320$, $p =.025 <.05$), suggests a moderate positive relationship between the number of issues covered in the organization's security policy and the effectiveness of the organization's security policy with a significant (p) value < 0.05. This indicates that the more issues the organization covers, the more effective their policy is felt to be.

R11: Do organizations that report greater adoption of security policy criteria also report more effective security policy?

Here Kendall's tau_b correlation test was used. Here the correlation is between two variables: Question 22, “please indicate the importance of each of the following criteria and the extent to which your information security policy is successful in adopting them”, and question 10, “How would you rate the overall effectiveness of your policy?”.

Adopted Criteria of Information Security Policy vs. the effectiveness of the security policy	Correlation	Probability Value (p)
Explain what is acceptable activity is and what is not	.529	.001
State the purpose of the policy and the scope of the organization	.582	.000
Specify the job responsibilities	.402	.011
Use a solid language rather than a abstract language	.447	.005
Dynamic in order to cover the changes in the environment of information security	.419	.008
Use simple language to ensure it is not difficult to understand	.550	.000
Style consistent with the organizations generally communication style	.502	.001
Fit the organizational culture, each organization provide different services	.387	.014

Table 5-4 The Correlation between the Level of Adoption of Information Security Criteria in the Organization and the Effectiveness of the Security Policy, (Kendall's tau_b correlation test).

Table 5-4 presents a correlation between the reported level of adoption of information security criteria in the organization and the reported effectiveness of the security policy. The result suggests a strong positive correlation between the two variables. This means that the more an organization reports adopting different criteria in their security policy the more they report a highly effective security policy. The probability value (p) of the result for all the criteria is less than or equal to 0.001, 0.01 and 0.05, so the result is statically significant.

R12: Do organizations that report a greater adoption of success factors report a more effective security policy?

Here Kendall's tau_b correlation test was used. The study looked at the correlation between two variables: Question 21, “Please indicate the importance of each of the following factors and the extent to which your organization is successful in adopting them?”, and Question 10, “How would you rate the overall effectiveness of your policy?”.

The output presented in Table 5-5 suggests a positive relationship between the reported number of adopted success factors in the organization and the reported effectiveness of the security policy. The probability value (p) for nearly all the success factors is significant, less than 0.05, 0.01 and 0.001, except for three success factors which are “effective and ongoing awareness program of security to all employees”, “providing suitable employee training and education”, and “sufficient budget for information security”. The correlation coefficient for the success factors versus the reported effectiveness of the security policy is positive. This indicates that the more the organization implements the success factors; the more effective they feel the security policy will be.

Organization Success Factor adopted vs. the effectiveness of the security policy	Correlation	Probability Value (p)
Organization clear goals and objectives of information security	.290	.054
Implementation of information security with a consideration of organizational culture	.549	.000
Visible commitment from management	.317	.036
A clear understanding of security risks	.433	.005
A clear understanding of security requirements	.320	.036
Effective and ongoing awareness program of security to all employees	.279	.065
Putting information security policy in practice	.356	.022
Providing suitable employee training and education	.281	.063
Sufficient budget for information security	.231	.128
Organization IT infrastructure	.501	.001

Table 5-5 The Correlation between the Adoption of Success Factors of Information Security in Organizations and the Effectiveness of the Organization's Security Policy, (Kendall's tau_b correlation test).

R13: Is there any relationship between the reported effectiveness of the information security policy and the reported effectiveness at detecting and responding to information security breaches?

Here Kendall's tau_b correlation test was used. Here a correlation has been used to find the relationship between: Question 10, “How would you rate the overall effectiveness of your policy?”, and Question 11, “How would you rate your organization's effectiveness at detecting and responding to attempted information security breaches from your own employees?”

The result is (r = .757, p =.00 <.001). Therefore the correlation between the reported effectiveness of the security policy in an organization and the organization's reported effectiveness at detecting and responding to information security breaches is highly positive. Organizations which report an effective information security policy also report being effective at detecting and responding to attempted information security policy breaches from their own employees. The probability value (p) confirms that the result is statistically significant.

5.3 Discussion

The findings indicate that 81 percent (N=34) of Omani organizations questioned have a security policy in place. Only 16 out of 34 organizations are practicing a documented security policy. Analysis of research question R1 “Do organizations with a security policy reported fewer breaches than organizations with out a security policy?” suggested that organizations with a documented security policy will report fewer breaches than organization who do not have a documented security policy. Analysis of the research question R3 “Do organizations with a documented security policy experience fewer reported security breaches?” suggests that there is a relationship between the documented security policy in organizations and the number of reported security breaches. According to Kessler (2001), the lack of a written security policy will result in low protection levels. If organizations do not have their security policy written, employees are not able to know what they are allowed to do or not regards their organization system, as it has been discussed in the findings from Chapter Four.

The results reveal two reasons why organizations do not have a documented security policy. One reason is that the organization has only recently taken security problems serious so is only now in the process of developing a documented security policy. The second reason is that the IT department of the organization feels that their organizations are not putting enough effort into doing so. Findings from Chapter Four also show the same result for the end-user employees. What could explain the slow effort from the organization is, as Siponen (2001) explains, that organizations usually do nothing in terms of information security as long as nothing goes wrong. From Chapter Four it has been suggested that having a security department separate from the IT department is helpful for the implementation of information security in organizations.

Chapter Four's findings introduced the importance of legislation in Oman to improve the implementation of information security. This study’s outcomes show 74 percent (N=25) of organizations feel legislation is required in Oman. 62 percent (N=21) of organizations believe that legislation for information security in the country would enhance the implementation of information security.

The results reveal that the analysis of the research question R4 “Do organizations with a policy with a broader scope experience fewer reported security breaches?” concludes that there is no relation between organizations with a security policy covering a broader scope (user login responsibilities, use of organization system & network, internet access, etc…) and the number of reported security breaches. The outcome reveals organizations believe in the importance of each of the 'success factors' (awareness and training, top management support, budget, information security policy enforcement and adaptation, organization mission and organization resources). The results also suggest the adoption of these factors has not been implemented by all organizations. Analysis of the research question R9 "Do organizations with greater adoption of 'success factors' also report fewer security breaches in their organization?" suggests no relationship between the greater reported adoptions of 'success factors' and the level of reported security breaches in their organization.

The above findings do confirm the findings from Chapter Four in that there is a gap between the importance of the success factors and their implementation. This could be related to recognising management attitudes, not enough money or complacency.

Organizations feel that the criteria of security are important. The adoptions of these criteria were not well implemented by all organizations. Analysis of the research question R5 "Do organizations with more adoption of security policy criteria experience fewer reported security breaches in their organization?" suggests no relationship between the reported levels of adoption of different criteria in the security policy and the number of reported security breaches in the organization.

44 percent (N=15) of organizations feel that their security policy is effective. The other 44 percent were not sure. This was also clear from Chapter Four's findings. This could be related to the fact that security is not easy to measure (Sandhu, 2003). Analysis of the research question R10 "Do organizations with a broader security policy report a more effective information security policy?" concludes that the more issues the organization covers in their security policy the more effective their policy will be reported to be. The results reveal organizations cover these issues differently. For example 91 percent (N=31) include user login responsibilities in their policy, 74 percent (N=25) include internet access and only 24 percent (N=8) include feedback system for suggesting policy improvement in their security policy. Analysis of the research question R11 "Do organizations that report greater adoption of security policy criteria also report more effective security policy?" concludes that the more an organization reports that they adopt criteria in their security policy, the more they report a highly effective security policy. Analysis of the research question R12 "Do organizations that report a greater adoption of

success factors report a more effective security policy?” suggests that the more the organization implements the ‘success factors’ the more effective they feel security policy will be.

Analysis of the research question R13 “Is there any relationship between the reported effectiveness of the information security policy and the reported effectiveness at detecting and responding to information security breaches?” suggests that organizations which report effective information security policy also report they are effective at detecting and responding to reported information security breaches.

The unexpected results of the analysis of the research question R5 “Do organizations with more adoption of security policy criteria experience fewer reported security breaches in their organization?” and R9 “Do organizations with greater adoption of ‘success factors’ also report fewer security breaches in their organization?” could be due to a couple of reasons:

Policy implementation and enforcement: according to David (2002), proper security could be realized through the implementation and enforcement of the policy. This was clear from the results of the analysis of the research question R1 “Do organizations with a security policy reported fewer breaches than organizations with out a security policy?” and R3 **“**Do organizations with a documented security policy experience fewer reported security breaches?” that organizations with a documented security policy will report fewer security breaches.

Employee compliance to policy: the highest security breaches that the findings suggest that organizations are experiencing in the last two years is by human error (38%, N=16). The results indicate that organizations with more employees will experience more reported security breaches as concluded in the analysis of the research question R7 “Is there any difference in reported security breaches across number of employees?”. Verdon (2006, p. 43) states, "*while not having a policy is bad, having a policy and not following it is just as bad, if not worse*". So employee compliance is the main aspect to concentrate on in order to strengthen the organization's defence and organizations need to ensure that their employees comply with their security policy (Nijhof et al., 2003).

Analysis of the research question R6 concludes that there is a correlation between the period of the time the organization checks their employee’s compliance with the reported security breach in the organization. For example, when organization's check compliance with their policy monthly, there is a difference in the reported level of breaches, compared with if they check annually or more than annually. The result shows 44 percent (N=15) of organizations check their employee compliance to their organization security policy. Another 44 percent (N=15) were either not sure of such compliance with security policy or they did not practice it.

5.4 Conclusion

When any professional in security or IT was asked the first thing that their organization needs to do to have a secured system they answer is that it is to have an information security policy (Wylder, 2007). In this case, information security starts with policies (Blakley et al., 2002) which it is the mainstay of security (Shorten, 2007). Of course, having a security policy is not the solution to all security problems (Howard, 2007), but without a security policy, security practices will struggle to meet the objectives of protecting organizational assets (Higgins, 1999). An information security policy is required to be in place to minimize the threat of unacceptable use of any of the organization’s information resources (Blakley et al., 2002).

Implementing an information security policy (AUP) is not as easy as it sounds; it needs to be written properly to meet the needs of the types of protection organizations are seeking. The sensitive nature of information security could make the participants reluctant to say what they do or what they truly believe. The number of security breaches the organizations are experiencing is not known exactly. Therefore, this research is all about *reported* frequency of breaches compared to *reported* attributes of security policy.

The lack of exact meaning concerning information security policy makes the concept of security policy complicated to define. Therefore, the effectiveness of security policy can not be explained by a single framework. The findings help us to understand what makes an effective security policy. The results conclude that organizations with broader issues covered in their security policy report greater adoption of security policy criteria and ‘success factors’. In other words, they report a more effective security policy.

There is no point in having a security policy where employees cannot have access to it or one which is never updated to handle new security threats. Some reasons have been suggested to help in understanding why when security policy uses a broad scope of criteria (explaining what acceptable activity is and what is not, stating the purpose of the policy and the scope of the organization, specifying the job responsibilities, etc…), and the security policy covers several issues (user login responsibilities, internet access,…etc), this does not seem to have an influence in reducing reported security breaches. For such surprising results a future investigation is suggested to help interpret and explain these findings.

Given the results of Chapter Four and Five further exploration into the compliance of employees in organizations is necessary. This will be presented in Chapter Six

Chapter Six

Compliance with Organization's Security Policy – Semi-Structured Interviews (Glasgow, UK)

This chapter builds on the findings of the previous chapters and uses UK based Interviews to further explore some of the issues raised. Analysis of the research question R5 suggested that there was no relationship between the reported levels of adoption of different criteria (e.g. explain what is acceptable activity and what is not, state the purpose of the policy and the scope of the organization, etc…) in the security policy and the number of reported security breaches in the organization. Analysis of the research question R9 suggested no relationship between the greater reported adoptions of 'success factors' (e.g. organization setting clear goals and objectives of information security, implementation of information security with a consideration of organizational culture, etc…) and reporting fewer security breaches in their organization. These unexpected findings suggest further investigation is required into employee compliance with their organization's information security policy.

In order to qualitatively explore the issues of employee compliance with security policy, an accessible UK sample was used. The result of this phase of the study were exploratory and of a sensitive nature and therefore it was felt that the UK sample might be more open in order to reveal some understanding of the issues of non-compliance. For such sensitive investigations about employee compliance with security policy it has been decided to conduct the interviews at the University of Glasgow for both the ease of access and the likelihood that participants feel more comfortable in discussing this matter with someone considered a colleague.

This chapter is organized as follows. The following section introduces the focus of the chapter. Section 6.2 presents the methodology for the research study. Section 6.3 summarizes the results of the analysis. Section 6.4 discusses the results. Section 6.5 presents the conclusion of this chapter.

6.1 Introduction

As shown in the previous chapters, employees are one of the major points of vulnerability in organisations. They also act positively to mitigate crises in organizations (Dhillon, 2006). On the other hand, organizational controls and restrictions become insufficient if employees in the organisation keep the required locks open through not complying with their organization's security policy.

Apparently, employees' minor decisions have the potential for creating a security incident (Hardee, et al. 2006; and Schwiderski-Grosche, 2006) purely because security policies and standards cannot prescribe how employees should behave in every possible circumstance they may come across (Leach, 2003). Such circumstances could be related to social engineering attacks. A social engineering attack involves manipulating someone into disclosing confidential information to be used for personal gain against the organization (Workman, 2007). The findings of the 2008 Information Security Breaches Survey show that employees are increasingly targeted by social engineering attacks. "*A further emerging area is the use of social networking sites (such as MySpace, Facebook and Bebo). Many of these sites can provide legitimate business benefits (e.g. through sharing experience and best practice with other businesses). However, many companies have found that the habitual nature of these sites can adversely affect staff productivity. In addition, businesses are becoming increasingly concerned about what is being said about them on these sites, and some have experienced loss of confidential information*" (see Information Security Breaches Survey 2008, 2008, p. 21).

A study by the ISF ('Information Security Culture', The Information Security Forum, November 2000) cited by Leach (2003) suggests that 80% of major security failures in organizations are related to poor security behaviour by employees. Vroom & von Solms (2004) state that not all security breaches carried out by the employees are malicious. They can be the result of negligence or ignorance of the security policies of the organization.

Some standards exist to specify how compliance is to be achieved in organizations such as existing standards ISO 17799/ISO 27001, as already discussed in Chapter Two. Compliance in ISO 17799/ISO 27001 (p. 60-64) is divided into three sections:

- "Compliance with legal requirements: to avoid breaches of any criminal and civil law, statutory, regulatory or contractual;
- Reviews of security policy and technical compliance: to ensure compliance of systems with organizational security policies and standards;

- System audit considerations: to maximize the effectiveness of and to minimize interference to/from the system audit process".

It is up to organizations to choose how to meet such requirements from the existing standards. Sundt (2006, p. 9) suggests some tips for organisation to ensure compliance:

- "Build on existing policies, procedures and guidelines taking account of requirements and constrains relevant to the business imposed by legislation and regulation;
- Create appropriate technical, procedural and personnel standards that support those policies in the most cost-effective way and verify compliance against them;
- Accredit business systems (not just the technical elements) for fitness for purpose against the security policies. There should be a risk assessment for every such system against which appropriate controls are defined;
- Make sure all your workers, whether employees, contractors, partners or whoever, are aware of their responsibilities-and keep reminding them;
- When you outsource any part of your business or make use of managed services, ensure that the contractors include all necessary security requirements and safeguards. In particular, there must be a right of audit of such external systems to enable you both to ensure compliance with your policies and standards, and to allow access for audit and investigative purposes;
- Maintain awareness of what is happening in the outside world. This is a fast-moving environment. It will be necessary to review all your information security policies on a regular basis".

It is important not only to formulate and set rules and regulations for security policies but also to ensure that employees comply with those rules (Nijhof et al., 2003). Therefore, the implementation of information security compliance is vital for an organization to protect its information assets (Thomson & von Solms, 2004) where the security policy compliance is the main activity that requires employee implementation to maintain organization security (Neal & Griffin, 2002). This embraces conforming to organization policy, regulations and actively protecting organization assets and values from one organization to another (Sundt, 2006).

Chapter Two, section 2.8.1 describes different factors that could influence employees' security behaviour. To recap, Leach (2003) suggests six factors that makes employees take security decisions, these are: employee's personal values; employee's own security experience; organization security culture, employee's psychological contract with their organization; and senior management behaviour. These factors result in internal security threats like employee's security errors; security carelessness; security negligence; and security attacks. It is not clear what Leach based these findings upon.

Dyne et al. (1994, p. 767) argue "*organizational participation is interest in organizational affairs guided by ideal standards of virtue, validated by an individual keeping informed, and expressed through full and responsible involvement in organizational governance*". According to McIlwraith, (2006) a good security environment in an organization is not as essential as getting employees to do what they are told. He suggests some helpful features for organizations to apply for managing their information security:

- Employees easily report security incidents, even if they are responsible for it.
- Employees are aware of their organization's security issues.
- Employees want to improve the security of their organization.

Findings from Chapter Four show employees do not practice feedback about security in their organizations. Chapter Five concludes that only 12 percent (N=4) of organizations provide training and awareness programmes to their employees. 24 percent of organizations (N=8) have feedback systems for suggesting policy improvements in their security policy.

Many organizations find it difficult to implement policies that will be followed and respected by all employees (Finegan, 1994). Thrasher (2003) also argues that organizations often fail to measure compliance. As a result they may:

- Not be able to determine where weakness exists to take preventive action.
- Lack data about whether employees understand the policy or which employees might need further training.

The previous chapter discussed some reasons for the unexpected result of the analysis of the research question R4 (Do organizations with a policy with a broader scope experience fewer reported security breaches) that there is no statistical relationship between the reported level of breaches and the issues covered in information security policy (e.g. user login responsibilities, use of organization system & network,…etc). One reason could be related to the compliance of employees. Understanding how employees make a security judgement is essential to designing security features that employees will implement and utilize well (Hardee et al., 2006). Wenzel (2004) argues that the reasons why employees carry out information security breaches are not well understood. According to Workman & Gathegi (2006), there is little in the literature to explain such problem in the field of information security.

In contrast, there is more research in the field of health and safety. Storr & Clayton-Kent (2004) describe how improving compliance with hand hygiene avoids infections. They explain that compliance with hand hygiene is low, not only in health care but also in wider society. Williams et al. (2004) also conducted a survey of New Hampshire restaurants to evaluate compliance with the Indoor Smoking Act. Their survey suggests that compliance with provisions of the Indoor Smoking Act is low. These studies in the health and safety field motivate the work in this chapter. The purpose of this study is to report upon the results of a study that investigates employees' compliance with organizations' security policies.

6.2 Research Methods

The review of the literature and the findings from Chapter Five, analysis of the research question R4 (Do organizations with a policy with a broader scope experience fewer reported security breaches), R5 (Do organizations with more adoption of security policy criteria experience fewer reported security breaches in their organization), R9 (Do organizations with greater adoption of 'success factors' also report fewer security breaches in their organization) and R10 (Do organizations with a broader security policy report a more effective information security policy) suggest some aspects related to compliance with organization security policy need further investigation.

The objective of this study is to:

- Explore if the different issues of information security that have been found from Chapter Four and Five are general issues in different environments.
- Investigate what are the reasons behind employee non-compliance with an organization's security policy.
- Investigate the impact of employees' non-compliance with an organization's security policy.

6.2.1 Semi-Structured Interview

The study was conducted in two parts. The first was based on an exploratory approach using a semi-structured interview method for collecting data. The grounded theory qualitative method was used to analyse the data as used in Chapter Four.

The semi-structured interview was set up to give a guiding structure for the discussion. The selected samples for the semi-structured interviews were a mixture representing a cross-section of twenty five employees from different organizations and different departments from Glasgow University. Laws and standards related to computer misuse and data protection laws were introduced in the UK in the nineteen-nineties as mentioned in Chapter Two, section 2.5. Therefore, employees are somewhat familiar with the idea of information security. For such sensitive investigations about employee compliance with security policy it has been decided to conduct the interviews at the University of Glasgow for both the convenience and the likelihood that participants feel more comfortable in discussing this subject with someone considered a colleague. To help to explore the issues of information security a general approach was taken. Broad levels of different professions were interviewed for variety of output. Below are descriptive statistics of the interviewee's current professional position and number of years of experience in Table 6-1.

	Job Title	Years of Experience
1-	Personal Assistant	27
2-	Secretary Faculty of Education	10
3-	Senior Resident.	2
4-	Research Support Officer	1
5-	Web Services Coordinator	4
6-	Corporate Senior Management	22
7-	Research Assistance	7
8-	Laboratory Manager	14
9-	Lecturer in the Department of Computing Science	27
10-	Laboratory Technician	10
11-	Principle Advisor Studies for Science	18
12-	Technician	20
13-	Store Technician	7
14-	Technician in Charge of 3rd, 4th Year and Postgraduate	28
15-	Clerk for Three Faculties of Science	11
16-	Professor of Science Education	11
17-	Engineering Technician	2
18-	Lecturer in the Department of Physics	15
19-	Librarian	20
20-	Personal Assistant	12
21-	Research Technician	10
22-	Lecturer in the Department of Science Education	17
23-	Lecturer in the Department of Curriculum Studies	13
24-	Lecturer in the Department of Computing Science	14
25-	Head of Estate of Administration	16

Table 6-1 Descriptive Details of the Participants.

The interviewer started off with warm-up questions and gradually narrowed the scope. To begin with, interviewees were given a written statement which pointed out ethical issues such as confidentiality. There was also a description of the research study and the right to decide whether or not to take part in the interview. Finally, permission was taken to record the interview. In the majority of cases, the interviewees engaged in the discussion about their compliance with security policies.

The semi-structured interview was based around three areas involved in compliance with information security policy.

- **Organization Information Security Policy:** this section investigated how long employees have been working with their organization. It asked whether they are aware of their organization’s policy and to whom they report, if at all, security incidents. They were also asked their opinion as to whether their organization’s policy was working or not.
- **Organizational Security Culture:** this section focused on the employee’s opinions about working in their organization; what is the culture of the organization in terms of information security and what would they do if a serious security breach happened?
- **Compliance with Security Policy**: this section covered three aspects, the first one focused on the employee’s compliance with their security policy and what impact it could have on the organization. The second section covered some scenario based questions. These described security breaches in different situations to help know more about the employee’s opinions. The last section entailed giving the participant a sample information security policy (see Appendix E, p. 271-273) and asking each of them to read one section of the policy. They then had to answer three questions related to their compliance with the provided policy.

The semi-structured interview questions are formulated to explore the following:

- How much do employees know about their organization's security policy?
- What is the organizational security culture?
- How do employees comply with organization policy?
- What are the reasons behind employee non-compliance with information security policy?

- What are the impacts of employee non-compliance with information security policy?

A copy of the qualitative interview questions are found in Appendix E (p. 271-273).

6.3 Research Findings

This section is divided into two sections. The first section presents the semi-structured interviews. The second includes the scenario based questions. Scenario-based questions were used to explore the interviewee's point of view of other activities where a choice had to be made. The interviewees were asked to provide opinions based on different scenarios on employees' behaviour.

6.3.1 Section 1: Semi-Structured Interview

Before presenting the analysis of this research a brief description of the type of organization this research conducted in useful to understand the different employees' answers. The university environment is more complex than other organizations in terms of thousands of new students entering the university every year. Universities consist of students, faculty, staff, administrators, workers, etc. Different campuses with different types of network resources, where staff, students for example, expect to have access to information or their own files from classrooms, labs, libraries or off campus. Faculties in universities consist of different departments where the need of security varies from department to department and from faculty to faculty.

6.3.1.1 Organization Information Security Policy

Findings from the interviews show that many of the employees are aware that their organization has a security policy. Surprisingly when the employees were asked if they know what the policy contains, few of them said *"yes"*. Many had no idea what the security policy contained, and commented:

“Not really, no", "Not in detail but I know where I can get it from ", "Not really. I do not know what they do contain", "Not sure, if it is written down", and *“not any thing, we have obligation for anonymity generalize standard"* and *" I am not sure what we call a security policy".*

It seemed as though some employees were guessing what the policy included:

"They have told me not to do certain things on the machine. I presume in terms of computer security they told me not to do certain things in the computer. When I said they

told me not to do certain thing you are not suppose to do non-work related things "; *"I suppose using the computer's university networks*".

Or completely unaware:

"I am not aware, that I can think of, of having seen a security policy but I am aware of restrictions that apply."

Some are aware but they do not implement this policy as explained:

"We keep all undergraduate files and for current students all the information was kept for graduates. These files are kept for some time, I can not remember exactly the precise time".

Employees, especially the ones who hold a senior post, or people who measure security policy in their work, were able to give details about what their policy contains:

"*Basically we have three classifications, its got no classification, internal use only and confidential. They used to have two additional security classifications which were confidential restricted and registered"*; and it *"… gives details about the kinds of information I can store, how it can not be stored, how long for, method of disposal and who can access it".*

The results show that some departments or sections develop their own security policy according to their needs on top of the overall organizational policy. For example:

"In this office I have details, personal details related to students and staff that are kept under controlled conditions; we also have in a main lab chemicals and bacteria that we have to keep in secure condition. So we have procedures to make sure they are kept safe and certain people can access it here".

Some employees stated that the policy is working because their organization does not experience any type of breach:

"I believe it is [working], I can not think of any breaches that I know of", (same output from previous interview in Oman).

One employee described the functionality of their policy:

"I believe it does yeah, because all the records are in a safe place nobody can access except the staff who have related direction to specific information and once this information is no longer in use it is destroyed".

6.3.1.2 Organization Security Culture

Several employees stated that they enjoyed their work environment. Many identify with the organization and share the same beliefs and values of senior management. They are “willingly striving towards the vision of their senior management for information security” (Thomson & von Solms, 2004). This will contradict with what they will explain later.

The organizations' behaviour in checking employee compliance differs from one employer to another. Many employees believe that their organization does not check employees' compliance and it is up to the individual or group of people’s judgment, for example:

"I am not aware if they are taking [any], they do not contact me and say your files are secure or you comply with the requirements of the data protection act... not on a regular basis or any kind of updates. No, whenever we destroy files after a period of time we have to make a judgment, but we need a judgment with a consultation of data protection staff. So we get advice for that from archive.” Moreover, *"The department does not check, it is just up to the individual.”*

Others said:

"…We do not really get checked up on. They assume that people will keep things safe but no one comes to check".

Only some employees were sure whether their organization checked their compliance to policy

"It does, my supervisor checks the information that could be held and it's held in an appropriate way";

Another employee describes how this checking takes place in his organization:

"…there are two ways in which the policy is implemented. One is that there are physical checks, for example security might come at 10 o'clock at night and check people's disks and see if anything confidential is left behind then they can get caught that way. The second way is that the electronic transmission of that information is checked".

But the results also show that some organizations check on their employees' compliance only if there is a problem:

" No, unless there is a problem…"; or because some departments or units are setting their own policy as described *"… there is nobody as far as I am aware checking that we do things correctly and that's because we are in charge on policy".*

Many employees are aware of whom to report information security incidents to. In some organizations employees will discuss the incident first then take action:

"Depending on what the problem was if it was relatively minor we will discuss it around here within the group. If it is something major, things we can not handle, we take it to the division head then up to management depends on what the security problem is"; also *" I won't report it to anybody in particular unless they is an issue I feel needs further investigation or discussion."* Moreover: *"Recently, because of the office refurbishment, we are looking at removing a front counter which just lies out and it is serious if someone goes into this area they could get access to the cabinets. I discussed that with the head of central services security about what the implications would be for just making an open plan area that was not before restricted and we discussed that with approval for what we plan to do".*

Some employees believe that they have never been told to whom they should report:

"I do not know if I have been told to report to a specific person but I think if it is a work problem I will call support (who are in charge of technical problems in computing)". Moreover: *“I do not know but I will ask my supervisor definitely”.*

6.3.1.3 Compliance with Organization Security Policy

The interviews show some reasons behind employee non-compliance with information security policy in organizations. Figure 6-1 summarized the findings. Some of the answers for this section related to questions which were asked after showing employees a sample of security policy.

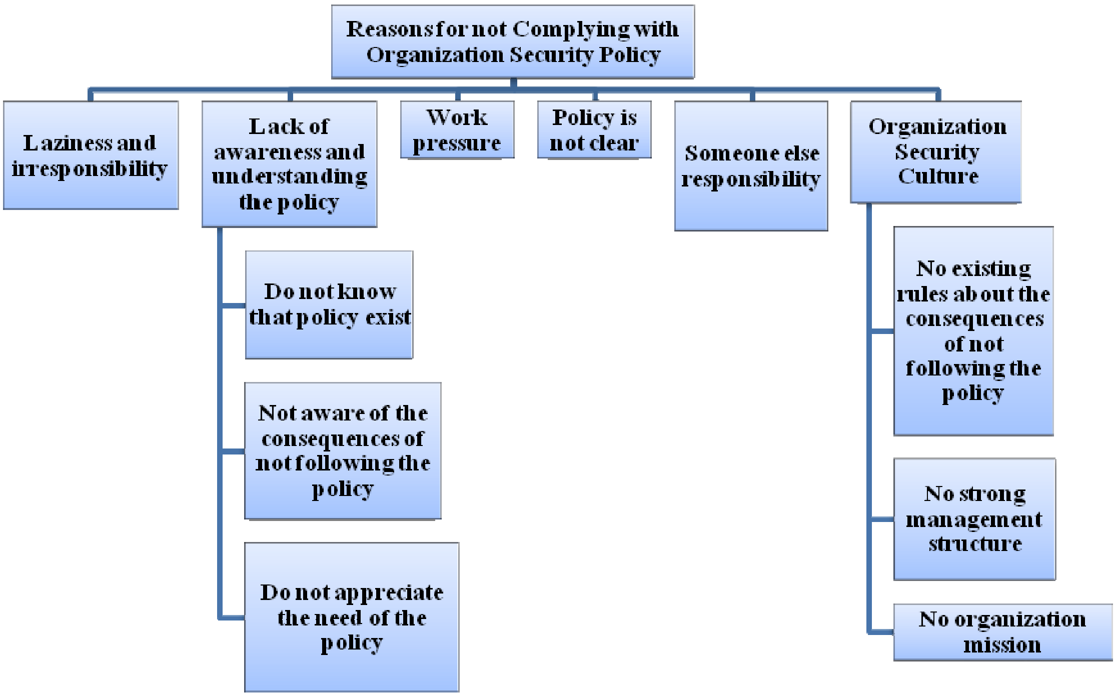

Reasons for not Complying with Organization Security Policy
Laziness and irresponsibility
Lack of awareness and understanding the policy
Work pressure
Policy is not clear
Someone else responsibility
Organization Security Culture
Do not know that policy exist
Not aware of the consequences of not following the policy
Do not appreciate the need of the policy
No existing rules about the consequences of not following the policy
No strong management structure
No organization mission

Figure 6-1 Reasons for Employee Non-Compliance with Information Security Policy.

Many employees claim to be willing to comply with their organizations' security policy. However, the result reveals some reasons that hinder compliance with policy. All of the employees expressed their views on what makes employees not comply with their organization's information security policy. These included laziness and irresponsibility.

"I think my ignorance about security policy is because there are people like MIS (management information services)";

Also another commented that they,

"could be careless in applying the system policy".

Some believe that they are skilled enough to bend the rules:

"a bit of laziness and a little of people thinking 'that won't happen' or they are 'too clever to allow it to happen to their machine' and sometimes people are frightened and do not understand how to set the computer up with the software". Also: *"Because they are crooked"*; and *"there are times if you have enough experience not to cause a problem you can manipulate things not to cause any problems but to deal with something that I would not advise an inexperienced person to do".*

Some related it to work pressure when jobs need to be done on time, as explained:

"Sometimes I want to do things that need finished. There have been times when I wanted to do things, maybe sometimes it is necessary to get things done".

Moreover, another response was: *"Overwork can be a problem, just too much to do at a particular time you are thinking of the paper record mainly where it is a time consuming task that might get delayed but that should not affect the security, but would holding on [to] information after that data protection people expect us to remove such information, but I do not see that as a serious failing".*

As well as:

"They are stressed at work they have too much work to do so it is something that can be ignored"; and: *" If staff require access to software to do their job the formal procedures are too time consuming and laborious and do not get software installed in the right time... I think it depends on having a procedure in place. That allows one to continue the work you have to do in a speedy manner".*

According to Spurling (1995), many people want to get their job finished and perhaps see controls and restrictions as needless bureaucracy.

Some related non-compliance to a lack of awareness and understanding of the policy, such as,

"Because they are not fully aware of the policy and they might not understand how important it is". Another said: *"It could be a lack of understanding of the system";*

Also, employees are not aware of the consequences of their organization's policy, for example, one responded that they were:

"Possibly unaware of the danger, possibly a burden as well not aware of security policy as well."

Another:

"they are not aware of the consequences of the importance of the policy"

Another:

“...either they are not aware of it and they do not say there is something wrong with what they are doing due to strict guidelines or they want people to follow and be more serious.”

Another:

“…they are aware of all these regulations but there is nobody telling them you must not do this or you must not do that.”

Another:

“they do not take it seriously”

Another:

"I am sure [it is] ignorance. Because I do not think we have seen something you would call security policy written anywhere. When you become a user of your information company's website [you] go and glance at that. Maybe we should have a hard copy of that somewhere in the office and make sure people are aware of it"; a

Another:

“They have not heard the information, they have not seen the information it has.”

Another:

“Employees do not know what exactly the organization policy is”.

Another employee explained that non-compliance could also be because that the policy itself is not clear:

“…if it were too complicated, too unclear to understand and whether the policy was not distributed among a number of different places”.

This is supported by a comment from one of the participants who noted that understanding the policy and appreciating the need for such policy makes him follow it:

"It's probably because I understand the need for it and I do not see there is anything in it that makes me say that it's stupid, I know the reasons for it".

This aspect was also explained by one of the end-users from the first investigation in Chapter Four, as commented:

"*Indeed if things are clear to us we know our rights and we know what to do and what not to do and this will make us follow the rules and the policy*".

Others see that compliance to the policy is for their own benefit in protecting themselves and their information as well as the machine's safety as evidenced by the following comment:

"This policy is to protect me." And to, "*Minimize the threat, I want also to protect my own machine data. For instance my machine knows who I am, knows about me, it has an idea where I live, it has an idea of my age, and my name. So there are reasons I do it for myself";*

Another answered: *"[I] suppose that's basic computer safety".*

One of the employees explained how some employees' behaviour is unpredictable even if the policy is working properly as commented:

"*Yes as far as I know, you can never guard against employees who want to make confidential information they have public*".

Other reasons for not complying could be related to the organization's culture as explained in previous chapters. If management is not paying attention to information security, employees may not take it seriously:

"I do not know, I suppose people do not think they will get caught. You know like copying a music CD and that kind of thing, people do that a lot, mainly because they do not have the facility at home. They do have equipment at work so they use work equipment".

Chapter Four also stressed the importance of management support to information security. The consequences of not complying are not clear or applied:

"People always think they know better, that they will never be caught. It is easier to do what you want to do, not what society wants you to do. They do not see the trouble of what they want to do. There is not a strong management structure nobody will bother".

Employees also offered explanations for why they comply with organizations' rules and regulations. Some employees explained:

"*If it came from the director directly to the head of department then we must follow this policy*"; "*it is the instructions from your supervisor that make you follow it. If somebody* *tells you to do it you will follow it*"; "*If it was the rule it was the rule. I guess if I do not see a problem with that*"; and "*It is an official policy, it is part of the rules you accept so you do not have a choice but just to follow it*".

The reason could be that employees cannot be an expert in everything. As one commented:

" The key part of any large organization is that you cannot do everything yourself but there are people who are experts with dealing with the press, there are people who are expert with dealing with security, people who are experts to deal with IT systems. So the individual is not expected to be an expert in all fields. In the majority of cases the individual employee does a fairly particular task which they do not anticipate or expect the employee to have very deep skills in all subjects related to that point".

One of the employees had a different opinion:

"I still believe that as a human you are capable of free thought and individual actions and if the company wants clones they can hire clones but I won't put myself in that category. I am an individual with free thought but I know where the line is, certain things you do not do. Sometimes you bend the rules a bit. It will depend on the circumstances whether it was not of a significant or serious enough nature to damage the company".

Another employee blamed technology for not being able to handle such situations:

"All computers should be protected with antivirus that is automatically updated on a daily basis through the university's server. You have to know the reason why the antivirus is not up to date. I think updating it always put behind a new virus coming out so if we get infected with something new and the antivirus can not cope with it; it is really not your fault. It is just how it happens".

6.3.1.4 Impact of Non-Compliance

The findings revealed some potential impacts of employee non-compliance with information security policy in organizations. Figure 6-2 summarized the findings.

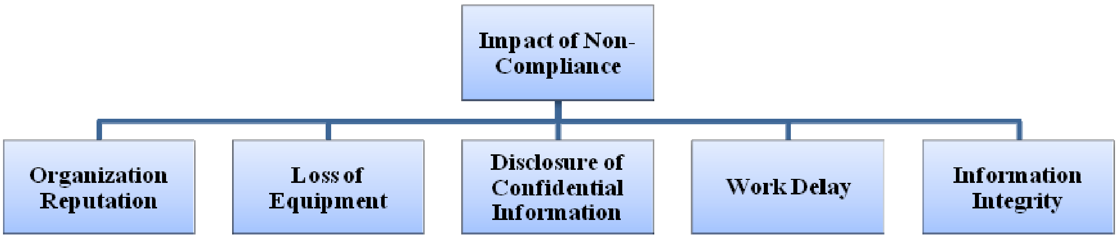


Figure 6-2 Impact of Employee's Non-Compliance with Information Security Policy.

Many employees identify the potential impact on the organization from not complying with the organization's information security policy. The organization's reputation may be affected:

"It can be from basically no impact to extremely severe. For example, a competitor having detailed knowledge about another company's product could have a major impact on that company's profitability".

Also it will lead to loss of equipment, as one employee said.

"Well we could have burglars, lose equipment; we would be open to sabotage, theft, it could cause a lot of problems".

Or a concern could be the disclosure of confidential information:

"Some ...documented leaks of information [happen] because we have confidential information about individuals which if we are not following our policy could get into the public domain."

It can be misused if it comes to wrong hands:

"it could allow data to be mis-appropriated."

It can be a total fiasco for network communication, as revealed by one of the employees:

"It would cause major damage to the departments. Departments now operate through networks that [if] destructed like that [means] we do not have other way to communicate. Particularly, a department like this will be remote in 3 locations [and] the only way we can communicate is by email".

The integrity of information may be affected:

"It could be disastrous if you have material in your database corrupted; since we are working individually for the benefit of our own research I think it is better to have a backup to accommodate that. Eventually, if you lost your own data no one else is to blame".

The results also show that some employees have no idea what impact non-compliance could have:

"*There is not really a lot of information that we have, it doesn't mean anything to anybody else because these are in numbers so unless there is somebody who knows what the project is about, then they will not able to interpret the results. If somebody else let this information out or it was given to someone, I really do not know what difference that will make".*

6.3.2 Scenario Based Questions

Employees are often faced with making decisions concerning security. This part of the study explores the opinions available to employees regarding typical activities with security implications within the organization. Scenario-based questions were used to explore the interviewee's point of view of other activities where a choice had to be made. The interviewees were asked to look at different scenarios on employees' behaviour. Scenario-based questions have been used in different studies. For example, Kreie & Cronan (1998) show that men and women view ethics differently. They use scenarios to ask participants whether a person’s behaviour was acceptable or not, and what factors influenced their judgment.

The employees were given an example of a serious information security incident (such as a virus occurring because someone clicked on an email attachment) in an area they have some responsibility for. They were asked what steps they thought should be taken to deal with the situation. Many employees said that they would not handle a security situation by themselves. They prefer experts to handle such situations

"I would like somebody else to deal with that, email support and tell them what is going wrong"; and *"We have our own information system department within the library. So we will contact them about anything like information security virus. They coordinate with what happens in the organization in terms of virus control [and] antivirus software, and so it is all consistent with what the university does".*

Some employees described their experience in similar situations:

"We had a problem like that and what we had to do was remove all the network computers from the network. I had to speak to the people in the IT services. They gave me a pin stick with virus check up and removal, we had to clean the machines and disinfect them and install new software with updates all from CD before going back online. That was the problem we went through".

But some employees would like to try by themselves to solve the problem and then if they fail to fix it they would then seek help:

"If I could. Funny you talk about that, two weeks ago I got an email saying an e-card was from a member of family. When I opened it I realised it contained a virus. Then I ran an anti virus and it seemed to be okay. If I cannot do that I will contact support".

At the end one of the employees asked the organization for support:

"*I am hoping that the organization's responsibility is to protect me from myself I suppose*".

In our interviews six different scenarios have been used to describe different activities in information security. Each scenario has been explained to employees with a request to give their opinion on people's behaviour in different situations. They were asked to explain what the employee should do?; why they should do it?; what they predict will happen?; and under what circumstances would employees be more inclined to do this activity?

Below is each scenario with a summary of participants' responses according to whether the behaviour is deemed acceptable or not acceptable followed by a discussion of each scenario. It has already been explained that the area of information security is sensitive in nature. Therefore a scenario was used that is question-based to give employees the freedom to give their opinion with no pressure to explain what they think about the mentioned different security activities. Each of the scenario questions is related to security activities all employees could be practicing in their organization. Security policy covers different issues, for example it explains employees responsibilities related to their login name and passwords or specifies if employees are allowed to use the Internet or not, and how they use it. Sometime these activities need decisions from employees. According to Schwiderski-Grosche (2006), employee security decisions have the potential for a security incident. These scenario based questions will help to reach the main objective of this research which is to investigate what the reasons are behind employee non compliance with an organization's security policy.

6.3.2.1 Scenario 1: Is it ok to Leave your PC Without Logging off when you are not Around

Your boss' secretary leaves her PC unattended when she leaves for a lunch break. She shares her office with other colleagues.

Employees gave different reasons for whether this activity is an acceptable behaviour or not. The Following Figure 6-3 summarizes the findings.

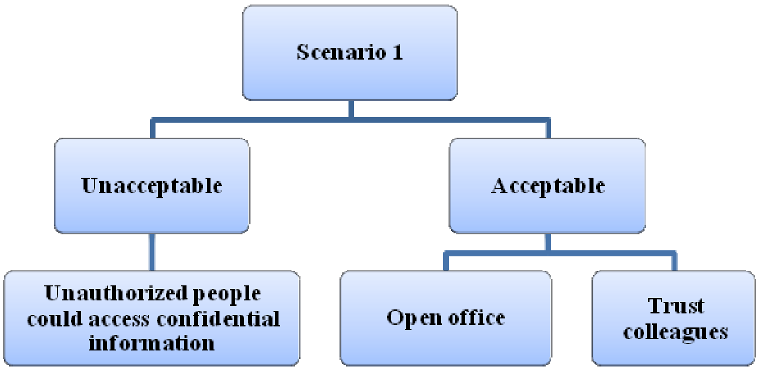


Figure 6-3 Scenario 1 Findings.

Acceptable behaviour:

- *"I do not think there would be any problem. If it is an open office, I do not know I leave my own (PC) on all the time, we share an office. They are trusting and do not go to look at it. Nothing will happen. If there is any problem say you are working in the exam paper, and students come in and out you will close the machine anyway";*
- *"I do not think there is anything wrong with it, I am quite strict; when I leave my office I lock the door but nobody else is in the room. I do not know if there should be something about the security of the building. Nothing. I do not know";* and
- *"Probably you will do that any way unless you do not trust. I feel it is difficult with this organization, it is not a business".*

Unacceptable Behaviour:

- *"She should ensure that a screen saver is functioning to put her password on. Or switch her computer off. Because she should be the only one accessing her computer using her own password. Somebody might use her machine or somebody might quickly have a look for some information. If they were very friendly and work closely together on similar job";*
- *"She should lock it. To avoid unauthorised people from accessing confidential information. Someone might come and access her PC. If she is aware of the issue";*
- *"You would normally log off your computer. Nobody else can have access to her computer. In this situation the people are honest enough so nothing would happen";*
- *"He should really close his machine down or have a screen saver which has a password in it so no one else views his data in his PC that could be confidential in nature. It's probably nothing but there is a possibility for someone to see his data. In this situation the people are honest enough so nothing would happen. I do not know, maybe if strangers around you need to be more careful to log off";* and
- *"Close down the PC log off and make sure his password is not known, it does not matter if you are friends with people. You cannot be 100 percent certain that you can trust them. Sooner or later someone will access information. Probably after it happens probably afterwards. I am sure 99 percent of people are honest. I would hope while her PC is running people will be there that she trusts, if they were not near it should be a locked door".*

Findings:

Many of the employees believe that this is unacceptable behaviour and believe the PC should be locked if the employee is not around. The possibility that someone will get access to something that they should not access is clearly a concern. The rest believe that there should be an element of trust between colleagues justifying why the secretary might not lock their PC when they are not around. Organizations should have technical solutions to such behaviour in forcing employees to add a password to their screensaver if they forgot to lock their machine, to avoid any disclosure of confidential information.

6.3.2.2 Scenario 2: Opening an Unknown Attachment

(Paul/Amanda) receives in his/her office an email with an executable file attached to it. He/She trusts the person the email came from.

Employees gave different reasons for if this activity is an acceptable behaviour or not. The following Figure 6-3 summarized the findings.

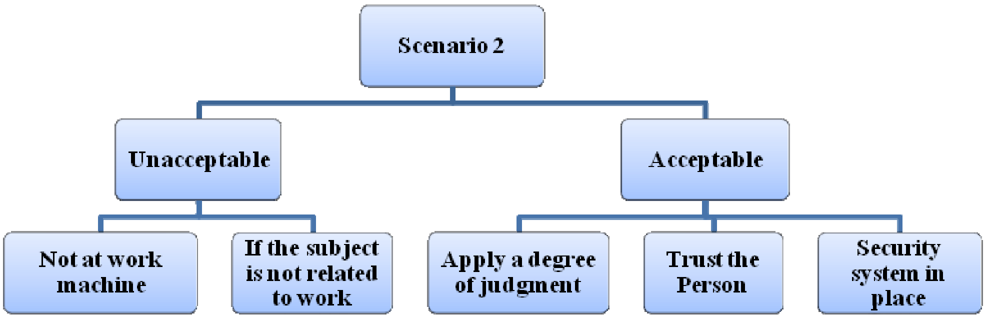


Figure 6-4 Scenario 2 Findings.

Acceptable Behaviour:

- *"Whether the individual is trusted is largely irrelevant in that context because what matters is whether or not he is expecting something from that person, for example, like a humorous video clip or it might be a piece of software. You have to apply a degree of judgment to the situation in that case. If you are not expecting it and it looks dodgy you won't do anything with it. If you are expecting then use it and if you are not sure you will ask. Knowledge of that person determines the action";*
- *"Open it as normal. The person must have sent it for a reason so you would want to forward the instruction of the emails. Somebody you know, you should be able to trust them to have the computer virus scanner and the person who sent it used virus software to remove any threat. If there is something suspicious in the heading then sometimes it not the right time to trust the email";* and

- *"I will say that your system should protect her against viruses, or whatever. And if you know the source of the email then if it were me I would open the file and hope that a security system is in place through the central admin setup. We are always getting or deal with warnings of viruses coming in attachments but I do think that we have screening that's why we have firewalls. But I do not know how secure things are in absolute terms and I know sometimes you are asked if you want to save it to disk rather than open something I am not even sure about the implication of that, if that means it is safer to do that. I think we accept that the protection system that exists to keep us right to stop any thing coming in that is doubtful in any way".*

Unacceptable Behaviour:

- *"She should not open it. Even though she trusts the person he/she or may not be aware that there could be a problem with that file. She will open it anyway. Just kind of being friendly and not being aware of possible friends and possible problems";*
- *"Probably not on the work machine. If he does want to run it take it away because you do not know who the other person trusts. You do not know where they got it from. So unless you have that information it is not worth being checked. Nothing will happen. 99 percent of the time nothing wrong will happen., if it was entertainment rather than work";*
- *"If its subject line is related to work he should contact the person to see if he sent the email and virus scan. Because it may possibly contain a virus. If it is a virus then it could damage a computer and affect the entire network. If it was a work related subject from someone trusted";* and
- *"Delete the file. Although you trust the person, you do not know who sent them the file. Many of these files are passed from one person to another, which is how my computer got affected. I opened a file which I should not have done. Eventually one of the files will be contaminated and will get a virus. Probably after it happens".*

Findings:

As the results reveal, many of the employees believe this behaviour is acceptable only if they trust the person who sent the email. Some offered ways to make sure that an email is not a virus by emailing the person who sent the email asking him/her if that email is from him/her. According to the interviewee, employees have to make their judgement and be responsible for their judgement. Also, the organization's security set-up can help employees to take decisions. Some believe this is not good behaviour on an organization’s machines if it is personal email. This could be because employees do not want to be blamed or responsible for any security incidents or they are aware that if the attachment contains a virus this will delay their job to be done.

6.3.2.3 Scenario 3: Giving your Password

(Chris/Stacy) is working on a confidential assignment assigned by his/her boss. He/she saved the work on his/her company PC. One day he/she was ill and could not go to work. His/her colleague phoned him/her asking about her password to get some files from his/her machine.

Employees gave different reasons for this activity being acceptable behaviour or not. The following Figure 6-5 summarizes the findings.

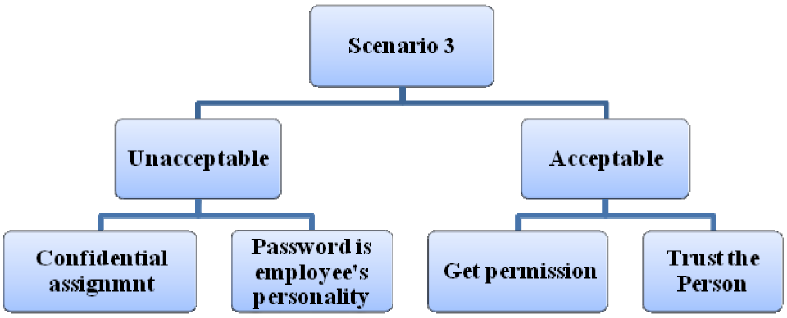


Figure 6-5 Scenario 3 Findings.

Acceptable Behaviour:

- *“If you have information you do not want people to see you can have it in locked files with different passwords. Only if she suspects they want it for any reason other than to access to the required file. If she does, well the person* *will be able to access the file, if she does not perhaps her boss will contact her and ask her for the password. When she is unable to go to work only if she thought the person looking for password for other reason to access her machine";* and

- *"Well I suppose company policy probably says you are not allowed to give out your password. I can understand from experience that people do trust people who they work with and would give them their password. You do trust each other; you do not expect them to give you viruses. That everything will be okay, I do not know".*

Unacceptable Behaviour:

- *"She should say no, you cannot access my computer. The assignment being worked on is confidential and the colleague might see it. She will probably give her password. If there are people who are friendly sharing the same item and if they are sharing the same boss she might feel it is acceptable risk giving her password to that person";*
- *"No he should not give his password, if his colleague can access his computer then he can access it with his own password but not his (Chris) password. Again it is about the data he has on his computer because he is working on a confidential thing nobody else should see his work. If he did not give him the password there should not be a problem. His colleague should understand that he is working on some confidential information; basically he should not ask him from the beginning. I won't see any circumstances but if there is one, it should be approved through his head manager but of course this should be documented for the future";*
- *"I do not think he should give it away, he should say no. The password is your responsibility and if you give it away to somebody else you take responsibility for what they do and do not really have control. So you will get in trouble for whatever they do. If it is really important he can give the password and he can change the password later. If it was really important";*
- *"Do not give him it, my boss asked me to give me his password I told him if it so important to do that you should make a backup and give me a backup. Every person should think of the scenarios [like] maybe I am going to be sick*

or maybe I am going to break my leg….. Get permission to do it from the head of the division"; and

- *He should not give his password out as the colleague would then have access to a lot of confidential information and there is the possibility that the colleague may misuse the password. If [it is] someone he trusts at work".*

Findings:

Many employees interviewed believe that it is not acceptable behaviour because there is a confidential assignment in the machine. One of the employees described the password as an employee personality (his machine has all his own information) which cannot be given out. The findings show that there are some circumstances where they would give someone else their password. This could be related to their boss' orders or trust with their colleagues. Others refer to the organization's culture when stating whether they would allow such behaviour or not.

6.3.2.4 Scenario 4: Write Down your Password

(Chris/ Rebecca) has too many passwords and cannot remember them. A friend tells him/her to write them on sticky notes and paste them inside his/her drawer.

Unacceptable Behaviour:

- *"By all means write them down but do not to put them in her drawer. Store them in a book where you may have phone numbers and have them coded in some way. Coded like you use your pin number of the bank and you can not remember it; make it as a phone number. Anyone could access them if the drawer is not locked and get into her machine. Any one could access [it]. Only if she does not have a good memory to remember her password. She can use the same password to her emails or machine to reduce the no. of passwords";*
- *"This is a very silly thing, I think, because you shouldn't write your password and put it in your drawers or even in your pocket. I consider it very, very dangerous; basically he seems careless. There are no circumstances will make him putting his passwords open to public and this is completely careless";*

- *"I probably wouldn't write them down. Again, your password is your responsibility. Your password identifies you to the system therefore you are responsible for whatever happens. I do not know, I am not aware of what the consequences could be. I think that 99 times out of 100 nothing would happen but the one time out of 100 when something does happen it is bad. I do not know, there are better ways to do it than that, do not write the password itself, write something to remind you or have one password*"; and
- *"Well to be perfectly honest she must record them somewhere in case she forgets them and she has got to trust to luck that no-one is going to find them. She should write them down but she could put them in a secure place like a lockable cupboard or something where she is confident no-one has access to it. Well, if they got access to it, it could create havoc and can you tell me what else you could do in these circumstances if she can not remember. She has to write it down, there is no other way if she can not write it down put it in her pocket and take it home with her. It is better than leaving it at the work place under lock and key. She will do it because she can not remember it".*

Findings:

As was clear from all of the employees' answers, this is not good practice. Employees were aware of the risks this activity could lead to. Also they offered some ways to avoid such problems such as having one password to all applications or try to code these passwords in such a way that would not be available to others.

6.3.2.5 Scenario 5: Illegal or Immoral Web Surfing

(Robin/ Sally) noticed that one of his/her colleagues was using the organisation's resources for illegal web surfing e.g. (porn surfing, email harassment). What do you think the organisation would want him/her to do? What pressures do you think he/she experiences in making his/her decision?

Unacceptable Behaviour:

- *"Either report it to her supervisor or have a word with the person, let them know that you know, if it is not stopped it will be reported. If she ignored the colleague's action and it was later found out she knew then she could be reprimanded";*

- *"They want her to report her colleague and this would be easier to do if done anonymously. She will feel pressure because if she reports it she will betray her friend but if she does not report it she will betray her employer";*
- *"It should be dealt with promptly and strictly to the relevant department in the organisation. I think he should consider this as protecting himself and his department and should report it. This also will help the staff himself to put him on the right track";*
- *"That's very simply a violation of the contract of the company so further disciplinary action should be taken. That would be a breach of security I would go to the security expert to deal with it. Depends very much on the relationship between the individuals, sometime in some instances you also have to bear in mind the cultures in different countries and differing levels of what is acceptable and what is not. What is the social level background on that activity and that varies from country to country";*
- *"Would expect her to inform them that this is happening, she could not do anything directly herself. I certainly wouldn't do anything myself, I would just inform the authorised people. I suppose the loyalty to that person and whether that person is a close colleague you do not want to be telling on your own friend or colleague";*
- *"Certainly report it; it is not acceptable and the organisation usually would have disciplinary rules. Very difficult to report someone for such things";* and
- *"The organisation would probably want him to report this situation. No-one would really want to put a colleague in a position to lose his job or be disciplined, it would be difficult, it would be a pressure on yourself".*

Findings:

Such activity was deemed unacceptable by almost all employees. This could be related to the clarity of this subject in terms of its illegality. From the interview employees insist on reporting such incidents for further action. This reporting could be done anonymously as the outcomes reveal. The most pressure employees might experience in such a situation is related to social factors. However, these opinions need not always prove an accurate indicator of actual behaviour.

6.3.2.6 Scenario 6: Opening a CD of Unknown Source in Work Machines

Some people are distributing CDs at central station early morning, saying that the CDs contain a special Valentine's Day promotion. (Chris / Rebecca) also got a CD there. What should he/she do with the CD?

Unacceptable Behaviour:

- *"If she knew it was from a reputable genuine source she could open the CD at work. She may not trust the source. If the policy says not to do it she should not do it although some people do";*
- *"He should throw it away. He does not know the source of the CD, it could be a virus, worm, or anything that could endanger his computer";*
- *"Probably bin it, but if he does want it, do not do it in the work machine. You are doing your best for the security of your organization which is not to do with non work related things";*
- *"Throw it away unless she is absolutely sure it is from a reputable organisation";*
- *"I suppose she should not trust the stranger that hands her that CD because it could be infected with viruses but it is okay to put it in her home computer but not at work computer. You do have the responsibility of not affecting your work computer then that's your decision to make or whether or not you trust the stranger giving the CD";*
- *"Straight to the bin. Could be full of viruses, Spyware. Any stuff you get from outside is not legitimate";* and
- *"Keep it until he gets home and play it in his CD player. If you use it in the work computer it may contain viruses you do not know and be unaware of how it might affect the computer or the network and could cause major problems. At home it is his own risk, before running it he should scan it and see if there is any problem with it but may not same of any way".*

Findings

The results show that all of the employees in our sample were aware of the consequences of inserting a CD from an unknown source into either a personal PC or their organisation's PC. From the interview, employees state they would not perform such activities. They know the consequences of such behaviour. Also they were aware that this activity is not allowed in work machines but that at home it is up to each person’s judgement.

6.4 Discussion

The results suggest that employees' activities represent a challenge to the security of the organization. No matter if they are an ‘expert’, more experienced or a completely unaware and uninformed employee. Unaware employee refers to not understanding the new technology that is involved in protecting an organization's assets or not understanding the security policy, or not being aware of such policy's existence, as well as the consequences of not following the policy. From the results the experts do know the rules; they do understand the policy and the risk of not complying with the rules but for them, as some explained, they think they know when to bend the rules.

Employees related the effectiveness of their organizational security policy to the level of breaches their organization is experiencing and their compliance to their security policy. The findings reveal that many organizations do not check their employees' compliance to the policy. According to Tomson & von Solms (2004), implementation of information security compliance is vital to protect organizational assets.

The findings revealed different reasons for employee non-compliance to organization security policy. Employees believe that their non-compliance to their organization's security policy is:

- **Someone else’s problem**: The results suggest that employees passively think of information security as someone else's job. As commented in the findings: "*I think my ignorance about security policy is because there are people like MIS (management information services)*". If a security breach occurs they often seem to believe it will affect the organization but not them. If they let in a virus then the IT technician will clean it up.
- **Individual values and beliefs**: The findings suggest that some employees do not like to handle security situations by themselves they prefer the experts to take care of such a situation. However, some employees would like to try by themselves to solve the problem and then if they fail to fix it they seek help. This could be related to an employee’s individual attitudes or personality; according to Posnser et al. (1987) people behave according to their attitudes and beliefs. Indeed this was

clear from the scenario based questions; the findings suggest employees themselves differ in their value classification. For some employees sharing a password is a clear violation of their organization's security policy. For others this behaviour could be seen as acceptable.

- **Work pressure**: Some related it to work pressure. In other words, when jobs need to be done on time they cannot comply with security policy. The goal of security policy is to protect information and the organizational system without limiting its effectiveness; the system should not be so secure as not to let the authorized employee get the needed information to carry out their job. Because employees concern more about finishing their job, so if security is going to delay their job they will by-pass it (Wood, 1982), and see controls and restrictions as needless bureaucracy (Spurling, 1995).
- **Lack of awareness**: Some related non-compliance to a lack of awareness and understanding of the policy. The findings suggest that employees do not know that a security policy exists in their organization and are not aware of the consequences of not following the policies as well as they do not appreciate the need of the policy. Zurko et al. (2002) stress that employees often are not aware of the consequences of their security practices. They do not understand enough about the impact of their security decisions.
- **Invisible security policy**: Security policy itself is not clear. A clear and visible information security policy will help employees to understand good security behaviour. Otherwise employees may try to find ways around security controls to let them do their job (Post & Kagan, 2007).
- **Organization security culture**: Organization security culture is how an organization handles its security. The findings suggest that there are no existing rules about the consequences of not following the security policy, no strong management structure and no organizational mission. Therefore, organization security culture plays a big part in making employees comply with their organization security policy. Though culture is difficult to study, Smith & Yetim (2004) believe that culture has an influence on the use of computer systems. The management role and organization mission has already been discussed in Chapter Four.
- **Trust**: Employees rely on trust in various aspects of security everywhere they use the organization's systems (Kaplan, 2007). The findings suggest that employees

often trust their colleagues, trust their organization’s web browsers, they trust their organization’s firewalls to filter spam emails, they trust their organization’s anti virus software and so forth. Chapter Four's findings show that employee trust is a reason for rule breaking, as commented: "*… we are human beings, we have a something called trust so sometimes we break the rules because we trust a colleague or a friend*". This trust may explain why some employees access email attachments where it could bring the risk of a virus. From the various descriptions of trust has been discussed in Chapter Two, section 2.8.1.1 and from the findings we can define organizational trust as: *the quality of an interest-based relationship controlled and managed by the experience of the individual characterized by the willingness of the individual to make him or herself vulnerable to another*. Trust need not be mutual, but the closer to mutual trust the individual gets, the closer the organization comes to a healthy working climate.

The findings reveal some impacts of non-compliance with organizational security policy and these can be summarized as follows:

- **Reputation of organization**: loss of information could be embarrassing to an organization. Organizations can face serious financial and legal implications if their information assets have been compromised (von Solms & von Solms, 2004).
- **Loss of equipment**: when organizations lose equipment this will lead to a delay in work; equipment may have critical software for certain tasks.
- **Privacy**: leakage of employee information can result in very serious risks to the organization (Kudo et al., 2007). These risks might result in financial loss or lawsuits against the organization (Cooper, 1984).
- **Work delay** (functionality): organizations are dependent on information technology to share information and other resources in order to get work done (Loch et al., 1992). Once employees fail to comply with policies this could cause the breakdown of their organization’s network and will lead to work delays.
- **Integrity of information**: Information is needed in decision making processes. If such information is not correct, organizations might reach unwanted decisions (Posthumus & von Solms, 2004) such as financial loss or organization reputation.

Non-compliance affects confidentiality, availability and integrity. Organizations need to encourage compliance with their policy to avoid such results. The literature suggests some keys issues:

- **Appreciate the Policy**: employees need to *appreciate* the policy which is defined for their organization. The findings from this research suggest that employees who understand the need for the security policy will help them to comply with organization's rules and regulations. The organization must make the policy values meaningful for their employees' daily activities. Employees must appreciate and understand security practices, help them and allow them to think of security and identify threats and vulnerabilities (Nijhof et al., 2003). It can also help them to mitigate damage by policy training and education for employees (McIlwraith, 2006).
- **Feedback and Incentives**: Neal & Griffin (2002) and Luker & Petersen (2003) stress that feedback and incentives can increase an employee's sense of responsibility, which will enhance the sense of attachment to the organization (Van Dyne et al., 1994). Feedback helps to pinpoint possible areas of weakness so they can be dealt with before an incident happens (Thrasher, 2003). Feedback was discussed in Chapter Four and from the findings it appears that feedback helps organization to improve security through sharing employee experience, reviewing organization's security and increasing confidence between all employees in the organization.
- **Awareness Programme**: If the problem is lack of knowledge or skill, the organization's awareness about understanding an employee's personal value is essential to close the gap between the person's values and work requirements (Finegan, 1994). Educating employees is a critical step in securing an organization's assets. Learning to identify and work without security incidents will enable employees to complete their work safely and efficiently (McDowell, 2006). McIlwraith (2006) suggest some methods that any organization could embrace to help increase employee awareness through education and training in security, like web based media, booklets, posters, leaflets, etc... Each organization could accommodate what is a suitable method according to their budget and the objectives of the organization.
- **Rewarding and Punishment**: organizational policies do not always associate punishment with non-compliance (Kessler, 2001). Reason (1997, p. 212)

summarises the effectiveness of this key in the safety field and it can accommodated in information security. Reason argues: "*rewards are the most powerful means of changing behaviour, but they are only effective if delivered close in time and place to the behaviour that is desired. Delayed punishments have negative effects: they generally do not lead to improved behaviour and can induce resentment in both the punished and could-be-punished*".

6.5 Conclusion

No matter how good an organisation's security policy is, the behaviour of its employees towards the information security systems put in place by that organisation can challenge the protection of their information assets (Thomson & von Solms, 2004). There is no point in an organization having a good policy with no possibility to monitor and enforce compliance to such policy (von Solms & von Solms, 2004). For organizations it is critical to be able to always monitor and measure the efficiency of their compliance program (Thrasher, 2003). To monitor compliance, and act when there are any inconsistencies, could be done through using technical and non- technical measurement tools. These measurement tools should not be dependent on annual or semi annual internal audit.

This chapter has highlighted some possible barriers that hinder employee compliance with security policies. Some recommendations have been offered to help organizations to encourage their employees' compliance. These barriers are made up of accounting for some one else's problem; individual values and beliefs; work pressure; lack of awareness; invisible security policy; and organizational security culture.

Understanding what makes employees make security decisions which might cause a security breach may help to develop security policy. It might help employees to practice security comfortably with no need to bypass organizational security controls.

The subsequent chapter will bring together what has been found from the results of the three investigations by suggesting some practical policies.

Chapter Seven

Consolidation

The purpose of this chapter is to bring together what has been found in the results of the three investigations and the literature analysis with some real life policies. What has been found is issues that security policy needs to cover, and also the criteria necessary to make the security policy effective. This chapter will give recommendations about how to formulate a security policy to encourage compliance and therefore reduce security incidents.

Four policies from different organizations in the UK have been used. These policies are from different types of organizations located in the UK. Each of these organizations provide different services. Three of these policies were available from the internet and one was provided by one of the employees of the organization. Copies of the policies are found in Appendixes F (p. 277), G (p. 283), H (p. 293) and I (p. 296).

7.1 Introduction

In Chapter Two, section 2.6.3.1 and 2.6.3.2 discussed the contents and the criteria of an information security policy. The findings from the three investigations reveal that adoption of the information security policy needs to fit the organizational culture. The results suggest that information security policy should be reviewed and updated frequently and that the policy needs to be straight forward, easy to use, and clear to understand. Analysis of the research question R10 concludes that the more issues the organization covers in their security policy the more effective their policy will be reported to be. Analysis of the research question R11 concludes that the more an organization reports adoption of criteria, the more they report a highly effective security policy.

No existing rules about the consequences of not following the policy and no organization mission were two of the reasons why employees are not complying with their organization security policy.

The aim of what follows is to cover what has been discussed above and check whether these criteria or issues are present in the four security policies covered. A recommendation will then be given about how to formulate a security policy to encourage compliance by employees.

7.2 Methodology

The approach adopted is to go through all the criteria that the security policy needs to cover and check these criteria with the available four policies. With the help of the literature and the findings from the previous chapters each criteria will be explained to aid an understanding of how to formulate a security policy. Each of these criteria will be looked at individually and then it will be checked if such criterion is offered in each of the four policies. There are no available metrics that could measure each criterion and provide a clear way to follow. This work could offer the first step to recommend developing metrics to measure these criteria in security policies.

What is going to be explained below is how the criteria can be used to formulate a security policy. Examples of some existing policies will be used to check for the criteria of the security policy and then recommendations will be made.

7.2.1 Fit the Organizational Culture

The security policy of an organization mostly depends on the common organizational culture. From the literature it has already been explained that there are three different types of environment that could be found in organizations. According to Thomson & von Solms (2004) these environments are coercive, utilitarian and goal consensus. A coercive environment is when employees perform tasks because they must do so, rather than because they agree with the actions and decisions of senior management. A utilitarian environment is one in which employees will do as senior management wishes because of an incentive system and not because they necessarily agree with them. Finally, the goal consensus environment is when employees identify with the organization and share the same beliefs and values of senior management. They willingly strive towards the vision of their senior management for information security in the organization. Hale (2000) explains that organizational security culture deals more with attitudes, beliefs, and perceptions shared by employees as defining norms and values, which determine how they respond in relation to threats. Section 2.7 discusses organizational information security culture in details.

Organizations differ in their security requirements. What is suitable for one organization may not be suitable for another. From the four policies each policy covers different aspects in terms of what activities the organization needs security controls for, to meet organizational objectives. It is not easy to check if the policy fits the organizational culture or not from these policies themselves. Many aspects needed to be considered like knowing the organizational perspective, activities, security aims and so forth.

The main issues that any policy needs to include, as explained in section 2.6.3.1, are: User Login Responsibilities, Use of Organization System & Network, Internet Access, Viruses, Worms & Trojans, Disclosure of Information, Definition of Responsibilities, Email Usage, Adoption of some Laws, Personal Usage of Organization Resources, Explaining the Consequences of Violations and Breaches, and a Feedback System for Suggesting Policy Improvements. Figure 7-1 below describes these issues in organizations.

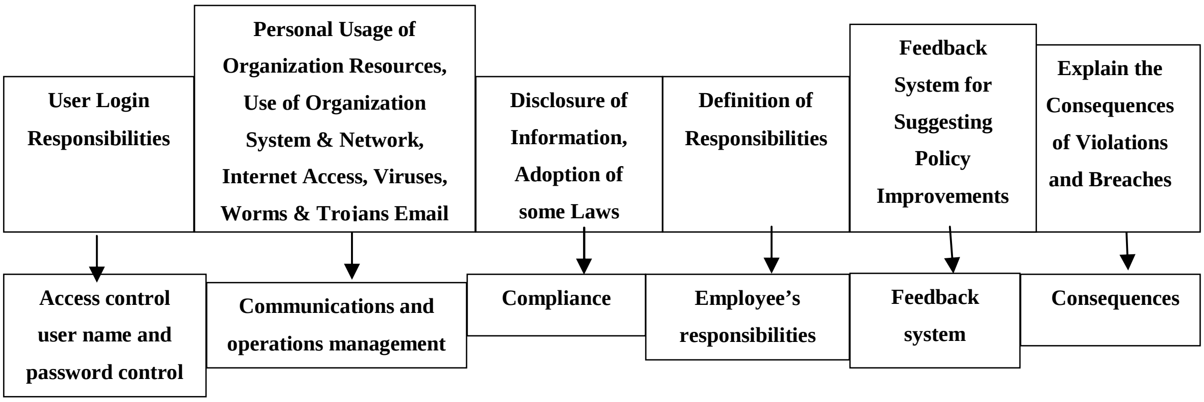

User Login Responsibilities
Personal Usage of Organization Resources, Use of Organization System & Network, Internet Access, Viruses, Worms & Trojans Email
Disclosure of Information, Adoption of some Laws
Definition of Responsibilities
Feedback System for Suggesting Policy Improvements
Explain the Consequences of Violations and Breaches
Access control user name and password control
Communications and operations management
Compliance
Employee's responsibilities
Feedback system
Consequences

Figure 7-1 Policy Contents.

Some of these issues, for instance user login responsibilities, determine access controls in the organization, such as Internet access, use of organization resources, email usage, etc, describing to employees what activities they are allowed to do and what they are not, as well as explaining employees responsibilities related to these issues. Other issues, like explaining the consequence of violations and breaches, are to describe and explain to employees what the consequences of failing to fulfil their organization's policy. Defining responsibilities means directing employees to where security breaches and violations are reported. Adoption of laws is to tell employees that the organization is complying with the appropriate legislation. A feedback system for suggesting policy improvements is to address how employees could input and communicate regarding information security policy improvement.

Checking with the four policies in this research work, it has been found that these policies cover all the mentioned areas, but not all of them cover the feedback system for suggesting policy improvements. The following is a description of what the policies are covering regarding feedback.

- **A Feedback System for Suggesting Policy Improvements**: this section addresses how employees could input and communicate regarding information security policy improvement.

Policy A:	All staff are expected to bring new security threats, often identified during or as a result of security awareness training, to the attention of management so that this security policy can be updated as appropriate.
Policy B:	Nothing.
Policy C:	Nothing.
Policy D:	Staff shall declare any potential conflicts of interest as required by the organisation’s Standing Orders.

In policy B and C nothing is mentioned about feedback system where employees could input opinions regarding their organization's security policy. Policy A did state that employees are requested to bring any new security threats for updating. Policy D did mention something important here: if the policy conflicts with an employee's interests then they need to bring it up. It needs more explanation on the reasons for such a declaration in order to give more weight to such activity.

Policy A goes into more depth in explaining the feedback system. However, they could also add one or two more sentences instructing that if the policy contradicts itself or is difficult to apply, employees need to bring it to the organisation's attention. At the end it is the employees in the organization who are implementing the security policy.

What has been explained previously about the importance of a feedback system in security policy in Chapter Four and Chapter Six needs to not be ignored in implementation. The feedback system needs support from the management to encourage smooth employee engagement in such activities. When employees share their point of views about the policy it will help in reviewing and updating the policy. Employee awareness and evaluation will help them understand and implement the feedback systems effectively. Going back to the security planning figure in Chapter Two, Figure 2-4, and the feedback system could be illustrated as Figure 7-2:

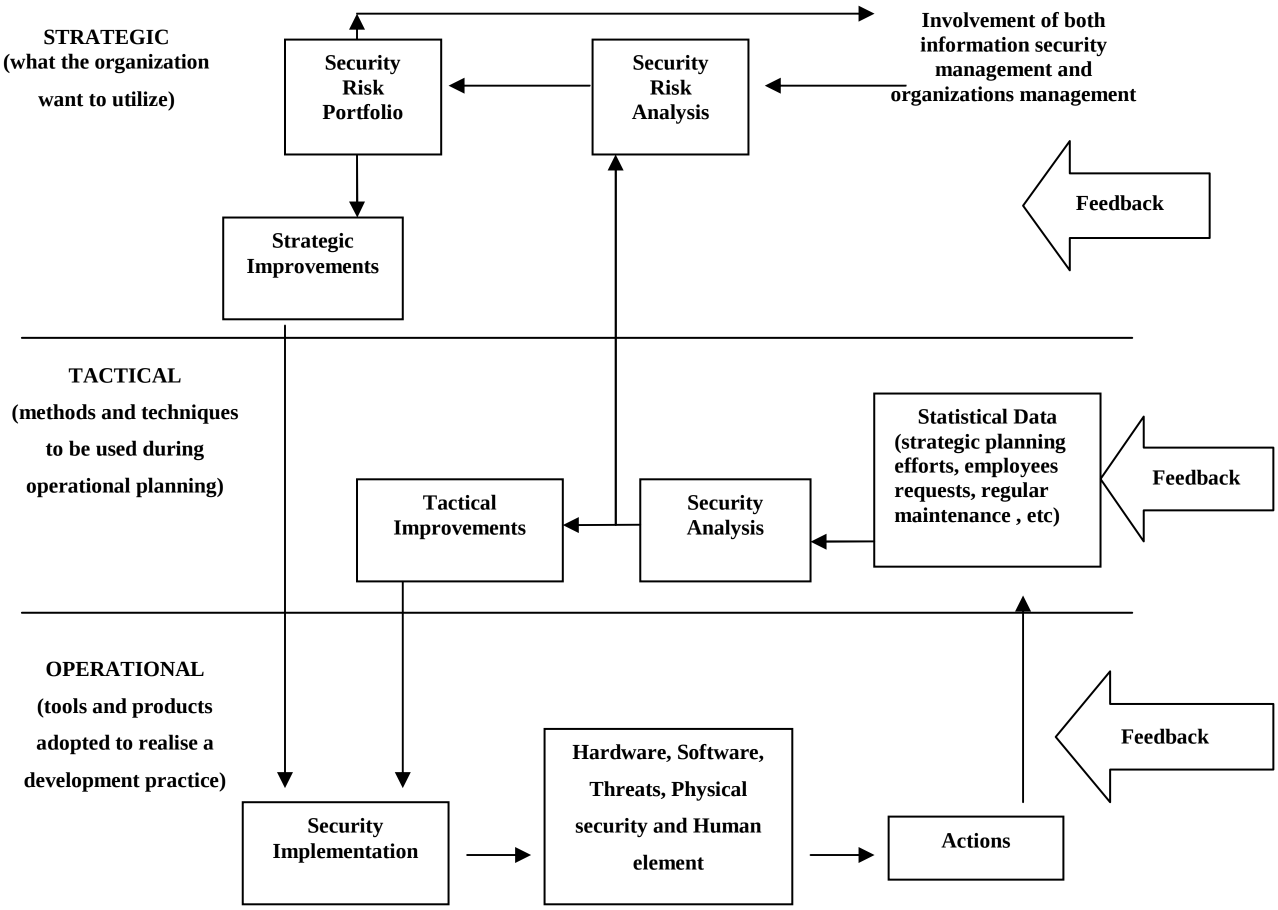

STRATEGIC
(what the organization want to utilize)
Security Risk Portfolio
Security Risk Analysis
Involvement of both information security management and organizations management
Feedback
Strategic Improvements
TACTICAL
(methods and techniques to be used during operational planning)
Statistical Data (strategic planning efforts, employees requests, regular maintenance , etc)
Feedback
Tactical Improvements
Security Analysis
OPERATIONAL
(tools and products adopted to realise a development practice)
Feedback
Hardware, Software, Threats, Physical security and Human element
Security Implementation
Actions

Figure 7-2 Feedback System Loop in Security Planning.

During security planning in an organization feedback can take place at each level (strategic, tactical and operational). Each stage of the security planning presents a corresponding security practice. More about this security planning is described in section 2.4. The arrows in the above figure indicate the feedback system loop in each stage.

7.2.2 Have a Style which is Consistent with the Organization’s General Communication Style

To assess a consistent style there is a need to compare the organization’s usual style with that of the security policy. This is very difficult to do as it is hard to access these organizations' other documents. Grudin (1989) suggests that consistency is an unreliable guide, therefore looking for the consistency within the policy is not important unless it causes problems in the security of the organization. Ortalo (1998, p. 69) states that "*the security policy is consistent if, starting from a secure state one cannot reach an insecure state without violating the security rules*". Ortalo discusses the different types of potential inconsistency in the security policy, in that: security purposes may be contradictive; security regulations contradict each other; security regulations fail to enforce the objectives of the policy; and organizations' operation regulations conflict with the security objectives.

Using Ortalo (1998) it is only possible to check one of the types of inconsistency, that being that the security regulations of the policy contradict each other. The other types require knowing more about the organizational environment: how the organization enforces the policy, how they check the implementation and how organizational security mechanisms work with the security policy.

Policy A states that :

> Policy A: **1.4 Laptops/portable and hand-held computers/remote use**
> Each individual is responsible for the portable computer they use and must ensure that the correct procedures are followed.
> 1.4.6 Do not display sensitive information in a public place where the screen could be overlooked.
> 1.4.7 No sensitive information should be held on the hard disk.
> 1.4.8 Any removable/transportable media containing sensitive information should not be held with the computer.

From the above activities it shows that in point 1.4.6 employees are allowed to have and work on sensitive information on their portable computers. The rest of the two points 1.4.7 and 1.4.8 contradict the previous rule which does not allow any sensitive information on the hard disk of the computer or even any removable media. This shows inconsistency in the policy which might result in confusing employees while practicing security.

The rest of the policies do not show any contradiction between rules.

7.2.3 Be Effective and Dynamic

Effectiveness of the policy is not simple to measure as security is a complex issue. The sensitive nature of information security might make the organizations reluctant to disclose the number of security breaches that they are experiencing. Anderson & Moore (2008) clarify that there is a shortage of statistics about information security failures as many of the available hard data is collected by different parties that have a big interest in reporting, such as security sellers or law enforcement agencies.

In Chapter Five, analysis of the research question R10 concludes that the more issues (i.e user login responsibilities, internet access, feedback system, etc) organizations cover in their security policy the more effective their policy will be reported to be. Analysis of the research question R11 concludes that the more an organization reports adopted criteria in their security policy, the more they report a highly effective security policy. Analysis of the research question R12 suggests that the more the organization implements the 'success factors' the more effective they feel security policy will be. The findings show *reported* frequency of breaches compared to *reported* attributes of security policy. This is because the sensitivity of the subject of information security could make the participants unwilling to say what they do or what they truly believe. Therefore the effectiveness of security policy cannot be explained by a single framework. The findings help to understand what makes an effective security policy.

What cannot be assessed to a scale is the effectiveness of the policy. If the above results applied to the four policies then all of the policies can be considered effective because all the four policies cover different issues. But which policy is more effective than another policy is not easy to measure. The other framework to make an effective security policy is what analysis of R11 suggests but at this stage it is hard to measure because each of the criteria that has been examined in the four policies does not show the same results. For example, not all of the criteria are available in the four policies. What analysis of R12 suggests is also not easy to implement with the four policies because it needs more information about the organization, for example how the top management work with information security and how much the organization budget is spending on information security. Whatever has been discussed about the effectiveness of the policy shows that although the analysis of the three research questions (R10, R11, and R12) that suggest what makes an effective security policy, it is not easy to assess the effectiveness of the policy. This indicates a need for more work to be done on the effectiveness of the policy.

To assess the effectiveness of the security policy is not possible; therefore this section will discuss mechanisms to ensure dynamism in the policies.

The dynamics of the organizational policy should be revised and changed regularly. The minimum period of time should be six months or less to avoid any threats from happening again as well as to help define new threats (Barman, 2001). Below are four explanations about the effectiveness and dynamics of the four policies.

Policy A: This policy is communicated to all employees on joining and should be implemented in conjunction with security awareness training made available to all staff. All staff are expected to bring new security threats, often identified during or as a result of security awareness training, to the attention of management so that this security policy can be updated as appropriate.

The company may alter this IT and security policy from time to time where required to reflect changes to the configuration of its systems and applications and to ensure its continued compliance with statutory and other legal requirements. You will be notified of any material changes to this IT and security policy from time to time. **September 2004**.

Policy B: The I.T. policy document is intended to be a living document, which will be updated, as and when necessary. Sections and appendices can be added to reflect new or amended procedures and guidelines when determined. **3 Oct 2002.**

Policy C: 5. Security Policy

This section deals with how staff will be made aware of the policy and how the policy will be reviewed and updated:

• Dissemination of the policy will be through the publication on the intranet together with summaries targeted at specific audiences and by providing training

• Reviews will be undertaken annually and, if necessary, updating will follow organisational changes or the identification of new risks. **31 March 2008**.

Policy D: All staff shall receive appropriate training and regular updates in organisational policies and procedures.
All staff shall be given an annual update on IT security. **24/2/2006.**

All the policies state in different words that their policy will go through updates. From the literature and the findings, threats come in different forms. When an organization is secure today it does not mean it is secure tomorrow (Schneier, 2001).

Only one policy from the above policies is updated, which is Policy C. This gives an indication that the organization is serious about information security and at the same time it shows that the process of security policy is ongoing. There could be some other documents or information included in the updated version of the policy but unfortunately it is not available on the Internet.

Employees will take information security seriously when their organization is taking it seriously (Neal & Griffin, 2002). This is one of the major problems with security policies: though organization's state that policy needs to be updated, unfortunately some are not putting effort into following this up, which in the end might effect employee compliance. Management following-up measures, such as auditing, help to force the IT department to update the policy.

7.2.4 Easy Language

The policy need not be a technical document, but should use simple language to ensure it is not difficult to understand. It should be free of jargon or technical terms, easy to understand and use solid rather than abstract language. To check the simplicity of the security policy's language there is some software available such as Flesch-Kinkaid grading score, Lexical density Exception lists and the Fog Index (Webography, 2008). To check the simplicity of the four policies, the Fog Index metric (FogIndex, 2008) has been used because free software is available which can be used to determine if the documents are written at the correct reading level for their target audience.

The Fog Index is usually used by people who want their writing to be read easily by a large section of the population. A Fog Index result number indicates the number of years of formal education a person needs to easily understand the test. For example, if a text has a Fog Index of 12 it means that it can be read to a wider group of people. Above 12 is too hard for most people to read. To use Fog index there is a formula:

Fog index = ((average number of words per sentence) + (number of words of 3 syllables or more)) * 0.4.

The steps to use the software involve highlighting text, copying it and then pasting the text in the provided box. Finally, click the 'Calculate the Fog index' button to get a result.

Checking with Fog Index, these result came out:

Policy A: “Fog Index: 11.90
Recommendations: Your text is very readable. Some experts advise to keep your fog index of 13 or lower while some others advise to keep it less than 10. It all depends on your audience. While college level should be around 13, for younger readers you may want to have it much lower than that. Fog Index more than 13 should be at least revised in search for reduction of the index”.

Policy B: “Fog Index: 12.51
Recommendations: Congratulations! The review of your text shows that it is equivalent to the articles of the Wall Street Journal and first year college. In other words, your text appears readable and it seems to be at college level”.

Policy C: “Fog Index: 21.21
Recommendations: You fog index seems a little high. TIPS for improving your writing and reducing the fog index:
1) Write short sentences. Most sentences may be written with 18 words or less. You may consider breaking down a sentence in two if that still keep the logic of your statements.
2) Replace long words (3 or more syllables) with smaller words. Applying these two cited actions will reduce your fog index and your text will become more readable”.

Policy D: “Fog Index: 10.33
Recommendations: Your text is very readable. Some experts

> advise to keep your fog index of 13 or lower while some others advise to keep it less than 10. It all depends on your audience. While college level should be around 13, for younger readers you may want to have it much lower than that. Fog Index more than 13 should be at least revised in search for reduction of the index".

The Fog Index test shows that policy A and D have scores less than 12 which indicates that a policy is readable by a wider audience. Policy B's reading level is first year college level, while policy C's reading level is a little high. Therefore, organizations when writing their policy need to make sure that it is easy to understand for all the employees in the organization. A feedback system is vital to improve this issue where employees can bring to attention that the policy is difficult to understand.

Farrell & Farrell (1998) state that language usage should be a major consideration in the writing security policies. They also mention that this is important because of the influence language has either to restrict or empower viewers. The purpose of the security policy is to guide employees' present and future actions (Murphy, 1989). Coates (1990) states that using "must" shows confidence in the proposition and "may" suggests a lack of confidence. Wood (2005) states that policies use definitive words like "must not", or "you must" or other equivalent words which express both certainty and unquestionable management support.

Therefore, organizations need to use a solid language rather than an abstract language in their security policy, to clear up any confusion for the employees in following the policy. For example,

Policy A states: 1.3.4 You must keep your passwords confidential and change them regularly. You may not disclose them to anyone, including IT staff.

The first part of the sentence is solid; employee passwords must always be confidential and changed regularly. The second part of the sentence is an abstract language, "you may not" leaves a possibility that employees will disclose the password. Giving the employees the option to do or not to do in situations that require protection is a big risk and dangerous. A threat such as social engineering is possible and there is a chance that any employee could disclose their password. The policy should use the same style and state “you must not disclose them to anyone, including the IT staff”.

7.2.5 Specify the Job Responsibilities

This criterion is about employee job responsibility. Describing the responsibilities of employees will allow employees to find out what their responsibilities are and what they are required to do to follow their organization's security policy.

Policy A: 1.2.1 It is the responsibility of each user to take all reasonable precautions to safeguard the security of the computer and the information contained upon it. This includes protecting it from physical hazards, including spilling liquids; not allowing unauthorised users access to the machine; and only using approved software.

Policy B: 4. Staff should take responsibility for the physical security of their Computer Equipment within their working environment. Windows and doors should be kept shut whilst unattended.

Policy C: It is the responsibility of all users of the network to adhere to the policy.

Policy D: 3.3. Staff responsibilities
1. Staff shall ensure that no breaches of security result from their actions.
2. Staff shall declare any potential conflicts of interest as required by the organisation’s Standing Orders

All the four policies state the responsibility of their employees to the organization's security policy. Policy A focuses more on user actions as employee responsibility. Policy B focuses more on the physical security of employee computer equipment. In policy D the employee responsibility is about ensuring no breach results from their actions. This shows that there seems to be a distinction between physical security and employee action. Any security policy covers different issues related to an organization's security need and when it comes to employee responsibility it is not only complying with one issue or another. Employee responsibility is about complying with the policy as a whole.

Policy C stresses that compliance to the policy is an employee responsibility. It is important to mention that compliance is vital and is a responsibility of all employees in the organization.

There is no excuse in not following or complying with organization security policy. The consequences of not following organization security policy need to be considered. This section in the policy describes and explains to employees what the consequences of failing to fulfill their organization policy are. Checking with the four policies this is what has been found:

Policy A: Persistent breach of this IT policy and/or misuse of the company's IT facilities is a disciplinary offence and, in appropriate circumstances, will lead to disciplinary action being taken against you, including summary dismissal.

Policy B: Any breach of the security policy will be investigated and may result in the individual being subjected to the Company’s disciplinary procedure. Councillors breaches will be referred to the Companies Standards Committee.

Policy C: I (Manager) expect and require all staff to adhere to the policy. Failure to do so may result in the use of disciplinary procedures as appropriate.

Policy D: It is a criminal offence to make or use unauthorised copies of commercial software and offenders are liable to disciplinary action.

All the policies somehow explain the consequences if a breach of the security policy occurs, except for policy D where the only offence requiring disciplinary action is related to making unauthorised copies of commercial software only. This needs to be clear to all the employees: not following the policy will lead to some disciplinary actions. One of reasons that employees do not comply with security policy (more information in Chapter Six) is that the consequence of not complying or violation is unclear. There are also ambiguities here, for example policy A uses the term “persistent breach”, but what does persistent really mean, five times or twenty times? Also, policy C says “may result” which indicates that the organization may possibly apply such consequences and this makes employees not take compliance to their organization security policy seriously.

7.2.6 State the Purpose of the Policy and the Scope of the Organization

The policy has to state the reasons for the policy, and what the organization aim is, to let the employees understand the benefit of such policy. This will help them appreciate the policy. The purposes of the covered policies are stated as:

Policy A: The purpose of these guidelines is to ensure that all of the company's users use the company's IT facilities in an effective, efficient, and ethical manner, and also to avoid the risk of the company and individual employees facing legal liability as a result of improper use, whether inadvertent or deliberate.

Policy B: PURPOSE OF THE SECURITY POLICY

1. The purpose of the policy is to provide a set of rules, measures and procedures that determine the Company's commitment to ensuring that its I.T. (Information Technology) resources are protected from physical and logical risk.
2. The main objectives of the policy are:-
   - ❑ To ensure that all the Company's assets, Staff, Councillors, data and equipment are adequately protected against any action that could adversely affect the I.T. services required to conduct the Company's business;
   - ❑ To ensure that Staff and Councillors are aware and comply with all relevant legislation and Company policies related to how they conduct their day-to-day duties in relation to IT.

Policy C: The purpose of the information security policy is to protect the Company, its staff and public from all information security threats, whether internal or external, deliberate or accidental.

Policy D: The information that Company D holds represents an extremely important and valuable asset. It is essential that this information is

> suitably protected from a wide range of threats in order to preserve confidentiality and to ensure continuity of service.

Considering the policy purposes above, policy D is not stating purpose clearly, unlike the rest of the policies. Not clearly mentioning the reasons for the policy makes it ambiguous for the users to use the organization resources accordingly. Information security policy needs to state directly, "the purpose of the policy is…" as this will make it easy for employees to get to the point rather than reading between lines. Policy B gives a good example by having a section called 'purpose of the security policy'. Policy C adds more weight to protecting its staff from security threats. This will make employees feel that protecting organizational assets is their responsibility because their organization cares about their security too.

7.2.7 Explain what Activity is Acceptable and what is not

In this section the policy gives details to employees on what is acceptable behaviour and what is not. Security policies cannot prescribe how employees should behave in every possible circumstance they may come across (Leach, 2003). Schneier (2001, p. 493) insist "*more security isn't always better*", giving an example of shoplifting at department stores happening mostly in dressing rooms. These departments could improve security by removing dressing rooms, but the losses in sales would be worse than the gains toward by a reduction in shoplifting.

Employees cannot avoid making security decisions in their daily work as Leach (2003) explains, suggesting that security policy needs minimum cover situations where applying a particular process properly is vital.

Password policy will be used to illustrate this issue of the policy, because a password is the magic word to access an organizational system. Each of the four policies describe password activity as the following:

Policy A: 1.3 Passwords and security

> 1.3.1 You are responsible for the security of your terminal, PC or laptop and for protecting any information or other data used and/or stored on your terminal, PC or laptop.
>
> 1.3.2 You must not make copies of system configuration files for your own, unauthorised personal use or to provide to other people/users for unauthorised uses.

1.3.3 You must not allow your PC/terminal to be used by an unauthorised person.

1.3.4 You must keep your passwords confidential and change them regularly. You may not disclose them to anyone, including IT staff.

1.3.5 When leaving your PC/terminal unattended or on leaving the office, you must ensure that you log off the system to prevent unauthorised users using your terminal in your absence.

Policy B: 1. Users are issued with guidance on good password management within the ‘Good Practice for Computer Users’. The guidance advocates the following:-

- Keep passwords confidential;
- Avoid keeping a paper record of passwords;
- Change passwords wherever there is any potential compromise in security;
- Select passwords with a minimum of six digits;
- Avoid basing passwords on potentially guessable formats;
- Change passwords regularly.

Policy C: 11. Logical Access Controls

This section sets out the rules which limit access to information, covering: user access management; user responsibilities; network access control; operating systems access control; application and information access control; mobile computing and home-working:

• User access is controlled by user identifiers and passwords and the varying level of access rights depending on need as set out in the Access Control Policy.

• Good practice in the use of passwords is mandatory and automatic log outs of PCs are enforced.

Policy D: 2.5.3. User password management

Staff shall choose sensible passwords i.e. that have a minimum of seven characters, and that are not easily guessed by others. Staff shall keep passwords secret and never disclose them to anyone.

Staff with authorised access to more than one system may have the same password on all systems to which they have access. This may give different access privileges on different systems depending on job need.

In the policies above, policy C does not cover much on what activities an employee needs to be aware of regarding password policy. For example, the policy states that “good practice in the use of the passwords is mandatory” but what does good practice in the use of password mean? The policy needs to explain a little more so employees understand and know exactly what activity is allowed and what is not. More explanation is like that seen in policy B above.

All the four policies did state what activity is acceptable and what is not in different areas, but not equally well in other areas. For example, software security in each policy is described as follows:

Policy A: 1.1 Software

1.1.1 Attachments which arrive via e-mail are virus-scanned as are software packages installed from the Web or removable media such as CD-ROM. However if you have not connected to the network for some time your virus scanning software could be out of date. Care should always be exercised and if there is any doubt seek advice from the IT service delivery team. (Also see 1.2 below).

1.1.2 All software used on any of the company's computers must be approved in advance by the IT Service Delivery Team. Only personnel authorised by the IT Service Delivery Team or the Head of Systems may load software onto any of the company's computers, connect any hardware or other equipment to any such computers or move or change any such computer equipment.

1.1.3 You must not make any copies of software except where this is expressly permitted by the copyright owner or as permitted by law. It is not permitted to use software for which the company does not own a current user licence. The making of 'extra' copies of software or the introduction of software packages from sources outside the organisation is expressly prohibited. The IT Service Delivery Team retains the legally-permitted back-up copies of all software used in the business and it should not be necessary for you to make copies for back-up purposes. The company has committed itself to obeying the user guidelines accepted in the industry and the company's reputation could be damaged if it were found to have infringed those guidelines.

1.1.4 If you have unlicensed software on a machine for which you are responsible, please remove it. This applies whether or not you actually use the software. If you are unsure whether you have a licence for a particular package, check with the IT Service Delivery Team. Where you are supplied software on a trial basis, you should delete it at the end of the specified time or purchase a licence. The company is committed to operating a fair policy on software purchase and will consider abuses seriously.

1.1.5 If you have a real need for a particular package, consult the IT Service Delivery Team.

Policy B: Covered in different places in the policy

- Under this Act (*Copyright Designs and Patent Act 1998*), any duplication of licensed software or associated documentation (e.g. manuals) without copyright owner’s permission is an infringement under copyright law. All proprietary software manuals are usually supplied under licence agreement, which limits the use of the products to specified machines and will limit copying to the creation of backup copies only. However in some instances, site licenses, permitting the use of software on all machines within a specified site are obtainable.
- No Staff should load or install software on any company computer without the prior consent of ICT Services.

Policy C: Only approved software and packages will be used.

Policy D: 2.6.2. Software

> Only licensed copies of approved commercial software shall be installed. It is a criminal offence to make or use unauthorised copies of commercial software and offenders are liable to disciplinary action.
>
> The installation of private software, shareware, or any non-standard application e.g. screensavers, games, utilities, etc. onto any computer owned by the company shall not be allowed. Exceptions will only be allowed with the prior authorisation of the IT Manager.

In the above software security policies, Policy B does not give more description on what activity is allowed, unlike how password security was explained. The mentioned examples show that all the four policies differ in covering the different issues in their security policy.

7.3 Good Practice

This section will give recommendation on what could be included in each criterion.

7.3.1 Fit Organizational Culture

Information security policy, as described in the previous chapters, needs to be tailored to organizational security culture. Therefore, organizations need to address security needs in the policy relating to their security culture (Zuccato, 2004). This criterion could not be evaluated in section 7.2 but some recommendations can be made to help in formulating organizational security policy. A relevant example of a security policy will be demonstrated later in the chapter.

Here in this section two issues of security policy will be described in detail: the feedback system and explaining the consequences of employee violations. These were the two main issues discussed in Chapter Six and they have an impact on employee non-compliance.

7.3.1.1 Feedback System for Suggesting Policy Improvements

In this section the organization needs to make it clear that there is a feedback system for suggesting policy improvements. A recommendation could be:

All staff should declare to the "information security department" the following so that this security policy is updated as appropriate:

1- *If any security threats appear in implementing organization security policy.*
2- *If any potential conflicts of interest are presented by the implementation of organization security policy.*
3- *Any difficulties in understanding and implementing organization security policy.*
4- *Any viruses detected or suspected on computers.*

7.3.1.2 Explain the Consequences of Violation and Breaches

This section needs to make it clear to employees that violation and non compliance to security policy will result in some consequences. A recommendation could be:

Any breach of this security policy will be investigated and result in the individual being subjected to the organization's disciplinary procedure.

7.3.2 Be Effective and Dynamic

Again the effectiveness of the policy is not easy to assess. The current discussion will give some tips to help organizations to formulate security policy that help employee compliance. The continuous discussion of this criterion is about the mechanisms to ensure dynamism in the policy. Organizational security policy needs to state the date of the last updates. As explained before, this will make the policy dynamic. A recommendation could be:

Information security policies are subject to change. The policy will be reviewed every six months. A review will also take place in response to significant security incidents, new vulnerabilities or changes to the organisational or technical infrastructure. If changes are made employees will be notified by their manager and electronic mail.

A feedback system has a big influence in updating the policy, for example when employees report new threats the security specialist department will have to change the policy to accommodate the new threats. Management monitoring is vital here, through checking how often the policy is updated, to ensure that employees are being made properly aware about changes.

7.3.3 Easy Language

Recommendations could relate to the language of the policy, which needs to be considered properly to influence employee compliance. This will help employees to have a clear guidance for their present and future security actions. Policies need to use definitive words like “must”, “must not, “should”, “should not”, “shall”, “shall not” to express the certainty to avoid employee confusion in taking actions.

7.3.4 Specify the Job Responsibilities

Job responsibilities in the policy make employees understand that responsibility towards organizational resources is there's. A recommendation could be:

It is the responsibility of all users of the organization's network to adhere to the policy.

7.3.5 State the Purpose of the Policy and the Scope of the Organization

This criterion describes the purpose of the security policy. A recommendation could be:

The purpose of the security policy is to protect the organization, its staff and public from all information security threats, whether internal or external, deliberate or accidental; to avoid the risk of the organization and individual employees facing legal liability.

7.3.6 Explain what Activity is Acceptable and what is not

Organizations need to consider that strict securities cannot guarantee good compliance, therefore there must be a balance of what the organization needs to protect and employee productivity, in terms of carrying out their daily tasks. Some of the activities, that explain what is acceptable and what is not, need to be tailored to organizational culture. For example, for Internet usage some organizations request employees not to use the Internet for private purposes and some do not allow employees to use the Internet at all or even to connect any machine that contains sensitive information to the Internet.

7.3.7 Have a Style which is Consistent with the Organization's General Communication Style

Security policy needs to have a consistence style to make employees understand it easily. This could be covered by checking the whole policy of the organization. In the proposed policy it shows that the policy is using a consistent style.

It should be emphasise that information security policy alone is not going to do any good to the organization unless other issues are merged with it, such as management and awareness. No matter how perfect organization security is if the management is not taking information security policy seriously the policy will fail in its purpose. If there are no awareness programs for employees to understand what they need to do about information security they will not be able to comply with policy easily.

7.4 Provision of an Example Policy

What follows is an example of what security policy could look like after checking with all the criteria above. Each of the following sections need to be tailored to the organization security culture. This example is a result of looking at the existing four policies that have been used for this chapter as well as searching the Internet for policies.
Some of the web sites that has been used to suggest the following policy are:

http://www.ecps.org/AUP2005.asp
http://www.molevalley.gov.uk/media/pdf/n/f/ANNEX_19_IT_POLICY.pdf
http://www.securityfocus.com/infocus/1504

The suggested policy is:

1. **Introduction**

The employee needs to understand the following:

1. This policy is based on the organization's information security policies. These policies are available from the employee's manager or on the organization's intranet.
2. The organization has legal obligations to maintain security under the following legislation: the Data Protection Act (1998); the Copyright Patents and Design Act (1988); and the Computer Misuse Act (1990). Employees will not use organization systems to perform any operation that would break this legislation.

3. Information security policies are subject to change. This policy will be reviewed every six months. A review will also take place in response to significant security incidents, new vulnerabilities or changes to the organizational or technical infrastructure.
4. If changes are made employees will be notified by their manager and electronic mail.
5. System, Network and Internet are to be treated as organization resources. This aims to address the following key principles of information security:

   Confidentiality - ensuring that only authorized persons have access to the information.

   Integrity - ensuring that the information is correct and complete.

   Availability - ensuring that authorized persons have access to the information when required.

2. Purpose of the Security Policy

The purpose of the security policy is to protect the organization, its staff and public from all information security threats, whether internal or external, deliberate or accidental; to avoid the risk of the organization and individual employees facing legal liability.

3. Employee Responsibilities

- It is the responsibility of every employee of the organization network to adhere to the policy.
- It is everyone's responsibility to ensure that security is implemented and maintained effectively.
- Every employee using the organization computer system should follow the following guidelines:

3.1 Feedback System

All employees should declare to the “information security department” the following, so that this security policy is updated as appropriate:

- If any security threats appear in implementing organizational security policy.
- If any potential conflicts of interest are presented by the implementation of organization security policy.
- Any difficulties in understanding and implementing organization security policy.

- Any viruses detected or suspected on computers.

3.2 User Login Responsibilities

Employees are advocated to do the following:-

- ❑ Keep passwords confidential;
- ❑ Avoid keeping a paper record of passwords;
- ❑ Change passwords wherever there is any potential compromise in security;
- ❑ Select passwords with a minimum of seven characters and a combination of letters and numbers;
- ❑ Avoid basing passwords on potentially guessable formats;
- ❑ Change passwords regularly, every six months.

3.3 Internet Access

- ❑ The organization reserves the right to monitor the system for legitimate business purposes;
- ❑ By choosing to use the organization's IT facilities, employees consent to the organization monitoring all Internet sites they access;
- ❑ Employees should not use the IT facilities to access Internet sites in particular any sites of an obscene, abusive, sexist or racist nature.

3.4 Email Usage

Employees are advocated to do the following:-

- ❑ May use the organization network to send and receive personal email;
- ❑ Personal emails should also adhere to the guidelines in this policy.
- ❑ Should not spread messages or emails that contain offensive materials;
- ❑ Should not open attachments unless you know who they are from and you are expecting to receive them. If you receive an email that seems suspicious contact the sender before opening to verify it is a valid email.
- ❑ Should not open EXE, BAT, VBS, and SCR type attachments ever, since they are common vectors for virus/malware infections.
- ❑ Always scan attachments manually with antivirus software before opening them, if they must be opened.

- The forwarding of chain letters, junk mail, jokes and executables is strictly forbidden.
- All messages distributed via the organization’s email system, even personal emails, are Organization’s property.

3.5 Virus Precautions

Employees are advocated to do the following:-

- Always use anti-virus software on your computer;
- Make sure your anti-virus software is up to date;
- Should not attempt to disable anti-virus software or prevent it from performing its daily update;
- Scan all files downloaded from the Internet;
- Scan all email attachments;
- Scan diskettes, memory sticks and CDs before use;
- Report all virus incidents immediately to your department. If you have a computer virus threat to report, please email security@organization.com.

3.6 Use of Organization's System & Network

- Should not install or distribute "pirated" or other software products that are not appropriately licensed for use by this organization;
- Should not bring any malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.);
- Should not provide information about, or lists of, this organization's employees to parties outside the organization;
- Should not use the organization's network to gain unauthorized access to any computer systems;
- Should not establish Internet or other external network connections that could allow non-organization employees to gain access to organization systems with critical or sensitive information unless prior approval has been received by the appropriate authority (*information security department*).

3.7 Disclosure of Information

- No employee should be subject to any punishment for having made a disclosure in good faith in agreement with this policy. This includes employees who may have been called as witnesses. Punishment refers to any administrative or disciplinary measure;
- Employees who consider they are subject to punishment as a direct result of having made a disclosure in agreement with this policy should bring the matter to the attention of the organization management;
- No confidential information should be disclosed that is protected under the organization's adopted legislations, unless required by law.

3.8 Personal Usage of Organization Resources

- Should not use organization's material or property in the care and custody of the organization for personal use without appropriate authority (*information security department*);
- Should not use your personal PC or Laptop within the organization's system without permission of the appropriate authority (*information security department*).

4 Consequences of Violation and Breaches

Any breach of this security policy will be investigated and result in the individual being subjected to the organization’s disciplinary procedure.

7.5 Conclusion

This chapter has given recommendations on how an effective security policy could be worded. With the help of this explanation organizations will be able to develop an effective security policy as well as reduce employee non compliance. According to Verdon (2006, p. 48) what makes a good policy is that it "*must be reasonable, understandable to their audience, and practicable, with very few exceptions*". It should be reasonable in the sense that each organization needs to run security according to their requirements (Hone & Ellof, 2002). It should be understandable by employees in terms of them being able to read it, understand and acknowledge (McIlwraith, 2006) the policy, as well as the implementation of the policy. Its practicability should be determined in terms of balancing the nature of the information and the related amount of threats (Wright & Kakalik, 2007).

Extrapolating upon the information found in the literature, as well as the findings from the three investigations, means a real life policy can be formulated that ensures compliance by employees. Security policy alone cannot do much without other factors being involved such as management and awareness. Management will enforce the policy through assigning different tasks, such as the IT department will make the policy available to all employees through the intranet of the organization. A hard copy should be given to employees so there will not be any confusion as to whether there is a policy in the organization or not. An awareness program is also needed which is approved by the management and applied by the IT department or the department who is in charge of information security. Also, monitoring employee compliance to the policy must take place either through regular auditing or available software.

Information security is a complex issue and employees cannot work alone, they need to work all together to ensure protection for organizational assets.

The four policies that have been used show that not all of them cover the same issues in the same level of depth, for example as it was explained in section 7.2.7, policy B gave more explanation about the usage of passwords but did not cover much about what activities employees need to practice for software security.

A metrics to give a value, for example out of 10, to measure each criterion in any policy is not available. As seen each policy has some weak points and some strong points, therefore it is hard to say which policy is a better policy and which is not. This work could provide the initial step towards developing some measures to evaluate what is a good policy and what is not.

Recommendations were suggested to formulate a security policy to maximize the benefit of the security policy and encourage employee compliance.

The subsequent chapter will conclude this thesis and describe potential future research directions.

Chapter Eight

Conclusion

This chapter concludes the thesis and suggests future research.

Lampson (2002) argues that many organizations' systems still remain vulnerable to attack after thirty years of accumulated work on security. This failing could result in unwanted situations like financial loss or lawsuits against the organizations (Cooper, 1984). Blakley et al. (2002, p. 98) explain that information security is a cyclical process were lessons are learned each time during one cycle and then implemented during the next cycle. It starts with policies which describe "*who should be allowed to do what to sensitive information*". The next stage is to enforce policies by applying a combination of processes and technical mechanisms. The final stage is an audit to "*determine the effectiveness of the measures taken to protect information against risk*".

Information security is an ongoing concern for any organization and is not merely a matter of putting mechanisms into place to protect resources, but also of ensuring user compliance by accommodating their needs and earning their trust by continually keeping their information secure. With the increase in varieties of threats information security has become a top agenda for organizations (Knapp & Marshall, 2007). Although the field of information security acknowledges that information security is a process not a product, organizations are still failing to recognize this issue in their operations, so they fall in the same pitfalls again and again.

8.1 Research Objectives and Contributions

The goal of this research study was to explore the success factors that are needed in an organization to implement information security effectively. It also investigated as to what made an effective security policy in terms of reducing security threats. It explored the reasons behind employee non compliance with organizational security policy; and investigated the impact of non-compliance by employees with organizational security policy. The primary contributions are:

- A set-guideline for organizations wishing to identify their requirements to implement information security successfully. The findings from chapter four suggested that organizations need to adopt and accommodate some ‘success factors’ which are awareness and training, top management support, budget, information security policy enforcement and adaptation, organization mission, and organization resources in order to implement information security successfully. The findings also suggested that each of these success factors is important and organizations might benefit more from implementing all the success factors identified.

- A set-guideline for organizations to better understand the steps needed to improve information security policy. The finding from the three investigations suggested that information security policy is vital for any organization to protect its assets. The findings suggested that an organization’s security policy needs to cover other issues in addition to the success factors. Findings from Chapter Five suggested that organizations with a documented security policy experience fewer reported security breaches.
- Enrich the literature in the field of information security to cover the human factor in the organization. The results over all suggested that employee’s security practices have the potential to weak the strength of information security in organizations. The results in Chapter Four and Six recommended organizations need to facilitate awareness programs to equip the employees with the proper knowledge to handle security decisions as well as help them to comply with organizations security policy comfortably.
- Help organizations to understand the reasons for an employee's non-compliance with information security policy. The findings from Chapter Six explored the issues of employee compliance with security policy. The employee’s compliance help to maintain organizations security as has been suggested from the results of Chapter Six. Knowing the reasons for employee non-compliance help the organization to understand the situation and work on encouraging compliance with their security policy to avoid any bypass organizational security controls.
- A set of recommendations about formulating security policy. All the three phases of the research recommended some issues and criteria that security policy needs to cover to make the security policy effective. Chapter Seven suggested recommendations about how to formulate a security policy to encourage compliance and therefore reduce security incidents.

8.2 Summary of the Results

The research study was divided into four stages.

8.2.1 Stage One: Success Factors in Information Security- Semi-Structured Interviews, Oman

Stage one starts with a qualitative semi-structured interview to explore and identify factors contributing towards successful implementation of information security in an organization.

The results show that only one organization in the entire selected sample (N=16 organizations) had a documented information security policy. Therefore the findings suggest that organizations need to be more proactive in producing a documented policy, where it is available to all the staff in one document and not in the form of scattered orders distributed from time to time. The results suggest that organizations are facing a lack of proper interventions related to deploying information security through employees. This result is that employees are not aware of information security policy or how to use technology properly.

The interviews reveal that there is no legislation in Oman for information security and findings suggest that legislation for information security in Oman would enhance the implementation of information security in their organizations (this investigation was conducted days after the establishment of the ITA in Oman).

The results also suggest that organizations are experiencing threats from their employees. This is in line with many other authors who suggest that the biggest threat to an organization is the insider threat.

The results suggest there should be feedback mechanisms in the organization which will help to increase confidence between the employees and the IT department (or the department responsible for the security). Feedback will help to review security policy and make employees share their experience regarding information security. Experts understood that the feedback mechanism was important in engaging employees in information security, but on the contrary employees never practiced feedback about security matters.

The end-users interviewed feel that setting up an organizational security policy needs different sections or departments involved. They believe that each of them know what kind of security they require. The interviews suggest that having a security department separate from the IT department is helpful for the implementation of information security in organizations. End-users explained the reason for not having a documented policy in their organization was that the management did not feel it was important.

Among the findings, the results suggest many factors organizations need to consider to implement information security successfully:

- **Awareness and training**: employees require continuous and ongoing training as well as education to understand and appreciate the need for information security and a security policy. From the findings end-users had concerns about their level of awareness to practice and implement security properly;
- **Top management support**: needs to understand the importance of information security and be concerned about information security. They also need to enforce the security policy, and provide an adequate budget as well as approve the appropriate training and education for their staff;
- **Budget**: needs to be sufficient in order to equip organizations with proper software, hardware and security policy. It should also include the required training for the staff of an organization;
- **Information security policy enforcement and adaptation**: organizations need an existing security policy to direct organizational goals and to spell out what is required from employees to protect their organizational assets. The security policy needs to be tailored to accommodate organizational culture;
- **Organization mission**: in general organizations need to have clear goals and objectives to address information security efficiently; and
- **Organization resources**: Organizations need software and hardware to implement information security mechanisms. A proper infrastructure would help in implementing information security in an organization successfully.

8.2.2 Stage Two: Information Security Policy – Questionnaire, Oman

Organizations must define the threats and vulnerabilities to their information resources to ensure the confidentiality, integrity and availability thereof (Gollmann, 1999; Pfleeger, 1997; Sebastiaan et al., 2003). One of the important mechanisms that organizations use to protect their information resources and valuable assets is information security policy, established to protect the organization from possible threats (Tryfonas et al., 2001; Fung et al., 2003; and Hinde, 2002). These policies also help organizations to identify their information assets and define the corporate attitude to these information assets (Canavan, 2003).

The second stage of the research starts from Chapter Five. It is based on the qualitative results. After analyzing the outcomes from the semi-structured interviews a questionnaire was developed including some relevant questions from the Doherty & Fulford (2005) survey questionnaire for information security policy. Questions were also identified from the literature.

The findings indicate that 81 percent (N=34) of Omani organizations questioned have a security policy in place. But only 16 out of 34 organizations are practicing a documented security policy. Analysis of the research question R1 suggests that organizations having a documented security policy will report fewer breaches than organizations not having a documented security policy. Analysis of the research question R3 concludes that there is a relationship between the documented security policy in organizations and the number of reported security breaches.

The results reveal two reasons why organizations do not have a documented security policy. One reason is that organizations are in the process of having a documented security policy. The second reason is that the IT department of the organization feels that their organizations are not putting enough effort into doing so.

The study outcomes show 74 percent (N=25) of organizations feel legislation is required in Oman. 62 percent (N=21) of organizations believe that legislation for information security in the country would enhance the implementation of information security.

Analysis of the research question R4 concludes that there is no relationship between organizations with a security policy covering a broader scope (user login responsibilities, use of organization system & network, internet access, etc…) and the number of reported security breaches. The outcome reveals organizations believe in the importance of each of the ‘success factors’ (awareness and training, top management support, budget, information security policy enforcement and adaptation, organizational mission and organization resources). The results also suggest that the adoption of these factors was not implemented by all organizations. Analysis of the research question R9 suggests no relationship between the greater reported adoptions of ‘success factors’ and the level of reported security breaches in the organization.

Organizations feel that the criteria of security are important. The adoption of these criteria was not well implemented by all organizations. Analysis of the research question R5 suggests that there were no relationship between the reported levels of adoption of different criteria in the security policy and the number of reported security breaches in the organization.

50 percent (N=17) of organizations feel that their security policy is effective. The other 41 percent (N= 14) were not sure. Analysis of the research question R10 concludes that the more issues the organization covers in their security policy the more effective their policy will be reported to be. The results reveal organizations cover these issues differently. For example, 91 percent (N=31) include user login responsibilities in their policy, 74 percent (N=25) include internet access and only 24 percent (N=8) include a feedback system for suggesting policy improvement in their security policy. Analysis of the research question R11 concludes that the more an organization reports adoption of criteria in their security policy, the more they report a highly effective security policy. Analysis of the research question R12 suggests that the more the organization implements the ‘success factors’ the more effective they feel the security policy will be.

Analysis of the research question R13 suggests that organizations which report effective information security policy also report they are effective at detecting and responding to reported information security breaches.

The highest level of security breaches that the findings suggest organizations' are experiencing in the last two years is by human error (38%, N=16). The results indicate that organizations with more employees have more reported security breaches as concluded by the analysis of the research question R7.

Analysis of the research question R6 concludes that there is a relationship in the period of the time the organization checks their employees' compliance with the reported security breaches in the organization. For example, when organizations check compliance with their policy monthly, there is a difference in the reported level of breaches than if they check annually or more. The result suggests 44 percent (N=15) of organizations check their employee compliance to their organizational security policy on a monthly basis. Another 44 percent (N=15) were either not sure of such compliance with security policy or they did not practice it.

8.2.3 Stage Three: Compliance with Organization's Security Policy – Semi-Structured Interviews, (UK, Glasgow).

Chapter Six presents the third stage of the research investigation. It is based on the unexpected findings derived from the analysis of the quantitative questionnaire. It shows a need for further investigation related to an employee's behaviour with security in an organization, using a semi structured interview.

The results suggest that employee activities represent a challenge to the security of the organization; no matter if they are 'expert', more experienced or completely unaware and uninformed employees. An unaware employee is the who does not understand the new technology that is involved in protecting an organization's assets or does not understand the security policy or is not even aware of such policy's existence, as well as the consequences of not following the policy. From the results the experts do know the rules; they do understand the policy and the risk of not complying with the rules but for them, as some explained, they think they know when to bend the rules.

Employees related the effectiveness of their organizational security policy to the level of breaches their organization experiences and their compliance to their security policy. The findings revealed that many organizations do not check their employee compliance to the policy.

The findings revealed different reasons for employee non-compliance to organizational security policy. Employees believe that their non-compliance to their organization security policy is:

- **Someone else's problem**: The results suggest that employees passively think of information security as someone else's job. For example, if a security breach occurs they often seem to believe it will affect the organization but not them. They believe that if they let in a virus then the IT technician will clean it up. The findings suggest that some employees do not like to handle security situations by themselves; they prefer the experts to take care of such situations. But some employees would like to try by themselves to solve the problem and then if they fail to fix it they would seek help.

- **Individual values and beliefs**: The findings suggest employees themselves differ in their value classification. For some employees sharing a password is a clear violation of their organization’s security policy. For others this behaviour could be seen as acceptable.
- **Work pressure**: Some related it to work pressure as in when jobs need to be done on time they cannot comply with security policy. The goal of security policy is to protect information and the organizational system without limiting its effectiveness, in other words the system should not be so secured so as to not allow the authorized employee to get the needed information to carry out their job.
- **Lack of awareness**: Some related non-compliance to a lack of awareness and understanding of the policy. The findings suggest that employees do not know that security policy exists in their organization and are not aware of the consequences of not following the policies, as well as that they do not appreciate the need of the policy.
- **Invisible security policy**: Security policy itself is not clear. A clear and visible information security policy will help employees to understand good security behaviour. Otherwise employees may try to find ways around security controls to let them do their job.
- **Organization security culture**: Organization security culture is how an organization handles its security. The findings suggested there are no existing rules about the consequences of not following the security policy, no strong management structure and no organization mission. Therefore, organizational security culture plays a big part in making employees comply with their organization security policy.
- **Trust**: The findings suggest that employees often trust their colleagues, trust their organization’s web browsers, they trust their organization’s firewalls to filter spam emails, they trust their organization’s anti virus software and so forth. This trust may explain why some employees access email attachments, which could bring the risk of a virus.

The findings revealed some impacts of non-compliance with organizational security policy and these can be summarized as follows:

- **Reputation of organization**: loss of information could be embarrassing to an organization. Organizations can have serious financial and legal implications if their information assets have been compromised.
- **Loss of equipment**: when organizations lose equipment this will lead to a delay in work as equipment may have critical software for certain tasks.
- **Privacy**: leakage of employee information can result in very serious risks to the organization. These risks might result in financial loss or lawsuits against the organization.
- **Work delay** (functionality): organizations are dependent on information technology to share information and other resources in order to get work done. Once employees fail to comply with policies this could cause the breakdown of their organization's network and will lead to work delays.
- **Integrity of information**: Information is needed in the decision making processes. If such information is not correct, organizations might experience unwanted effects such as financial loss or a drop in organizational reputation. The majority of the employees were aware of the fact that their organization has a security policy, but they had no idea what the security policy contained.

8.2.4 Stage Four: Consolidation

Chapter Seven takes the findings of the three studies and brings them together to give recommendations about how to formulate a security policy to encourage compliance and therefore reduce security threats. All the three study findings discussed common issues such as the awareness of employees, the clarity of the organization security policy and the management of the organization.

When the security policy is understandable by employees will make them most likely to comply. The awareness program has to be done by the security or IT department in the organization with the approval of the management, although there is no evidence on how awareness could help employees to comply with security policy, somehow organizations could rely on this issue and give its employee the required knowledge. Management influence is very serious in the implementation of information security and in employee compliance with security policy.

8.3 Reflecting on the Research

From what had been discussed so far it seems that the new problems appear along with old problems. This shows that organizations are still not giving enough attention to information security. Employees are still not aware of their organization security program. Organizations are not putting effort into helping their employees to understand security. Why after all these years is the information security problems still the same? The reason could be that the progress of information security is going slow because of repeating the same mistakes rather than learning from them. It also appears that information security cannot be explained by a single framework as every issue in information security is linked to the other. To have a good implementation of information security an organization needs to consider all the findings of this research.

8.4 Constraints

This research has relied on interviews and questionnaires, recognizing that this is an effort to achieve an insight into a hidden area. The idea of information security is sensitive and not easy; the most difficult parts of the research were trying to describe what was being explored and also thinking of different ways to assess those that were valid. Indeed this research is an initial investigation. It has tried to get some initial information on the subject and therefore there is no assurance that employees revealed their genuine views but their responses may have revealed a positive element of an objective. However, the three investigations seem to confirm some of the findings.

The majority of this research explored the opinions of employees regarding typical activities with security implications within their organizations. Therefore, the effect of the small size of the samples was that it decreased the generalisability of the findings.

ITA involvement during the first two investigations of the research, which was conducted in Oman, had both positive and negative effects. The positive effect is that most of the respondents willingly took part in the research. The high response rate for the quantitative questionnaire was related to the involvement of the ITA in distributing the questionnaire and following up with organizations.

The negative effect is there is a chance that the interviewers, because of the sensitivity of the information may not be very open in their responses in order to prove that they do their work properly and there is no breach of information security. Participants not wishing to record their interviews might have had an impact on the reliability of the contribution in the study through inaccurate reporting of what they believe or practice with information security.

Future work is suggested as follows.

8.5 Future Work

As with all research, this research study has raised many further questions and issues for future work. For example, the work needs to be conducted in different cultures to see if the results found are generalisable. The first two investigations were done in a governmental environment in Oman. The future work could be by using the same methodology during the two investigations with governmental organizations in the UK. This will show if there is culture difference and if the results are similar to the findings in Oman.

The same methodology could be used in private organizations to explore the similarities or differences in the findings. This comparison could be between the private and government organizations in Oman or in the UK as well as between the two countries.
It can also be done using different instruments such as ethnography or observation that could give a directly observable picture of information security in an organization.

However, if the findings are generally true then an employee’s engagement in information security is crucial to make them employ information security policy smoothly and may reduce the bypass of organization security controls to finish his job. Is this engagement related to training and awareness programs which will result in the sharing of knowledge among employees and reduce the non-compliance of an organizational security policy? This needs to be explored.

There is also a need for some measurement to formulate good policies that increase employee compliance with security policy. A feedback mechanism in engaging employees in information security required more investigation to help organization to develop their security policy effectively. More future work is needed on how budget is determined for information security.

The recommendations from Chapter Seven about how to formulate a security policy to encourage compliance and therefore reduce security threats might help new researchers to define information security policy to be used in different organizations. This could be done by identifying one organization which has no information security policy who is prepared to work with the researcher to establish the current state of security practices in the organization. Use system security testing techniques such as vulnerability scanning tool, security test and evaluation or penetration testing or a check list of widely regarded typical major threats. The researcher can implement the information security policies in the chosen organization for 6 months for example. Then the researcher can assess the new state of security in the organization by using the same techniques for comparison.

Bibliography

Adams, A., Sasse, M. A., & Lunt, P. (1997). Making Passwords Secure and Usable. *Proceedings of HCI on People and Computers XII*, (pp. 1 – 19).

Albrechtsen, E. (2007). A Qualitative Study of Users' View on Information Security. *Computers & Security, 26*, 276-289.

Anderson, J. M. (2003). Why we Need a New Definition of Information Security. *Computers & Security, 22* (4), 308-313.

Anderson, R. (1993). Why Cryptosystems Fail. *1st Conference Computer and Comm. Security*, (pp. 215-227).

Anderson, R., & Moore, T. (2008). Information Security Economics - and Beyond. *Interdisciplinary Workshop on Security and Human Behaviour (SHB 2008).*

Anderson, R., & Moore, T. (1998). The Economics of Information Security. *Science , 314* (5799), 610--613.

Appleyard, J. (2005). Information Classification: A Corporate Implementation Guide. In H. F. Tipton, & M. Krause, *Information Security Management Handbook* (Fifth ed.). CRC Press LLC.

Ashkanasy, N. M. (2002). Studies of Cognition and Emotion in Organisations: Attribution, Effective Events, Emotional Intelligence and Perception of Emotion. *Australian Journal of Management, 27*, 11-20.

Austen, S., Jefferson, T., & Thein, V. (2003). Gendered Social Indicators and Grounded Theory. *Feminist Economics, 9* (1), 1-18.

Bandyopadhyay, K., Mykytyn, P. P., & Mykytyn, K. (1999). A Framework for Integrated Risk Management in Information Technology. *Management Decision, 37* (5), 437-444.

Barber, B., & Davey, J. (1996). Risk Analysis in Health Care Establishments. In B. Barber, A. Treacher, & K. louwerse, *Towards Security in Medical Telematics: Legal and Technical Aspects* (pp. 120-124). Amsterdam: IOS Press.

Barman, S. (2001). *Writing Information Security Policies* (1st ed.). SAMS.

Barnett, J. H., & Karson, M. J. (1987). Personal Values and Business Decisions: An Exploratory Investigation. *Journal of Business Ethics, 6*, 371-382.

Baskerville, R., & Siponen, M. (2002). An Information Security Meta-Policy for Emergent Organizations. *Logistics Information Management, 15* (5/6), 337-346.

BBC. (2007, February). Retrieved 2007 February, from http://news.bbc.co.uk/2/hi/business/6360715.stm.

BBC. (2007, November). Retrieved November 2007, from http://news.bbc.co.uk/1/hi/uk_politics/7104945.stm.

BBC. (2008, January). Retrieved January 2008, from http://news.bbc.co.uk/2/hi/uk_news/politics/7199658.stm.

Bell, E., Taylor, S., & Thorpe, R. (2002). A Step in the Right Direction? Investors in People and the Learning Organisation. *British Journal of Management, 13,* 161–171.

Bell, J. (1984). *Conducting Small Scale Investigations in Education Management.* London: Harper & Row.

Bhagyavati, & Hicks, G. (2003). A Basic Security Plan for A Generic Organization. *Journal of Computing Sciences in Colleges, 19* (1), 248-256.

Bishop, M. (2003). What is Computer Security. *IEEE Security & Privacy,* 67-69.

Bjorck, F. (2001). Implementing Information Security Management Systems – An Empirical Study of Critical Success Factors. Lic thesis. Stockholm University & Royal Institute of Technology.

Bjorck, F. (2004). Institutional Theory: A New Perspective for Research into IS/IT Security in Organizations. *Proceedings of the 37th Hawaii International Conference on System Sciences.* IEEE.

Black, S. E., & Lynch, L. M. (2001). How to Compete: The Impact of Workplace Practices and Information Technology on Productivity. *The Review of Economics and Statistics, 83* (3), 434–445.

Blake, S. (2000). Protecting the Network Neighbourhood. *Security Management, 44* (4), 65-71.

Blakley, B., McDermott, E., & Geer, D. (2002). Information Security is Information Risk Management. *New Security Paradigms Workshop*, (pp. 97-104).

Brancheau, J. C., & Wetherbe, J. C. (1986). Key Issues in Information Systems Management: A Delphi Study of IS Executives and Corporate General Managers. In: (Second Edition ed.), *Working Paper Series-MISRC-WP-87-09*, University of Minnesota, Management Information Systems Research Center, School of Management.

Briggs, A. R., & Coleman, M. (2007). *Research Methods in Educational Leadership and Management* (2nd ed.). Sage.

Briney, A. (2000). Security Focused. *Information Security Survey*, 40-68. www.infosecuritymag.com.

Brodie, S. J., Biley, F. C., & Shewring, M. (2002). An Exploration of the Potential Risks Associated with Using Pet Therapy in Healthcare Settings. *Journal of Clinical Nursing, 11*, 444-456.

Brostoff, S., & Sasse, M. A. (2001). Safe and Sound: A Safety-Critical Approach to Security. *Proceedings of the 2001 Workshop on New Security Paradigms* (pp. 41 - 50). ACM.

Brown, J. S., & Duguid, P. (2002). *The Social Life of Information.* Boston: Harvard Business School Press.

Bruce, B. L. (2004). *Qualitative research methods for the social sciences* (5th ed.). London: Pearson.

Brunetto, Y. (2000). Management of Policy Implementation within Australian Universities. *Asia Pacific Journal of Human Resources, 38* (1), 50-66.

Bunker, E. (2003). Optimizing an Organization's Security Effectiveness by Using Vulnerability Management to Support the Audit Function. *Information Systems Control Journal, 4.*

Buszta, K. (2005). Security Management. In H. F. Tipton, & M. Krause, *Information Security Management Handbook* (Fifth ed.). CRC Press LLC.

Campbell, J. P., Gasser, M. B., & Oswald, F. L. (1996). *The Substantive Nature of Performance Variability In Individual Differences and Behaviour in Organizations.* San Fancisco: Jossey-Bass.

Canavan, S. (2003). An Information Security Policy Development Guide for Large Companies. *SANS Institute* .

Caralli, R. A., & Wilson, W. R. (2004). *The Challenges of Security Management.* Retrieved February 2006, from http://www.cert.org/archive/pdf

Carr, L. T. (1994). The Strengths and Weaknesses of Quantitative and Qualitative Research: What Method for Nursing? *Journal of Advanced Nursing, 20* (4), 716-721.

Carstens, D. S., McCauley-Bell, P. R., & DeMara, R. F. (2004). Evaluation of the Human Impact of Password Authentication Practices on Information Security. *Information Science Journal, 7*, 67-85.

Castelfranchi, C., & Pedone, R. (1999). A Review on Trust in Information Technology. *In Alfebiite project deliverable D1,* 33-57.

Caudle, S. L. (1990). Managing Information Resources in state Government. *Information Management Review, 50* (5), 515-524.

Cavusoglu, H. (2004). Economics of IT Security Management. In L. J. Camp, & S. Lewis, *Economics of Information Security* (pp. 71-83). Kluwer Academic Publishers.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2002). The Effect of Internet Security Breach Announcements on Market Value of Breached Firms and Internet Security Developers. *International Journal of Electronic Commerce, 9* (1), 69-105.

Chen, Y.-H., & Barnes, S. (2007). Initial Trust and Online Buyer Behavior. *Industrial Management and Data Systems, 107*, 21-36.

Chestnutt, I. G., Morgan, M. Z., Hoddell, C., & Playle, R. (2004). A Comparison of a Computer-Based Questionnaire and Personal Interviews in Determining Oral Health-Related Behaviours. *Community Dentistry and Oral Epidemiology, 32*, 410-417.

Chia, P. A., Maynard, S. B., & Ruighaver, A. B. (2006). Understanding Organizational Security Culture. In M. Hunter, & K. Dhanda, *Information systems: the challenges of theory and practice* (pp. 335-365). Las Vegas, USA: Information Institute.

Childs, D. (2002). Information Tecnology Security System Engineering Methodology. *Aerospace Conference 2003 Proceedings. 7*, pp. 3393-3401. IEEE.

Cisco. (2007, August). Retrieved October 2007, from Study Reveals Insight, Opportunity for IT to protect Mobile Wireless Users: http://newsroom.cisco.com/dlld/2007/prod_082107b.html.

Cisco. (2006). *Perceptions and Behaviors of Remote Workers: Keys to Building a Secure Company.* Cisco Systems.

Cockton, G. (2004). *A Tutorial: Grounded Design and HCI.* Pretoria: University of South Africa.

Cohen, L., Manion, L., & Morrison, K. (2007). *Research Methods in Education* (Sixth Edition ed.). Routledge.

Computer Misuse Act 1990. (2008). Retrieved February 2008, from http://www.opsi.gov.uk/acts/acts1990/UKpga_19900018_en_1.htm.

Conway, R. W., Maxwell, W. L., & Morgan, H. L. (1972). On the Implementation of Security Measures in Information Systems. *Communications of the ACM, 15* (4), 211-220.

Cooper, J. A. (1984). *Computer- Security Technology.* D.C.: Heath and Company.

Corbin, J., & Strauss, A. (1990). Grounded Theory Research: Procedures, Canons, and Evaluative Criteria. *Qualitative Sociology, 13* (1), 3-21.

Corritore, C. L., Kracher, B., & Wiedenbeck, S. (2003). On-line Trust: Concepts, Evolving Themes, A Model. *International Journal of Human-Computer Studies, 58* (6), 737-58.

Creswell, J. (1994). *Research Design: Qualitative & Quantitative Approaches.* Sage Publications Inc.

Creswell, J. W. (2003). *Research Design: Qualitative, Quantitative, and Mixed Method Approaches.* Thousand Oaks, CA: Sage.

Cuppens, F., & Saurel, C. (1996). Specifying a Security Policy: A Case Study. *IEEE Computer Society Computer Security Foundations Workshop (CSFW9),* (pp. 123–135).

Danchev, D. (2003). *Building and Implementing a Successful Information Security Policy*. Retrieved June 2005, from WindowSecurity: http://www.windowsecurity.com.

Data Protection Act. (1998). Retrieved January 2008, from OPSI: http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_1.

David, J. (2002). Policy Enforcement in the Workplace. *Computers & Security,* 506-513.

DE Villiers, M. R. (2005). Three Approaches as Pillars for Interpretive Information Systems Research: Development Research, Action Research and Grounded Theory. *SAICSIT*, 142-151.

Denning, D. E. (1999). *Information Warfare and Security.* ACM Press.

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why Phishing Works. *CHI 2006.* Montreal, Quebec, Canada: ACM.

Dhillon, G. (1999). Managing and Controlling Computer Misuse. *Information Management & Computer Security, 7* (4), 171-175.

Dhillon, G. (2001). Challenges in Managing Information Security in the New Millennium. In G. Dhillon, *Information Security Management: Global Challenges in the New Millennium.* Hershey: Idea Group Publishing.

Dhillon, G. (2006). *Principles of Information Systems Security, Text and Cases.* New York: John Wiley and Sons.

Dhillon, G., & Backhouse, J. (1996). Risks in the Use of Information Technology within Organizations. *International Journal of Information Management, 16* (1), 65-74.

Dhillon, G., & Backhouse, J. (2000). Information System Security Management in the New Millennium. *Communications of the ACM, 43* (7), 125-128.

Di Milia, L., & Gorodecki, M. (1997). Some Factors Explaining the Reliability of a Structured Interview System at a Work Site. *International Journal of Selection and Assessment,* 193-202.

Dinnie, G. (1999). The Second Annual Global Information Security Survey. *Information Management & Computer Security, 7* (3), 112-120.

Dixon, B. R., Bouma, G. D., & Atkinson, G. B. (1987). *A Handbook for Social Sciences Research; a Comparative and Practical Guide for Students.* Oxford: Oxford University Press.

Doherty, N. F., & Fulford, H. (2005). Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis. *Information Resources Management Journal, 18* (2), 21-39.

Donald, D. (2000). Behavioural effects of attitudes toward constraint in CASE: the impact of development task and project phase. *Information Systems Journal, 10*, 151–163.

Doney, P. M., Cannon, J. P., & Mullen, M. R. (1998). Understanding the Influence of National Culture on the Development of Trust. *Academy of Management Review, 23* (3), 601-621.

Dourish, P., Grinter, R. E., Dalal, B., de la Flor, J. D., & Joseph, M. (2003). *Security Day-to Day: User Strategies for Managing Security as an Everyday, Practical Problem.*

Dourish, P., Grinter, R. E., de la Flor, J. D., & Joseph, M. (2004). Security in the Wild: User Strategies for Managing Security as an Everyday, Practical Problem. *Personal and Ubiquitous Computing, 8,* 391-401.

DTI. (2004). *Information Security Breaches Survey.* Retrieved January 2006, from http://www.pwc.co.uk/pdf/dti_technical_report_2004.pdf.

DTI. (2006). *Information Security Breaches Survey.* Retrieved April 2007, from http://www.enisa.europa.eu/doc/pdf/studies/dtiisbs2006.pdf.

Du Plooy, G. M. (2002). *Communication Research; Techniques, Methods and Applications.* Landsowne: Juta.

Duncan, R. B. (1972). Characteristics of Organizational Environments and Perceived Environmental Uncertainty. *Administrative Science Quarterly, 17* (3), 313-327.

Duncan, R. J. (1995). There are some Cracks in the Cornerstone of Information Security. *Computers & Security, 14* (8), 675-680.

Dyne, L. V., Graham, J. W., & Dienesch, R. M. (1994). Organizational Citizenship Behavior: Construct Redefinition, Measurement, and Validation. *Academy of Management Journal, 37* (4), 765-802.

Echahed, R., & Prost, F. (2005). Security Policy in Declarative Style. *Proceedings of PPDP'05* (pp. 153-163). Lisbon: Portugal.

Egger, F. N. (2000). "Trust Me, I'm an Online Vendor":Towards a Model of Trust for E-Commerce System Design. *CHI '00 Extended Abstracts on Human Factors in Computing Systems* (pp. 101 - 102). The Hague, The Netherlands: ACM.

Eiser, J. R. (1994). *Attitudes, Chaos and the Connectionist Mind.* UK: Blackwell Publishers.

Ellison, C., & Schneier, B. (2000). Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure. *Computer Security Journal, 16* (1), 1-7.

Eloff, J. (2003). Information Security Management-A New Paradigm. *Proceedings of SAICSIT*, (pp. 130-136).

Ernst & Young. (2006). Retrieved September 2008, from http://www.ey.com/Publication/vwLUAssets/Global_Information_Security_-_2006/$FILE/GISS_2006.pdf.

Ernst & Young. (2004). Retrieved September 2008, from http://www2.eycom.ch/publications/items/saas_global_security_survey_2004/en.pdf.

E-Transactions Law. (2008). Retrieved September 2008, from http://www.egovnews.org/?p=4001.

Evans, D., & Larochelle, D. (2002). Improving Security Using Extensible Lightweight Static Analysis. *IEEE Software* .

Evers, V., & Day, D. (1997). The Role of Culture in Interface Acceptance. *Proceedings Human Computer Interaction, Interact’97,* (pp. 260-267). Chapman and Hall, London.

Farrell, H., & Farrell, B. J. (1998). The Language of Business Cods of Ethics: Implications of Knowledge and Power. *Journal of Business Ethics, 17,* 587-601.

Fensen, B. (2001). Implementation of Success Factors in New Product Development-the Missing Links? *European journal of Innovation Management, 4* (1), 37-52.

Fenton, J. H. & Wolfe, J. M. (2004). Organizing for Success: Some Human Resources issues in Information Security. In H. F. Tipton, & M. Krause, *Information Security Management Handbook* (pp. 1181-1197). CRC Press LLC.

Fernandez, J. (2008). *NHS Manager Suspended after Losing Laptop*. Retrieved July 2008, from E-Health Insider: www.e-health-insider.com/News/3910/nhs_manager_suspended_after_losing_laptop

Ferreira, B. R. (2007). Business and Industrial Security: Past, Present and Future. *Security Journal, 20*, 31-34.

Festinger, L. A. (1964). *Conflict, Decision, and Dissonance.* Stanford, CA: Stanford University Press.

Festinger, L., & Katz, D. (1954). *Research Method in the Behavioral Sciences.* London: Staples Press Limited.

Finegan, J. (1994). The Impact of Personal Values on Judgments of Ethical Behaviour in the Workplace. *Journal of Business Ethics, 13*, 747-755.

Fitzgerald, K. J. (1995). Information Security Baselines. *Information Management & Computer Security, 3* (2), 8-12.

Fitzgerald, T. (2007). Information Security Governance. In H. F. Tipton, & M. Krause, *Information Security Management Handbook* (Sixth ed., pp. 15-34).

Flick, U. (1998). *An Introduction to Qualitative Research.* SAGE Publications Ltd.

FogIndex. (2008, October 17). Retrieved October 24, 2008, from http://en.wikipedia.org/wiki/Gunning-Fog_Index.

Ford, G., & Gelderblom, H. (2003). The Effects of Culture on Performance Achieved through the Use of Human Computer Interaction. *Proceedings of SAICSIT,* (pp. 218-230).

Forte, D., & Power, R. (2007). Compliance: With what, and to what End? *Computer Fraud & Security*, 18-20.

Fulford, H., & Doherty, N. F. (2003). The Application of Information Security Policies in Large UK-Based Organizations: An Exploratory Investigation. *Information Management & Computer Security, 11* (3), 106-114.

Fung, P., & Jordan, E. (2002). Implementation of Information Security: A Knowledge-based Approach. 523-539.

Fung, P., Kwok, L.-f., & Longley, D. (2003). Electronic Information Security Documentation. *Australasiam Information Security Workshop (AISW2003). 21*. Australian Computer society.

Furnell, S. M., & Dowland, P. S. (2000). A Conceptual Architecture of Real- Time Intrusion Monitoring. *Information Management & Computer Security, 8* (2), 65-75.

Furnell, S. M., & Karweni, T. (1999). Security Implications of Electronic Commerce: A Survey of Consumers and Businesses. *Internet Research: Electronic Networking Applications and Policy, 9* (5), 372-382.

Furnell, S. M., & Warren, M. J. (1997). Computer Abuse: Vandalizing the Information Society. *Internet Research: Electronic Networking Applications and Policy, 7* (1), 61-66.

Garbars, K. (2002). *Implementing an Effective IT Security Program.* SANS Institute.

Garg, A., Curtis, J., & Halper, H. (2003). Quantifying the Financial Impact of IT Security Breaches. *Information Management & Computer Security, 11* (2), 74-83.

Garg, A., Curtis, J., & Halper, H. (2003). The Financial Impact of IT Security Breaches: What Do Investors Think? *Information Systems Security,* 22-33.

Gaunt, N. (1998). Installing an Appropriate Information Security Policy. *International Journal of Medical Informatics, 49,* 131-134.

Glaser, B. G., & Strauss, A. L. (1968). *The Discovery of Grounded Theory: Strategies for Qualitative Research.* London: Weidenfeld & Nicolson.

Glassner, B., & Moreno, J. (1989). *The Qualitative-Quantitative Distinction in the Social Sciences.* Dordrecht, Boston: Springer.

Glazer, R. (1993). Measuring the Value of Information: The Information-Intensive. *IBM Systems Journal, 32* (1), 99-109.

Goede, R., & De Villers, C. (2003). The Applicability of Grounded Theory as Research Methodology in Studies on the Use of Methodologies in IS Practices. *SAICSIT,* 208-217.

Goering, P. N., & Streiner, D. L. (1996). Reconcilable Differences: The Marriage of Qualitative and Quantitative Methods. *The Canadian Journal of Psychiatry, 41* (8), 491-497.

Gollmann, D. (1999). *Computer Security*. New York: John Wiley & Sons Ltd.

Gordon, L. A., & Leob, M. P. (2006). Budgeting Process for Information Security Expenditures. *Communications of the ACM, 49*, 121-125.

Gordon, L. A., & Leop, M. P. (2002). The Economics of Information Security Investement. *ACM Transactions on Information and System Security, 5* (2), 438-457.

Gorman, G., & Clayton, P. (1990). *Qualitative Research for the Information Professional: A Practical Handbook.* London: Library association publishing.

Greenwald, S. J. (1999). Discussion Topic: What is the Old Security Paradigm? *Proceedings of the 1998 workshop on New security paradigms* (pp. 107-118). New York, NY, USA,: ACM Press.

Gritzalis, D. (1997). A Baseline Security Policy for Distributed Healthcare Information Systems. *Computers & Security, 16* (8), 709-719.

Grudin, J. (1989). The Case Against User Interface Consistency. *Human aspects of Computing, 32* (10), 1164-1173.

Guadagno, R. E., & Cialdini, R. B. (2002). On-Line Persuasion: An Examination of Differences in Computer-Mediated Interpersonal Influence. *Group Dynamics: Theory, Research and Practice, 59,* 78-92.

Hale, A. R. (2000). Culture's Confusions. *Safety Science, 34*, 1-3.

Haley, C. B., Laney, R. C., & Nuseibeh, B. N. (2004). Deriving Security Requirements from Crosscutting Threat Descriptions. *Proceedings of the 3rd international Conference on Aspect-Oriented Software Development* (pp. 112 - 121). ACM.

Haley, C. B., Laney, R. C., Nuseibeh, B., & Moffett, J. D. (2003). Using Trust Assumptions in Security Requirements Engineering. *Second Internal iTrust Workshop On Trust*, (pp. 15-17). Imperial College, London, UK.

Hammersley, M. (1987). Some Notes on the Terms 'Validity' and 'Reliability'. *British Educational Research Journal, 13* (1), 73-81.

Hardee, J. B., West, R., & Mayhorn, C. B. (2006). To Download or Not to Download: An Examination of Computer Security Decision Making.

Hare, C. (2007). Policy Development. In H. F. Tipton, & M. Krause, *Information Security Management Handbook* (pp. 475-497). Auerbach Publications.

Hayes, R. (2007). Focused Asset Protection. *Security Journal, 20*, 41-43.

Hedrick, T. E., Bickman, L., & Rog, D. J. (1993). *Applied Research Design.* United States of America: Sage Publications, Inc.

Henry, K. (2007a). The Human Side of Information Security Information Security Governance. In H. F. Tipton, & M. Krause, *Information Security Management Handbook* (Sixth ed., pp. 139-154).

Henry, K. (2007b). Risk Management and Analysis Information Security Governance. In H. F. Tipton, & M. Krause, *Information Security Management Handbook* (Sixth ed., pp. 321-329).

Hentea, M., Dhillon, H. S., & Dhillon, M. (2006). Towards Changes in Information Security Education. *Journal of Information Technology Education, 5*, 221-233.

Higgins, H. N. (1999). Corporate system Security: Towards an Integrated Management Approach. *Information Management & Computer Security, 7* (5), 217-222.

Hinde, S. (2002). Security Surveys Spring Crop. *Computers & Security,* 310-321.

Hinde, S. (2003). Cyber-Terrorism in Context. *Computer & Security, 22* (3), 188-192.

Hitchings, J. (1995). Deficiencies of the Traditional Approach to Information Security and the Requirements for a new Methodology. *Computers & Security, 14* (5), 377-383.

Hoffer, J. A., & Straub, D. W. (1994). The 9 to 5 Underground: Are you Policing Computer Crimes? *In P. Gray, W. R. King, E. R. Mclean, & H. Watson (Eds.), Management of Information Systems* (pp. 388–401). Fort Worth, TX: Harcourt Brace.

Hollway, W., & Jefferson, T. (2000). *Doing Qualitative Research Differently: Free Association, Narrative and the Interview Method.* Sage Publications Ltd.

Hone, K., & Eloff, J. H. (2002). What Makes an Effective Information Security Policy? *Network Security, 20* (6), 14-16.

Hoo, K. J. (2000). How Much is Enough? A Risk-Management Approach to Computer Security. *Consortium for Research on Information Security and Policy,* (CRISP), Stanford University.

Hove, S. E., & Anda, B. (2005). Experiences from Conducting Semi-Structured Interviews in Empirical Software Engineering Research. *11th IEEE international Software Metrics Symposium*, (pp. 23-32).

Howard, P. D. (2007). The Security Policy Life Cycle: Functions and Responsibilities. In H. F. Tipton, & M. Krause, *Information Security Management Handbook* (Sixth ed., pp. 377-387).

Huang, H., Keser, C., Leland, J., & Shachat, J. (2003). Trust, the Internet, and the Digital Divide. *IBM Systems Journal, 42* (3), 507-518.

Huff, S. L., & Munro, M. C. (1985). Information Technology Assessment and Adoption: A Field Study. *MIS Quarterly, 9* (4), 327-340.

Huff, W. D. (2000). Colleges and Universities: Survival in the Information Age. *Computers & Geosciences, 26,* 635-640.

Huston, T. (2001). Security Issues for Implementation of E-Medical Records. *Communications of the ACM, 44* (9), 89-94.

Information Security Breaches Survey 2008. (2008). Retrieved April 2008, from http://www.pwc.co.uk/eng/publications/berr_information_security_breaches_survey_2008.html.

ISO. (2000). *Information Security Management Systems: Specification with Guidance for Use.* London: British Standards Institute.

ISO. (2001). *Information Technology: Code of Practice for Information Security Management.* London: British Standards Institution.

ITAA Global Cyber Security Survey (2003). Retrieved February 2005, from http://www.itaa.org/infosec/docs/BrainbenchITAAGlobalCyberSecuritySurvey.pdf.

Ives, B., Olson, M. H., & Baroudi, J. J. (1983). The Measurement of User Information Satisfaction. *Communications of the ACM, 26* (10), 785-793.

Janczewski, L., & Shi, F. X. (2002). Development of Information Security Baselines for Healthcare Information Systems in New Zealand. *Computer & Security, 21* (2), 172-192.

Jhonson, E. C. (2006). Security Awareness: Switch to a Better Programme. *Network Security*, 15-18.

Jolibert, A., & Baumgartner, G. (1997). Values, Motivations, and Personal Goals: Revisited. *Psychology & Marketing, 14* (7), 675-688.

Jones, C. (2004). *Quantitative and Qualitative Research: Conflicting Paradigms or Perfect Partners?* Retrieved June 2005, from Networked Learning Conference: http://www.networkedlearningconference.org.uk/past/nlc2004/proceedings/symposia/symposium4/jones.htm.

Jr, R. C., & Carver, C. (2007). Phishing for User Security Awareness. *Computers & Security, 26*, 73-80.

Kabay, M. E. (2002). Using Social Psychology to Implement Security Policies. *Computer Security Handbook*, 1-22.

Kankanhalli, A., Teo, H., Tan, B., & Wei, K. (2003). An Integrative Study of Information Systems Security Effectiveness. *International Journal of Information Management, 23* (2), 139-154.

Kansal, R. (2004). *Mitigate Risks Associated with Insider Threats.* Retrieved November 2007, from SDA India Magazine: Http://www.sda-india.com/sda/article/psecom,id,86,nodeid,5,_language,India.html.

Kaplan, R. (2007). A Matter of Trust. In H. F. Tipton, & M. Krause, *Information Security Management Handbook* (Sixth ed., pp. 295-310). CRC Press.

Katz, F. H. (2005). The Effect of a University Information Security Survey on Instruction Methods in Information Security. *Proceedings of the 2nd Annual Conference on Information Security Curriculum Development,* (pp. 43 - 48).

Kessler, G. C. (2001). Nontechnical Hurdles to Implementing Effective Security Policies. *IT Pro*, 49-52.

Kim, K. K., & Prabhakar, B. (2002). Initial Trust and the Adoption of B2C e-Commerce: The Case of Internet Banking. *The DATA BASE for Advances in Information Systems.*

Kis, M. (2002). Information Security Antipatterns in Software Requirements Engineering. *9th Conference of Pattern Languages of Programs.*

Knapp, K. J., & Boulton, W. R. (2006). Cyber-Warfare Threatnes Corporations: Expansion into Commercial Environments. *Information Systems Management, 23* (2), 76-87.

Knapp, K. J., & Marshall, T. E. (2007). Top Management Support Essential for Effective Information Security. In H. F. Tipton, & M. Krause, *Information Security Management Handbook* (Sixth ed., pp. 51-58). CRC Press.

Knapp, K. J., Marshall, T. E., Jr., R. K., & Morrow, D. W. (2006). The Top Information Security Issues Facing Organizations: What Can Government Do to Help. *Information Systems Security, xxxiv* (4), 51-58.

Kotulic, A. G., & Clark, J. G. (2004). Why there aren't more Information Security Research Studies. *Information & Management, 41,* 597-607.

Kreie, J., & Cronan, T. P. (1998). How Men and Women View Ethics. *Communications of the ACM, 41* (9), 69-76.

Kudo, M., Araki, Y., Nomiyama, H., Saito, S., & Sohda, Y. (2007). Best Practices and Tools for Personal Information Compliance Management. *IBM System Journal, 46* (2), 235-253.

Kvale, S. (1996). *Interviews: An Introduction to Qualitative Research Interviewing.* Thousand Oaks, CA: Sage.

Lachello, G. (2003). Protecting Personal Data: Can IT Security Management Standards Help? *Proceedings of the 19th Annual Computer Security Applications Conference,* (pp. 266- 275).

Lampson, B. W. (2002). Computer Security in the Real World. *Principles of Computer Systems, 37* (6), 37-46.

Lawton, R. (1998). Not Working to Rule: Understanding Procedural Violations at Work. *Safety Science, 28* (2), 77-95.

Leach, J. (2003). Improving User Security Behaviour. *Computer & Security, 22* (8), 685-692.

Lemon, N. (1973). *Attitudes and Their Measurement.* New York: Halsted Press.

LeVeque, V. (2006). Information Security: A Strategic Approach. *IEEE Computer Society*.

Lewandowski, J. O. (2005). Creating a Culture of Technical Caution: Addressing the Issues of Security, Privacy Protection and the Ethical Use of Technology. *Proceedings of SIGUCC'05* (pp. 184-187). Monterey, California, USA: ACM.

Lindup, K. R. (1995). A New Model for Information Security Policies. *Computer & Security, 14*, 691-695.

Liu, L., Yu, E., & Mylopoulos, J. (2003). Security and Privacy Requirements Analysis within a Social Setting. *Proceedings IEEE International Conference on Requirements Engineering (RE'03).* Monterey, California.

Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to Information Systems: Today's Reality, Yesterday's Understanding. *Computer Security,* 173-186.

Luker, M., & Petersen, R. (2005). *Computer and Network Security in Higher Education.* San Francisco: Jossey-Bass.

Madigan, E. M., Petrulich, C., & Motuk, K. (2004). The Cost of Non-Compliance-When Policies Fail. *Proceedings of the 32nd Annual ACM SIGUCCS Conference on User Services* (pp. 47-51). ACM.

Majchrzak, A., & Jarvenpaa, S. L. (2004). Information Security in Cross-Enterprise Collaborative Knowledge Work. *E:CO, 6* (4), 4-14.

Martins, A., & Eloff, J. (2001). Measuring Information Security. *Proceedings of Workshopon Information Security – System Rating and Ranking.* Virginia. http://philby.ucsd.edu/~cse291_IDVA/papers/rating-position/Martins.pdf.

Martins, A., & Eloff, J. H. (2002). Information Security Culture. *SEC,* 203-214.

Mascini, P. (2005). The Blameworthiness of Health and Safety Rule Violations. *Law & Policy, 27* (3), 472-485.

May, C. (2003). Dynamic Corporate Culture Lies at the Heart of Effective Security Strategy. *Computer Fraud and Security* (5), 10-13.

Maynard, S. B., & Ruighaver, A. B. (2006). What Makes a Good Information Security Policy: A Preliminary Framework for Evaluating Security Policy Quality. *5th Annual Security Conference.* Las Vegas, Nevada USA.

Mayring, P. (2000, June). *Qualitative Content Analysis.* Retrieved April 2005, from Qualitative Social Research: http://qualitative-research.net/fqs/fqs-e/2-00inhalt-e.htm

McCance, T. V., McKenna, H. P., & Boore, J. R. (2001). Exploring Caring Using Narrative Methodology: An Analysis of the Approach. *Journal of Advanced Nursing, 33,* 350–356.

McCoy, C., & Fowler, R. T. (2004). "You are the Key to Security" Establishing a Successful Security Awareness Program. *Proceedings of SIGUCCS'04* (pp. 346-349). Baltimore, Maryland, USA: ACM.

McDowell, K. (2006). Now That we are All so Well-Educated about Spyware, Can we Put the Bad Guys out of Business? *Proceedings of SIGUCCS Conference,* (pp. 235-239). Edmonton, Alberta, Canada.

McGraw, G. (2003). From the Ground Up: The DIMACS Software Security Workshop. *IEEE Security & Privacy*, 59-66.

McHugh, J., & Gates, C. (2004). Locality: A New Paradigm for Thinking About Normal Behavior and Outsider Threat. *Proceedings of the 2003 Workshop on New Security Paradigms*, (pp. 3 - 10). Ascona, Switzerland.

McIlwraith, A. (2006). *Information Security and Employee Behaviour.* England: Gower publishing.

McKay, J. (2003). *Pitching the Policy: Implementing IT Security Policy through Awareness.* SANS Institute.

Mears, L., & von Solms, R. (2004). *Corporate Information Security Governance: a Holistic Approach.* Retrieved April 2007, from http://icsa.cs.up.ac.za/issa/2004/Proceedings/Research/041.pdf.

Milberg, S. J., Burke, S. J., Smith, J. H., & Kallman, E. A. (1995). Values, Personal Information Privacy, and Regulatory Approaches. *Communications of the ACM, 38* (12), 65-74.

Mitnick, K., & Simon, W. L. (2002). *The Art of Deception: Controlling the Human Element of Security*. New York: John Wiley & Sons.

Morden, T. (2004). *Principles of Management* (Second ed.). Aldershot: Ashgate.

Morgan, G. (1997). *Imaginization: New Mindsets of Seeing, Organizing and Managing.* London: Sage Publications.

Mouratidis, H., Giorgini, P., & Manson, G. (2004). Using Security Attack Scenarios to Analyse Security During Information Systems Design. *Proceedings of the International Conference on Enterprise Information Systems (ICEIS 2004),* (pp. 10-17). Porto, Portugal.

Nau, D. (1995, December). *Mixing Methodologies: Can Bimodal Research be a Viable Post-Positivist Tool?* Retrieved March 2005, from http://www.nova.edu/ssss/QR/QR2-3/nau.html.

Neal, A., & Griffin, M. A. (2002). Safety Climate and Safety Behaviour. *Australian Journal of Management, 27*, 67-75.

Newman, E. (2001). Human Security and Constructivism. *International Studies perspectives, 2*, 239-251.

Nicastro, F. M. (2007). People, Processes, and Technology: A Winning Combination. In H. F. Tipton, & M. Krause, *Information Security Management Handbook* (Sixth ed., pp. 389-399).

Nierenberg, A. (2002). Tips on Encouraging Positive Networking Tactics. *Wiley Periodicals, Inc*, pp. 27-31.

Nijhof, A., Cludts, S., Fisscher, O., & Laan, A. (2003). Measuring the Implementation of Codes of Conduct. An Assessment Method Based on a Process Approach of the Responsible Organisation. *Journal of Business Ethics, 45*, 65-78.

Nikander, P., & Karvonen, K. (2001). Users and Trust in Cyberspace. *Security Protocols*, 24-35.

Nyanchama, M. (2005). Enterprise Vulnerability Management and its Role in Information Security Management. *Information Systems Security, 14* (3), 29-56.

Nyanchama, M., & Wilson, A. (2005). Managing Enterprise Security Information. In H. F. Tipton, & M. Krause, *Information Security Management Handbook* (Fifth ed.). CRC Press LLC.

O'Connor, A. D. (1993). Successful Strategic Information Systems Planning. *Journal of Information Systems, 1*, 71-83.

Omanet. (2006, April). Retrieved from http://www.omanet.om.

Oost, D., & Chew, E. (2007). *Invistigating the Concept of Information Security Culture.* Retrieved July 2007, from www.business.uts.edu.au/management/workingpapers/files/Oost2007.pdf.

Oppenheim, A. N. (1992). *Questionnaire Design, Interviewing and Attitude Measurement.* Continuum, London.

Oppliger, R. (2007). IT Security: In Search of the Holy Grail. *Communications of the ACM, 50* (2), 96-98.

Orlandi, E. (1998). Computer Safety and Security Policies: A Technical Issue Enforced by Law. 121-125.

Orlikowski, W. J. (1993). CASE Tools as Organizational Change: Investigating Incremental and Radical Changes in Systems Development. *Management Information System Quarterly, 17* (3).

Orna, E., & Stevens, G. (1995). *Managing Information for Research.* Open University Press.

Ortalo, R. (1998). A Flexible Method for Information System Security Policy Specification. *In Proceedings of 5th European Symposium on Research in Computer Security (ESORICS 98),* (pp. 67-84). Louvain-la-Neuve, Belgium, Springer-Verlag.

Ozaki, R. (2002). Housing as a Reflection of Culture: Privatised Living and Privacy in England and Japan. *Housing Studies, 17* (2), 209-227.

Paine, K. D. (2003). Guidelines for Measuring Trust in Organizations. *The Institute for Public Relations*.

Pandit, N. R. (1996). The Creation of Theory: A Recent Application of the Grounded Theory Method. *The Qualitative Report, 2* (4).

Patton, M. Q. (2002). *Qualitative Research and Evaluation Methods* (3rd ed.). Sage Publication.

Payne, S. C. (2006). A Guide to Security Metrics. *SANS Security Essentials Practical Assignment Version 1.2e*.

Payne, S. (2003). Campuswide Security Education and Awareness. *Copmuter and Network Security in Higher Education,* 89-104.

Pfleeger, C. P. (1997). *Security in Computing* (2nd ed.). Prentice Hall PTR.

Pfleeger, C. P., & Pfleeger, S. L. (2003). *Security in Computing.* Prentice Hall, div. of Pearson Education Inc.

Pieterse, V., & Sonnekus, I. P. Rising to Challenges of Combining Qualitative and Quantitative Research. *6th World Congress on Action Learning, Action Research and Process Management in Conjunction with the 10th Congress on Participatory Action Research.* Petoria, South Africa.

Posey, B. (2005). Keeping your Organization's Security Current. *Misc Network Security*.

Posnser, B., Randolph, W., & Schtuidt, W. (1987). Managerial Values Across Functions: A Source of Organizational Problems. *Group and Organization Studies, 12* (4), 373-385.

Post, G. V., & Kagan, A. (2007). Evaluating Information Security Tradeoffs: Restricting Access can Interfere with User Tasks. *Computers & Security, 26*, 229-237.

Post, G., & Kagan, A. (2000). Management Tradeoffs in Anti-Virus Strategies. *Information & Management, 37,* 13-24.

Posthumus, S., & von Solms, R. (2004). A Framework for the Governance of Information Security. *Computers & Security, 23*, 638-646.

Prenzler, T. (2007). The Human Side of Security. *Security Journal, 20,* 35-39.

Punch, K. F. (2003). *Survey Research: The Basics.* London: Sage.

Purser, S. A. (2004). Improving the ROI of the Security Management Process. *Computers & Security, 23,* 542-546.

Rainer, R. K., Jr., Marshall, T. E., Knapp, K. J., & Montgomery, G. H. (2007). Do Information Security Professionals and Business Managers View Information Security Issues Differently? *Information Systems Security, 16*, 100-108.

Rainer, R. K., Synder, C. A., & Carr, H. H. (1991). Risk Analysis for Information Technology. *Journal of Management Information Systems, 8* (1), 129–147.

Rasmusson, L., Rasmusson, A., & Janson, S. (1997). Using Agents to Secure the Internet Marketplace Reactive Security and Social Control. *Proceedings of PAAM'97.* London, UK.

Reason, J. (2000). Human Error: Models and Management. *BMJ, 320*, 768-770.

Reason, J. (1997). *Managing the Risks of Organizational Accidents.* England: Ashgate Publishing.

Reid, N. (2003). *Getting Started with Pedagogical Research in the Physical Sciences.* Hull: LTSN Physical Science.

Reid, N. (2006). Thoughts on Attitude Measurement. *Research in Science & Technological Education, 24* (1), 3-27.

Rich, M., & Ginsburg, K. R. (1999). The Reason and Rhyme of Qualitative Research: Why, When, and How to Use Qualitative Methods in the Study of Adolescent health. *Journal of Adolescent health, 25,* 371-378.

Riegelsberger, J., & Sasse, M. A. (2003). Designing E-Commerce Applications for Consumer Trust. In O. Petrovic, M. Ksela, M. Fallenböck, & C. Kittl, *Trust in the Network Economy* (pp. 97-110). Wien, New York: Springer.

Rieger, B., Kleber, A., & von Maur, E. (2000). Metadata-Based Integration of Qualitative and Quantitative Information Resources Approaching Knowledge Management. *Proceedings of the Eleventh International.*

Risjord, M. W., Dunbar, S. B., & Moloney, M. F. (2002). A New Foundation for Methodological Triangulation. *Journal of Nursing Scholarship, 34* (3), 269-275.

Rivlin, A. M. (1971). *Systematic Thinking for Social Action.* Washington, D.C.: The Brooking Institution.

Robson, C. (2000). *Real World Research* (Second ed.). Blackwell Publishers.

Rokeach, M. (1973). *The Nature of Human Values.* New York: The Three Press.

Roth, W. M. (2005). *Doing Qualitative Research Praxis of Method.* Sense.

Rubin, H. J., & Rubin, I. S. (1995). *Qualitative Interviewing.* Sage.

Rubin, H. J., & Rubin, I. S. (2005). *Qualitative interviewing the Art of Hearing Data* (Second ed.). Sage Publications.

Ruighaver, A. B., Maynard, S. B., & Chang, S. (2007). Organisational Security Culture: Extending the End-User Perspective. *Computers & Security, 26*, 56-62.

Ruppel, C. P., & Harrington, S. J. (2001). Sharing Knowledge through Intranets: A Study of Organizational Culture and Intranet Implementation. *IEEE Transactions on Professional Communication, 44* (1), 37-51.

Salam, A. F., Lyer, L., Palvia, P., & Singh, R. (2005). Trust in E-Commerce. *Communications of the ACM, 48* (2), 73-77.

Sandhu, R. (2003). Good-Enough Security: Toward a Pragmatic Business-Driven Discipline. *IEEE Internet Computing, 3*, 66-68.

Sasse, M. A. (2004). Usability and Trust in Information Systems. *Cyber Trust & Crime Prevention Project.* University College London.

Sasse, M. A., & Flechais, I. (2005). Usable Security: What is it? How do we Get it? In L. F. Cranor, & S. Garfinkel, *Security and Usability: Designing Secure Systems that People Can Use* (pp. 13-30). O'Reilly Books.

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the "Weakest Link": A Human-Computer Interaction Approach to Usable and Effective Security. *BT Technology Journal, 19* (3), 122-131.

Saunders, M. N., Lewis, P., & Thornhill, A. (2000). *Research Methods for Business Students* (2nd ed.). Prentice Hall.

Savola, R. M. (2007). Towards a Taxonomy for Information Security Metrics. *Proceedings of the 2007 ACM Workshop on Quality of Protection*, 28 - 30.

Scandura, A., & Williams, E. (2000). Research Methodology in Management: Current Practices, Trends and Implication for Future Research. *Academy of Management Journal, 143* (6), 1248-1264.

Schein, E. S. (2004). *Organizational Culture & Leadership* (3rd ed.). San Francisco, CA: Jossey-Bass.

Schilenger, T., & Teufel, S. (2003). Analyzing Information Security Culture: Increased Trust by an Appropriate Information Security Culture. *Proceedings of the 14th International Workshop on Database and Expert Systems Applications (DEXA'03).* IEEE Computer Society.

Schneider, F. B. (2000). Enforceable Security Policies. *Information and Systems Security, 3* (1), 30-50.

Schneier, B. (2001). Managed Security Monitoring: Network Security for the 21st Century. *Computers & Security, 20*, 491-503.

Schneier, B. (2003). *Beyond Fear.* United Stats: Copernicus Books.

Schwiderski-Grosche, S. (2006). *Security: An End User Perspective.* Information Security Technical Report, 11(3), 109-110.

Seidel, J. V. (1998). *Qualitative Data Analysis.* Retrieved 2005 April, from Qualis Research Associations: http://www.qualisresearch.com.

Seidman, R. B. (1978). Why Do People Obey the Law? The Case of Corruption in Developing Countries. *British Journal of Law and Society, 5* (1), 45-68.

Sharp, D. E. (2005). Information Security in the Enterprise. In H. F. Tipton, & M. Krause, *Information Security Management Handbook* (Fifth ed.). CRC Press LLC.

Shorten, B. (2007). Information Security Policies from the Ground Up. In H. F. Tipton, & M. Krause, *Information Security Management Handbook* (pp. 465-474). Auerbach Publications.

Siegel, C. A., Sagalow, T. R., & Serritell, P. (2002). Cyber-Risk Management: Technical and Insurance Controls for Enterprise-Level Security. *Security Management Practices*, 33-49.

Siegel, D. A., Reid, B., & Dray, S. M. (2006). IT Security: Protecting Organizations in Spite of Themselves. 20-27.

Silverman, D. (1997). *Qualitative Research Theory, Method and Practice.* Sage.

Sima, C. (2005). Security at the Next Level: Are your Web Applications Vulnerable. *SPI Dynamica*, 1-23.

Singleton, J. P., McLean, E. R., & Altman, E. N. (1988). Measuring Information Systems Performance: Experience with the Management by Results System at Security Pacific Bank. *MIS Quarterly, 12* (2), 325-337.

Siponen, M. (2006). Information Security Standards Focus on the Existence of Process, not it Content. *Technical Opinion, 49* (8), 97-100.

Siponen, M. T. (2000). A Conceptual Foundation for Organizational Information Security Awareness. *Information Management & Computer Security, 8* (1), 31-41.

Siponen, M. T. (2001). Five Dimentions of Information Security Awareness. *Computers and Society*, 24-29.

Siponen, M. T., & Oinas-Kukkonen, H. (2007). A Review of Information Security Issues and Respective Research Contributions. *SIGMIS Database, 38* (1), 60-80.

Slater, C., Saydjari, O. S., Schneier, B., & Wallner, J. (1998). *Toward a Secure System Engineering Methodology*. Retrieved January 2006, from http://www.schneier.com/paper-secure-methodology.html.

Slay, F. (2003). IS Security, Trust and Culture: A Theoretical Framework for Managing IS Security in Multicultural Settings. *Campus-Wide Information Systems, 20* (3), 98-104.

Smith, A., & Yetim, F. (2004). Global Human-Computer systems: Cultural Determinants of Usability. *Interacting with Computers*, *16*, 1-5.

Spurling, P. (1995). Promoting Security Awareness and Commitment. *Information Management & Computer Security, 3* (2), 20-26.

Stahl, S. (2007). Beyond Information Security Awareness Training: It is Time to Change the Culture. In H. F. Tipton, & M. Krause, *Information Security Management Handbook* (Sixth ed., pp. 555-565). Taylor & Francis Group, LLC.

Stajano, F. (2003). Security for Whom? The Shifting Security Assumptions of Pervasive Computing. 16-27.

Stajano, F., & Anderson, R. (2002). The Resurrecting Duckling: Security Issues for Ubiquitous Computing. *Security & Privacy,* 22-26.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of End User Security Behaviours. *Computers & Security, 24,* 124-133.

Starling, J. D. (1968). Organization and the Decision to Participate. *Public Administration Review, 28* (5), 453-460.

Stead, W. E., Worrell, D. L., & Stead, J. G. (1990). An Integrative Model for Understanding and Managing Ethical Behavior in Business Organizations. *Journal of Business Ethics, 9*, 233-242.

Stocker, R. (2000). Applying Usability Testing and Techniques to Develop User-Centered Security. *CIS 732 - Design of Interactive Systems*.

Storr, J., & Clayton-Kent, S. (2004). Hand Hygiene. *Nursing Standard*, *18* (40), 45-51.

Straub, D. W. (1989). Validation Instruments in MIS Research. *MIS Quarterly, 13* (2), 147-169.

Straub, D. W., & Welke, R. J. (1998). Coping with System Risk: Security Planning Models for Management Decision Making. *MIS Quarterly, 22* (4), 441-470.

Strauss, A., & Corbin, J. (1998). *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory* (Second ed.). Sage Publications, Inc.

Strobl, J., Cave, E., & Walley, T. (2000). Data Protection Legislation: Interpretation and Barriers to Research. *British Medical Journal, 321*, 890-892.

Strong, K., & Weber, J. (1998). The Myth of the Trusting Culture: A Global, empirical Assessment. *Business and Society, 37* (2), 157-184.

Sundt, C. (2006). Information Security and the Law. *Information Security Technical Report, 11*(1), 2-9.

Swanson, M., & Guttman, B. (1996). *Generally Accepted Principles and Practices for Securing Information Technology Systems.* Technical report, NIST, Technology Administration, Department of Commerce, U.S.

Tashakkori, A., & Teddlie, C. (1998). *Mixed Methodology: Combining Qualitative and Quantitative Approaches*. Thousand Oaks, CA: Sage.

Taylor-Powell, E., & Renner, M. (2003). *Analyzing Qualitative Data*. Retrieved May 2005, from University of Winsconsin: http://cecommerce.uwex.edu/pdfs/G3658_12.pdf.

Theoharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2005). The Insider Threat to Information Systems and the Effectiveness of ISO17799. *Computers & Security, 24*, 472-484.

Thomson, K., & von Solms, R. (2004). *Cultivating Corporate Information Security Obedience.* Retrieved March 2007, from http://icsa.cs.up.ac.za/issa/2004/Proceedings/Research/039.pdf.

Thorne, L., & Saunders, S. B. (2002). The Socio-Cultural Embeddedness of Individuals' Ethical Reasoning in Organizations (Cross-Cultural Ethics). *Journal of Business Ethics, 35*, 1-14.

Thrasher, K. (2003). A Direct Defense: Using an Employment Practices Compliance Approach to Avoid Employee Lawsuits. *Employee Relations Law Journal, 29* (1), 25-37.

TimesOnline. (2008, January). Retrieved January 2008, from Three Military Laptops with Secure Data Missing: http://www.timesonline.co.uk/tol/news/uk/article3227172.ece.

Tipton, H. F., & Krause, M. (2007). *Information Security Management Handbook.* New York: Auerbach Publications.

Torres, J. M., Sarriegi, J. M., Santos, J., & Serrano, N. (2006). Managing Information Systems Security: Critical Success Factors and Indicators to Measure Effectiveness. *Managing Information Systems Security*, 530-545.

Tryfonas, T., Kiountouzis, E., & Poulymenakou, A. (2001). Embedding Security Practicies in Contemporary Information Systems Development Approaches. *Information Management & Computer Security, 9* (4), 183-197.

Tyler, T. R. (2006). *Why People Obey the Law*. Princeton University Press.

Valentine, D. W. (2005). Practical Computer Security: A New Service Course Based Upon the National Strategy to Secure Cyberspace. *Proceedings of SIGITE'05*, (pp. 185-189). Newark, New Jersey, USA.

Van Dyne, L., Graham, W. J., & Dienesch, R. M. (1994). Organizational Citizenship Behavior: Construct Redefinition, Measurement, and Validation. *Academy of Management Journal, 37* (4), 765-802.

Varney, C. A. (1996). Consumer Privacy in the Information Age: A View from the United States. *Remarks before the Privacy and American Business National Conference.* Washington.

Venter, H. S., & Eloff, J. H. (2003). A Taxonomy for Information Security Technologies. *Computers and Security*, 299-307.

Verdon, D. (2006). Security Policies and the Software Developer. *IEEE Security & Privacy*, 42-49.

Von Solms, B. (2000). Information Security – the Third Wave? *Computers & Security, 19* (7), 615-620.

Von Solms, B., & von Solms, R. (2004). The 10 Deadly Sins of Information Security Management. *Computer & Security, 23,* 371-376.

Von Solms, R. (1996). Information Security Management: The Second Generation. *Computer & Security, 15,* 281-288.

Von Solms, R. (1999). Information Security Management: Why Standards are Important. *Information Management & Computer Security, 7* (1), 50-57.

Von Solms, S. H., & Eloff, J. H. (2003). *Information Security.* B & D Printers.

Voss, C. (1985). Determinants of Success in the Development for Applications Software. *Journal of Product Innovation Management, 2,* 122-129.

Vroom, C., & von Solms, R. (2004). Towards Information Security Behavioural Compliance. *Computer & Security, 23,* 191-198.

Watson, J. G., & Barone, S. (1976). The Self-Concept, Personal Values, and Motivational Orientations of Black and White Managers. *The Academy of Management Journal, 19* (1), 36-48.

Webography. (2008). Retrieved November 2008, from http://www.writeitpro.co.uk/ta_overview.htm.

Wenzel, M. (2004). The Social Side of Sanctions: Personal and Social Norms as Moderators of Deterrence. *Law and Human Behavior, 28,* 547-567.

Westrum, R. (1993). Cultures with Requisite Imagination. In J. A. Wise, V. D. Hopkin, & P. Stager, *Verification and Validation of Complex Systems: Human Factors Issues* (pp. 401-416). Springer-Verlag.

Whitman, M. E. (2003). Enemy at the Gate: Threats to Information Security. *Communications of the ACM, 46* (8), 91-95.

Whitman, M. E. (2004). In Defense of the Realm: Understanding the Threats to Information Security. *International Journal of Information Management, 24,* 43-57.

Whitman, M. E., Caylor, J., Fendler, P., & Baker, D. (2005). Rebuilding the Human Firewall. *Information Security Curriculum Development Conference* (pp. 104-106). Kennesaw, GA, USA: ACM.

Williams, A., Peterson, E., Knight, S., Hiller, M., & Pelletier, A. (2004). Survey of Restaurants Regarding Smoking Policies. *J public Health Management Practice, 10* (1), 35-40.

Witty, R., Girard, J., Graff, J., Hallawell, A., Hallawell, A., Hildreth, B., et al. (2001). *The Price of Information Security.* Gartner.

Wong, K., & Watt, S. (1990). *Managing Information Security.* Elsevier Science Publishers Ltd.

Wood, C. C. (2005). *Information Security Policies Made Easy*. Information Shield, Inc.

Wood, M. B. (1982). *Introducing Computer Security*. NCC Publications.

Workman, M. (2007). Gaining Access with Social Engineering: An Empirical study of the Threat. *Information Security Journal: A Global Perspective, 16* (6), 315-331.

Workman, M., & Gathegi, J. (2006). Punishment and Ethics Deterrents: A Study of Insider Security Contravention. *Journal of the American Society for Information Science and Technology, 58* (2), 212-222.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security Lapses and the Omission of Information Security Measures: A Threat Control Model and Empirical Test. *Computers in Human Behavior, xxx*, 1-18.

Wright, M., & Kakalik, J. (2007). *Information Security Contemporary Cases.* USA: Jones and Bartlett Publishers Inc.

Wylder, J. (2007). *Strategic Information Security.* Taylor & Francis.

Zuccato, A. (2004). Holistic Security Requirement Engineering for Electronic Commerce. *Computer & Security, 23*, 63-76.

Zurko, M. E., Kaufman, C., Spanbauer, K., & Bassett, C. (2002). Did you Ever have to Make up your Mind? What Notes do when Faced with a Security Decision. *Proceedings of 18th Annual Computer Security Applications Conference.* Las Vegas, Nevada.

Appendix A

Information Technology Authority (ITA) Policy

The Information Technology Authority (ITA) was set up by Royal Decree 52/2006 promulgated on the 1st June 2006. This independent legal body is affiliated to the Ministry of National Economy. The ITA is accountable for implementing national IT infrastructure projects and supervising all projects related to implementation of the Digital Oman Strategy, while providing professional leadership to other e-Governance initiatives of the Sultanate.

More details about ITA Policy is available at
http://www.ita.gov.om

UNIVERSITY
of
GLASGOW

Information Sheet

Title: Information Security, People's behaviour and attitude

Researcher: Maryam Al_Awadi

The aim of this research is to explore the human aspects that influence information security in order to identify the motivations for different practices in an organization and the objective is to find out what are the factors that might affect people's behaviour and attitudes towards information security procedures?

It is completely up to you to decide whether or not to take part in my interview questionnaire. If you decide to take part you are free to withdraw the interview at any time without giving a reason. You also have the right to withdraw retrospectively any consent given, and to require that any data gathered on you be destroyed.

All information collected about you during the interview will be kept strictly confidential. Data will be stored for analysis and then destroyed.

For further information about this study please contact:

Maryam Al-Awadi
Department of Computing Science, University of Glasgow
17 lilybank Gardens
Glasgow, G12 8QQ
Email: mawadi@hotmail.com
Tel: 0141 330 2000 ext : 0918

(1) IT& Information Security Experts Semi-Structured Interview Questionnaire

Interview Number:

Name:

Place:

Date:

Interview length:

1. Respondent's background

Job title:

Job function related to the IT or Information security:

Qualifications:

Experience:

2. Organization Security Mechanism

How you make sure that only your employees access your sensitive data in your organization system?

What is the present status of the information security in your organization?

If you didn't achieve all your goals, what do you think were the main obstacles?

Who recognized the need for the IT and Information security strategy? Why?

Who was involved in the process of planning the implementation of Information security?

Did you use any external advisors? If not, do you think it would have helped?

What was the sequence of events when implementation was planned?

Did you or anyone else study the implementation of Information security in other organizations before you implemented it into your own organization?

If yes, explain how this was done?

How did you evaluate the results of the study?

Who was involved in the process of planning the implementation of the policy?

How you maintain the confidentiality of the data in the organization?

How you maintain the integrity of the data in the organization?

3. Information Security Policy

Does your organization have an Information Security policy? If yes, do you have a copy of the policy?

If No, Why?

Who wrote/compiled the Policy?

How long have you had an Information security policy?

Who is involved in the development of the information security policy?

Does this team (security or IT team) review the information security policy regularly? If yes, How often?

If no, why not?

Do you involve any members of the organization outside the IT department in the process of developing information security policy?

Do you involve any members of the organization outside the IT department in the process of formulating information security policy?

Is the Information security policy integrated with the overall business plan for the organization?

Does the policy explain what is an acceptable, and what is not an acceptable activity in the organization?

Does the top management support the implementation of the policy?

If yes, how does the top management support the implementation of the policy?

What did you plan to achieve from the implementation of the policy?

What are the goals from the implementation of the policy?

How successful is the policy?

How do you measure its success?

Was there any resistance in introducing the Information security policy?

Do you think that the information security policy should be the same or different in all organizations?

How do you enforce the Information security policy in the organization?

How do you make sure that all employees understand the information security policy?

How do you make sure that your organization employee follows the information security policy?

4. Types of Threats that Occurs in the Organization

Have you experienced any security incidents in the organization over the past year?

If yes, what type of security incidents? Insider threat, Outsider threat?

How you make sure that these incidents won’t happen again, or reduced?

What are your plans for handling future security incidents?

5. Success Factors of Information Security

Do you think that the implementation of Information security was successful?

In what way it was successful / unsuccessful?

If successful what made the implementation successful?

If unsuccessful what options you will advise others who are in the process to implement Information security policy to exclude?

What are you basing this judgment on?

What else could have been done to improve the success of the implementation?

Does the organization put sufficient budget into Information security Technology such as Software, Firewalls... etc?

Does the organization put sufficient budget into, preparing the policy, distributing the policy, keeping it up to date, enforcing the policy?

6. Different Practices of Information Security in Organization

Do you get any feedback on how effective or ineffective the policy is?

If yes, what do you do if it is not effective?

How do you handle feedback?

Are there formal mechanisms for feedback?

Any other comments?

(2) End-Users Semi-Structured Interview Questionnaire

Interview Number:

Name:

Place:

Date:

Interview length:

1. Respondent's background

Job title:

Job function related to the IT or Information security:

Qualifications:

Experience:

2. Organization Security Mechanisms

How you make sure that only employee can access data in the organization system?

How you make sure that your colleagues don’t see or access to your work?

Do you think that security technology such as antivirus software; firewalls, etc are available in your organization?

3. Information Security (Information security) policy

Does your organization have a security policy? If yes, do you have a printed copy of the policy?

How long have you had an Information security policy?

Does the organization change the security policy regularly? If yes, how often has the policy changed?

How the organization deliver the policy to employee when it changes?

How is the information security policy enforced in the organization?

Does the organization train employees in understanding the policy?

Does the organization explain the need of the policy?

How the information security policy enforced in the organization?

Does the policy explain what is an acceptable, and what is not an acceptable activity in the organization?

Is the current security policy sufficient for protecting the information you work with as part of your job?

Is the current security policy sufficient for protecting your own personal information held by the organization?

Do you conform to the organization security policy? If no, why not?

If yes do you obey all the instructions or only those that make sense to you?

Does your manager show concern about enforcing the security policy? How?

Do you know what the purpose is of the implementation of the security policy?

If yes, what?

Do you think that the security policy is relevant to you in terms of your job?

If no, how do you think it should be different?

Looking back, do you think that the security policy helped the organization to reduce threats, such as: losing data, viruses etc…? If no, why?

Do you feel it is important to have security policy in the organization?

4. Different Practices of Information Security in Organization

Would you like to be involved in setting up the Information security policy?

If yes, How? If No, why?

Have you provided feedback suggestions for improvement in Information security to your organization?

If yes, Can you describe your experiences in contributing towards the improvement of the information security to your organization?

Do you think having feedback mechanism will improve information security in your organization?

Describe any concerns for security in your organization?

Any other comments?

Appendix B

Computing Science Department
Glasgow University
E-mail: mawadi@dcs.gla.ac.uk

IMPLEMENTING INFORMATION SECURITY IN OMAN
Best Practice Approach

ALL RESPONSES WILL BE TREATED IN THE STRICTEST CONFIDENCE

Would you like a copy of the findings: yes □ no □

If yes, please supply name and address for receipt of your copy of the findings. Alternatively, if you would prefer your responses to remain completely anonymous, put an email address in the address section.

Name:
Address:

Section A: Background Information

1. Please specify your organization sector ______________________________ (e.g. Government, Private) .

2. Approximately how many people are employed in your organization?

Less than 500 □ 500-1000 □ 1001-1500 □ 1501-2000 □
2001-3000 □ 3001-5000 □ 5001-10000 □ Over10000□

Section B: Security Breaches to your Organization

3. Please record in the table below the **approximate number of IT security breaches** that your organization has experienced in the past two years, and **indicate the severity of the worst breach** of each type, using the scale provided.

Breach	**Approximate no. of occurrences in last two years**						**Severity of worst incident**				
							Quite Insignificant				*Highly Significant*
Computer virus	0	<5	5-10	> 10	>100	>1000	1	2	3	4	5
Installation/ use of unauthorized hardware, peripherals.	0	<5	5-10	> 10	>100	>1000	1	2	3	4	5
Abuse of computer Access controls	0	<5	5-10	> 10	>100	>1000	1	2	3	4	5
Physical Theft of Hardware / Software	0	<5	5-10	> 10	>100	>1000	1	2	3	4	5
Computer-based fraud	0	<5	5-10	> 10	>100	>1000	1	2	3	4	5
Human mistake	0	<5	5-10	> 10	>100	>1000	1	2	3	4	5
Natural Disaster	0	<5	5-10	> 10	>100	>1000	1	2	3	4	5
Damage by Displeased Employee	0	<5	5-10	> 10	>100	>1000	1	2	3	4	5
Spam Emails	0	<5	5-10	> 10	>100	>1000	1	2	3	4	5
Use of organization resources for illegal communications or activities. (porn surfing, e-mail harassment)	0	<5	5-10	> 10	>100	>1000	1	2	3	4	5
Installation/ use of unauthorized software	0	<5	5-10	> 10	>100	>1000	1	2	3	4	5
Hacking incident (external)	0	<5	5-10	> 10	>100	>1000	1	2	3	4	5
Other? Please specify ______________________________ ______________________________	0	<5	5-10	> 10	>100	>1000	1	2	3	4	5

Please use this space if you wish to make any comments about these security breaches.

Section C: Information Security Policy

4. Does your organization have an Information security policy? Yes □ No □

*If **no**, please answer question 5 below and return your questionnaire in the envelope supplied.*

5. Why does your organization not have an information security policy?
____

*If **yes**, please answer the questions in the remaining sections of the questionnaire.*

6. Is the information security policy ***documented***? Yes □ No □

7. If not, please specify why your organization does not have a ***documented*** information security policy ____

8. If so, how long has your organisation been actively using a documented information security policy? _____ years

9. How is the policy distributed to employees?

Organization intranet □ Staff handbook□ Other □ Please specify ___________

10. How would you rate the overall effectiveness of your policy? *Using the table below, please indicate the effectiveness of your policy.*

Not at all Effective	Somewhat Effective	Neither	Effective	Very Effective
1	2	3	4	5

11. How would you rate your organization's effectiveness at detecting and responding to attempted information security breaches from your own employees? *Using the table below, please indicate the effectiveness at detecting and responding to information security breaches.*

Not at all Effective	Somewhat Effective	Neither	Effective	Very Effective
1	2	3	4	5

12. Do you think legislation for information security is required in the country
Yes □ No □

13. How would you rate the success of implementing information security in your organization when there is legislation for information security in the country? *Using the table below, please indicate the success of implementing information security in your organization when there is legislation in the country.*

Not at all Successful	Somewhat Successful	Neither	Successful	Very Successful
1	2	3	4	5

14. How do you check the compliance of employees to your security policy?

Please specify ____

15. How often do you check compliance to your security policy?

Weekly □ Monthly □ Quarterly□ Annually□ Less often Annually□ Unknown□

16. Do you record the number of security breaches that occur in your organization?
    Yes □ No □

17. Are the organization's computers and network devices (e.g. routers, and switches) regularly tested for usable vulnerabilities? Yes □ No □

18. Are all computer systems protected with up-to-date anti-virus software and other defenses against malicious software attacks? Yes □ No □

19. How the systems are kept updated? Please Specify ______________________________
____
____
____

20. Using the table below, please indicate the issues covered in your Information security policy. If you do not clearly cover an issue through your policy please leave blank.

Issue	**Information Security Policy**
User Login Responsibilities	❐
Use of Organization System & Network	❐
Internet Access	❐
Viruses, Worms & Trojans	❐
Disclosure of information	❐
Define Responsibilities	❐
Email Usage	❐
Adoption of some Laws, for example: Data Protection Law, International standards (ISO 17799), Privacy Law...etc.	❐
Personal usage of Organization Resources	❐
Explain the Consequences of Violations and Breaches	❐
Feedback system for suggesting policy improvements	❐
Other? Please specify ______________________ ______________________ ______________________	❐

Section D: The Success of your Information Security.

21. Using the table below, please indicate the **importance** of each of the following factors and the extent to which your organization is **successful** in adopting them.

Factors	How **important** do you believe the following factors to be for **the successful implementation of Information security** in your organization?					How **successful** do you believe your organization has been in **adopting each of these factors?**				
	Not Important				***Very Important***	***Not Successful***				***Very Successful***
Organization clear goals and objectives of information security	***1***	***2***	***3***	***4***	***5***	***1***	***2***	***3***	***4***	***5***
Implementation of information security with a consideration of organizational culture	***1***	***2***	***3***	***4***	***5***	***1***	***2***	***3***	***4***	***5***
Visible commitment from management	***1***	***2***	***3***	***4***	***5***	***1***	***2***	***3***	***4***	***5***
A clear understanding of security risks	***1***	***2***	***3***	***4***	***5***	***1***	***2***	***3***	***4***	***5***
A clear understanding of security requirements	***1***	***2***	***3***	***4***	***5***	***1***	***2***	***3***	***4***	***5***
Effective and ongoing awareness program of security to all employees	***1***	***2***	***3***	***4***	***5***	***1***	***2***	***3***	***4***	***5***
Putting information security policy in practice	***1***	***2***	***3***	***4***	***5***	***1***	***2***	***3***	***4***	***5***
Providing suitable employee training and education	***1***	***2***	***3***	***4***	***5***	***1***	***2***	***3***	***4***	***5***
Sufficient budget for information security.	***1***	***2***	***3***	***4***	***5***	***1***	***2***	***3***	***4***	***5***
Organization IT infrastructure	***1***	***2***	***3***	***4***	***5***	***1***	***2***	***3***	***4***	***5***
Others, Please Specify ______________________________ ______________________________	***1***	***2***	***3***	***4***	***5***	***1***	***2***	***3***	***4***	***5***

If you have a ***documented*** information security policy, please answer the following question, if no please use the space provided in the next page to make any comments with respect to the formulation, application or effectiveness of Information security within your organization.

Section E: The Criteria of Information Security Policy.

22. In order to have an effective information security policy, an organization should select a set of criteria to be implemented accurately and to give good results. Using the table below, please indicate the **importance** of each of the following criteria and the extent to which your information security policy is **successful** in adopting them.

Criteria	How **important** do you believe the following criteria to be for **the successful implementation of Information security** policy in your organization?					How **successful** do you believe your information security policy has been in **adopting each of these criteria?**				
	Not Important				***Very Important***	***Not Successful***				***Very Successful***
Explain what acceptable activity is and what is not.	*1*	*2*	*3*	*4*	*5*	*1*	*2*	*3*	*4*	*5*
State the purpose of the policy and the scope of the organization	*1*	*2*	*3*	*4*	*5*	*1*	*2*	*3*	*4*	*5*
Specify the job responsibilities.	*1*	*2*	*3*	*4*	*5*	*1*	*2*	*3*	*4*	*5*
Use a solid language rather than an abstract language.	*1*	*2*	*3*	*4*	*5*	*1*	*2*	*3*	*4*	*5*
Dynamic in order to cover the changes in the environment of information security.	*1*	*2*	*3*	*4*	*5*	*1*	*2*	*3*	*4*	*5*
Use simple language to ensure it is not difficult to understand.	*1*	*2*	*3*	*4*	*5*	*1*	*2*	*3*	*4*	*5*
Style consistent with the organizations generally communication style.	*1*	*2*	*3*	*4*	*5*	*1*	*2*	*3*	*4*	*5*
Fit the organizational culture, each organization provide different services.	*1*	*2*	*3*	*4*	*5*	*1*	*2*	*3*	*4*	*5*
Other Criteria you consider important? Please specify ____________________________ ____________________________	*1*	*2*	*3*	*4*	*5*	*1*	*2*	*3*	*4*	*5*

Please use this space if you wish to make any comments with respect to the formulation, application or effectiveness of Information security within your organization.

Appendix C

Grounded Theory

The grounded theory method was developed by the two sociologists Glaser & Strauss in 1967. Grounded theory is used to develop a theory from data rather than collecting data for testing a theory or hypothesis. Grounded theory is used in qualitative data to transform data into theory (Cohen et al., 2007) that is grounded in reality. Strauss & Corbin (1998, p. 12) explain that "*theory derived from data is more likely to resemble the reality… and will offer insight, enhance understanding, and provide a meaningful guide to action*". Grounded theory can, however, provide results that are difficult to generalize (Austen et al., 2003). For example, the interpretation of data depends on the context (social citing) of the participants.

Glaser & Strauss (1968) argue that the grounded theory differs from other research in that it begins with an area of study and allows relevant theory to emerge from that area. Using the grounded theory approach, the researcher first develops conceptual categories from the data and then makes new observations to clarify and elaborate these categories. Therefore, grounded theory should explain, as well as describe, in order to provide a theoretical explanation of the phenomena (Corbin & Strauss, 1990). Grounded theory has some characteristics, as described by Creswell (1994), such as constant evaluation of data with emerging categories and theoretical sampling of different groups to maximize the similarities and the differences of information.

Strauss & Corbin (1998, p. 9-10) argue that development of grounded theory recognises "*the need to get out into the field to discover what is really going on; the relevance of theory, grounded in data, to the development of a discipline of phenomena and of human action; the belief that persons are actors who take an active role in responding to problematic situations; the realization that persons act on the basis of meaning; the understanding that meaning is defined and redefined through interaction; a sensitivity to the evolving and unfolding nature of events; and an awareness of the interrelationships among conditions, actions, and consequences*".

Grounded theory consists of three types of coding for data analysis (Strauss & Corbin, 1998, p. 3):

- **Open coding**: Deals with labelling and categorizing the phenomena. To be able to identify related concepts and categories that have similar properties.
- **Axial coding**: Making connections between a category and its sub-categories. Axial coding joins data that was fractured during open coding (Strauss & Corbin, 1998, p. 124). The categories are formed from facts from the research data. They can be characterised into subcategories that identify answers to why, how, when, where, who and with what consequences, rrgarding categories (Goede & De Villers, 2003).
- **Selective coding**: Involves the integration of the categories that have been developed to find a connection between all the important categories in the research.

Coding is an analytical process, through which data moves from open, to axial, to selective coding, to form theory (Pandit, 1996). The aim is to recognize, build-up and relate the concepts that are the basic elements of theory (Goede & De Villers, 2003).

Grounded theory has been used in the field of computing (De Villiers, 2005; Cockton, 2004; Dourish et al. 2004; and Orlikowski, 1993). The grounded theory approach allows a focus on context-based explanation of the phenomena. Grounded theory develops conceptual categories from the qualitative data. New observations are made to clarify and elaborate these categories. The data has been categorized through identifying some patterns or themes and organized to bring meanings into categories.

Appendix D

The Percentages of the Occurrences and Severity of 12 Different Types of Security Breaches in Organization.

Type of Breach	Incidence of Breaches						Severity of Worst Breach				
	Approximate no. of breaches in last two years						*Quite Insignificant*		*Highly Significant*		
	0	<5	5-10	> 10	>100	>1000	1	2	3	4	5
Computer virus.	5% 2	43% 18	10% 4	21% 9	21% 9	0% 0	12% 5	24% 10	43% 18	19% 8	2% 1
Installation/ use of unauthorized hardware, peripherals.	12% 5	29% 12	17% 7	26% 11	17% 7	0% 0	17% 7	31% 13	36% 15	17% 7	0% 0
Abuse of computer Access controls.	17% 7	26% 11	19% 8	12% 5	26% 11	0% 0	12% 5	29% 12	38% 16	19% 8	2% 1
Physical Theft of Hardware / Software.	64% 27	19% 8	14% 6	0% 0	2% 1	0% 0	55% 23	31% 13	7% 3	5% 2	2% 1
Computer-based fraud.	45% 19	31% 13	19% 8	2% 1	2% 1	0% 0	59% 25	24% 10	10% 4	5% 2	2% 1
Human error. (Violation)	7% 3	21% 9	14% 6	17% 7	38% 16	2% 1	14% 6	19% 8	38% 16	24% 10	5% 2
Natural Disaster.	74% 31	24% 10	2% 1	0% 0	0% 0	0% 0	50% 21	29% 12	12% 5	7% 3	2% 1
Damage by Displeased Employee.	33% 14	41% 17	21% 9	5% 2	0% 0	0% 0	29% 12	50% 21	14% 6	7% 3	0% 0
Spam Emails. (Opining)	19% 8	38% 16	10% 4	12% 5	21% 9	0% 0	19% 8	24% 10	38% 16	19% 8	0% 0
Use of organization resources for illegal communications or activities. (porn surfing, e-mail harassment).	29% 12	29% 12	28% 12	7% 3	7% 3	0% 0	28% 12	33% 14	29% 12	10% 4	0% 0
Installation/ use of unauthorized software.	14% 6	38% 16	24% 10	12% 5	12% 5	0% 0	17% 7	33% 14	36% 15	14% 6	0% 0
Hacking incident (external).	31% 13	31% 13	21% 9	7% 3	10% 4	0% 0	29% 12	24% 10	33% 14	14% 6	0% 0

Percentages of Importance of Each Success Factors and Adoption of these Factors in Organization.

Factors	*How important do you believe the following factors to be for the successful implementation of Information security in your organization?*					*How successful do you believe your organization has been in adopting each of these factors?*				
	Not Important			**Very Important**		**Not Successful**			**Very Successful**	
Organization setting clear goals and objectives of information security	3% 1	0% 0	3% 1	41%1 4	53% 18	12% 4	26% 9	38%1 3	18% 6	6% 2
Implementation of information security with a consideration of organizational culture	0% 0	0% 0	9% 3	32% 11	59% 20	3% 1	21% 7	56% 19	21% 7	0% 0
Visible commitment from management	0% 0	0% 0	12% 4	32% 11	56% 19	6% 2	29% 10	38% 13	21% 7	6% 2
A clear understanding of security risks	0% 0	3% 1	3% 1	9% 3	85% 29	9% 3	12% 4	53% 18	24% 8	3% 1
A clear understanding of security requirements	0% 0	3% 1	3% 1	35% 12	59% 20	6% 2	21% 7	50% 17	18% 6	6% 2
Effective and ongoing awareness program of security to all employees	0% 0	3% 1	0% 0	15% 5	82% 28	9% 3	41% 14	29% 10	12% 4	9% 3
Putting information security policy in practice	0% 0	0% 0	9% 3	26% 9	65% 22	3% 1	18% 6	62% 21	12% 4	6% 2
Providing suitable employee training and education	0% 0	0% 0	3% 1	26% 9	71% 24	6% 2	32% 11	38% 13	15% 5	9% 3
Sufficient budget for information security.	0% 0	0% 0	3% 1	29% 10	68% 23	6% 2	29% 10	41% 14	18% 6	6% 2
Organization IT infrastructure	0% 0	0% 0	3% 1	38% 13	59% 20	3% 1	24% 8	41% 14	26% 9	6% 2

Percentages of Importance of Each Criteria of Security Policy and Adoption of these Criteria in Organization.

Criteria	*How important do you believe the following criteria to be for the successful implementation of Information security policy in your organization?*					*How successful do you believe your information security policy has been in adopting each of these criteria?*				
	Not Important		**Very Important**			**Not Successful**		**Very Successful**		
Explain what is acceptable activity is and what is not.	0% 0	0% 0	6% 1	61% 11	33% 6	0% 0	33% 6	44% 8	17% 3	6% 1
State the purpose of the policy and the scope of the organization.	0% 0	0% 0	6% 1	33% 6	61% 11	0% 0	28% 5	50% 9	22% 4	0% 0
Specify the job responsibilities.	0% 0	0% 0	11% 2	44% 8	44% 8	11% 2	33% 6	39% 7	17% 3	0% 0
Use a solid language rather than a abstract language.	0% 0	0% 0	22% 4	39% 7	39% 7	6% 1	28% 5	39% 7	28% 5	0% 0
Dynamic in order to cover the changes in the environment of information security.	0% 0	0% 0	17% 3	33% 6	50% 9	17% 3	33% 6	33% 6	17% 3	0% 0
Use simple language to ensure it is not difficult to understand.	0% 0	0% 0	6% 1	39% 7	55% 10	0% 0	22% 4	39% 7	22% 4	17% 3
Style consistent with the organizations generally communication style	0% 0	11% 2	0% 0	50% 9	39% 7	0% 0	44% 8	28% 5	17% 3	11% 2
Fit the organizational culture, each organization provide different services.	0% 0	0% 0	17% 3	39% 7	44% 8	6% 1	6% 1	44% 8	39% 7	6% 1

No.	Total of Reported Security Breaches
1	29
2	37
3	27
4	27
5	13
6	31
7	11
8	58
9	73
10	76
11	70
12	34
13	39
14	9
15	21
16	25
17	13
18	30
19	35
20	14
21	0
22	64
23	768
24	277
25	173
26	122
27	34
28	172
29	167
30	224
31	86
32	82
33	168
34	183
35	360
36	121
37	34
38	228
39	134
40	271
41	38
42	367

Analysis of the Research Questions

R1: Do organizations with a documented security policy reported fewer breaches than organizations with non-documented policy?

Ranks

	Is the information security policy documented?	N	Mean Rank	Sum of Ranks
Total reported security breaches	Yes	18	13.33	240.00
	No	16	22.19	355.00
	Total	34		

Test Statistics

	Total reported security breaches
Mann-Whitney U	69.000
Wilcoxon W	240.000
Z	-2.588
Asymp. Sig. (2-tailed)	.010
Exact Sig. [2*(1-tailed Sig.)]	.009

R2: Do organizations with a security policy report fewer security breaches?

Correlations

			Is the information security policy documented?
Kendall's tau_b	Total reported security breaches	Correlation Coefficient	-.112
		Sig. (2-tailed)	.387
		N	42

R3: Organization with a documented security policy experience fewer reported security breaches?

Correlations

			Is the information security policy documented?
Kendall's tau_b	Total reported security breaches	Correlation Coefficient	-.374
		Sig. (2-tailed)	.010
		N	34

R4: Organizations with a policy with a broader scope experience fewer reported security breaches?

Correlations

			Total reported security breaches
Kendall's tau_b	Border scope of the policy	Correlation Coefficient	-.219
		Sig. (2-tailed)	.052
		N	42

R6: Is there any difference in the number of reported security breaches between organizations reporting different levels of compliance of employees to the organization security policy?

Kruskal-Wallis Test	Total reported security breaches
Chi-Square	9.783
Df	4
Asymp. Sig.	.044

R7: Is there any difference in reported security breaches across number of employees?

Kruskal-Wallis Test	Total reported security breaches
Chi-Square	15.335
Df	6
Asymp. Sig.	.003

R8: Do organizations that report an effective security policy also report fewer security breaches?

Correlations

			How would you rate the overall effectiveness of your policy?
Kendall's tau_b	Total reported security breaches	Correlation Coefficient	-.340
		Sig. (2-tailed)	.013
		N	34

R10: Do organizations with a broader security policy report a more effective information security policy.

Correlations

			How would you rate the overall effectiveness of your policy?
Kendall's tau_b	Indicate the issues covered in your Information security policy?	Correlation Coefficient	.320
		Sig. (2-tailed)	.025
		N	34

R13: There is relationship between the reported effectiveness of the information security policy and the reported effectiveness at detecting and responding to information security breaches.

Correlations

			How would you rate your organization's effectiveness at detecting and responding to attempted information security breaches from your own employees?
Kendall's tau_b	How would you rate the overall effectiveness of your policy?	Correlation Coefficient	.757 .00
		Sig. (2-tailed)	34
		N	

Results of the Quantitative Questionnaire.

Section A: Background Information		
No.	1. Please specify your organization sector	2. No. of employees
1	Gov	2001-3000
2	Gov	2001-3000
3	Gov	2001-3000
4	Gov	500 - 1000
5	Gov	1001-1500
6	Gov	1001-1500
7	Gov	3001-5000
8	Gov	3001-5000
9	Gov	1001-1500
10	Gov	2001-3000
11	Gov	5001-10000
12	Gov	3001-5000
13	Gov	2001-3000
14	Gov	2001-3000
15	Gov	1001-1500
16	Gov	3001-5000
17	Gov	2001-3000
18	Gov	1001-1500
19	Gov	500-1000
20	Gov	1001-1500
21	Gov	5001-10000
22	Gov	1001-1500
23	Gov	1501-2000
24	Gov	1501-2000
25	Gov	less than 500
26	Gov	500-1000
27	Gov	500-1000
28	Gov	2001-3000
29	Gov	500-1000
30	Gov	less than 500
31	Gov	1001-1500
32	Gov	1001-1500
33	Gov	2001-3000
34	Gov	1501-2000
35	Gov	1501-2000
36	Gov	1501-2000
37	Gov	2001-3000
38	Gov	1501-2000
39	Gov	1001-1500
40	Gov	1001-1500
41	Gov	500-1000
42	Gov	1501-2000

Section B: Security Breaches to your Organization

3. Approximate no. of occurrences in last two years

No.	Computer Virus	Installation/ use of unauthorized hardware, peripherals.	Abuse of Computer Access Controls	Installation/ use of unauthorized hardware, peripherals.	Computer-based fraud
1	>10	<5	5- 10	<5	0.00
2	>10	>10	<5	>10	5-10
3	<5	<5	5-10	<5	0
4	<5	<5	<5	<5	<5
5	<5	0.00	0	0.00	0
6	<5	5-10	<5	5-10	<5
7	5-10	>10	0	>10	0
8	0	<5	<5	<5	0
9	<5	>100	<5	>100	0
10	>10	<5	<5	<5	0
11	<5	0	>10	0	>10
12	<5	5-10	<5	5-10	<5
13	5-10	5-10	>10	5-10	5-10
14	>10	0	0	0	0
15	<5	0	<5	0	0
16	<5	<5	<5	<5	<5
17	<5	<5	0	<5	<5
18	<5	<5	<5	<5	5-10
19	5-10	5-10	<5	5-10	<5
20	<5	<5	0	<5	0
21	0	0	0	0	0
22	<5	<5	0	<5	0
23	>100	>100	>100	>100	<5
24	>100	>10	>100	>10	5-10
25	>100	<5	>10	<5	0
26	>100	>10	>10	>10	0
27	<5	5-10	>10	5-10	<5
28	<5	>10	>100	>10	<5
29	>100	>10	>100	>10	0
30	5-10	>100	>100	>100	0
31	>10	>10	5-10	>10	0
32	>100	>10	5-10	>10	0
33	>100	>10	>100	>10	<5
34	>10	5-10	5-10	5-10	5-10
35	>100	>10	>100	>10	<5
36	<5	>10	>100	>10	0
37	>10	>100	5-10	>100	5-10
38	>10	5-10	>100	5-10	<5
39	<5	>100	5-10	>100	<5
40	>10	>100	>100	>100	5-10
41	<5	<5	5-10	<5	5-10
42	>100	>100	>100	>100	>100

No.	Spam Emails	Damage by Displeased Employee	Natural Disaster	Human mistakes
1	<5	<5	0	>10
2	<5	5-10	0	>10
3	<5	<5	0	>10
4	<5	<5	0	5-10
5	0	0	0	>10
6	<5	<5	<5	<5-10
7	0	0	0	<5
8	0	0	0	>100
9	<5	0	<5	<5
10	>100	<5	0	5-10
11	<5	0	0	>100
12	<5	5-10	0	5-10
13	5-10	<5	0	<5
14	0	0	0	5-10
15	<5	0	<5	5-10
16	0	0	<5	<5
17	<5	0	0	<5
18	5-10	0	5-10	0
19	<5	<5	<5	<5
20	0	0	0	<5
21	0	0	0	0
22	>100	0	0	>10
23	>100	>10	<5	>1000
24	>100	<5	<5	>100
25	<5	<5	<5	>100
26	0	<5	0	>100
27	>10	<5	0	0
28	<5	<5	0	>100
29	5-10	<5	0	>100
30	5-10	5-10	<5	>100
31	>10	<5	0	>10
32	>10	5-10	0	>10
33	<5	5-10	0	>100
34	>100	5-10	0	>100
35	>100	0	0	>100
36	<5	5-10	0	>100
37	<5	<5	0	<5
38	>100	>10	0	>100
39	>10	<5	0	>100
40	>100	5-10	0	>100
41	>10	5-10	0	<5
42	>100	<5	<5	>100

No.	Hacking incident (external)	Installation/ use of unauthorized software	Use of organization resources for illegal communication or activities(porn surfing, email harassment
1	<5	<5	<5
2	0	<5	5-10
3	<5	<5	<5
4	<5	<5	<5
5	0	<5	<5
6	<5	<5	<5
7	0	0	0
8	0	<5	0
9	0	>10	<5
10	0	5-10	>10
11	0	>10	0
12	<5	<5	<5
13	5-10	<5	5-10
14	0	0	0
15	<5	5-10	0
16	<5	<5	<5
17	0	0	0
18	<5	5-10	5-10
19	<5	<5	<5
20	0	<5	5-10
21	0	0	0
22	0	5-10	0
23	5-10	5-10	>100
24	5-10	>10	>100
25	>10	>100	0
26	<5	<5	5-10
27	5-10	5-10	5-10
28	<5	>100	0
29	0	<5	<5
30	>10	>100	5-10
31	>100	>10	5-10
32	<5	5-10	<5
33	5-10	0	0
34	5-10	5-10	5-10
35	>100	>100	>100
36	5-10	<5	0
37	5-10	0	0
38	>100	5-10	>10
39	5-10	5-10	>10
40	>100	>10	<5
41	<5	<5	5-10
42	>10	>100	5-10

Section B: Security Breaches to your Organization
Severity of worst incident

No.	Computer-based fraud	Physical Theft of Hardware/Software	Abuse of Computer Access Controls	Installation/ use of unauthorized hardware, peripherals.	Computer Virus
1	1	1	2	2	3
2	2	2	3	2	3
3	1	3	3	1	2
4	1	2	2	3	4
5	1	1	1	1	1
6	1	1	2	2	2
7	1	1	1	2	3
8	1	1	4	3	1
9	5	5	5	4	5
10	1	1	2	2	1
11	1	2	2	3	4
12	2	2	2	2	2
13	2	2	2	3	3
14	2	4	3	2	3
15	1	1	3	1	2
16	1	2	2	3	2
17	1	2	3	2	2
18	1	2	3	2	2
19	3	2	3	2	3
20	1	1	1	1	1
21	1	1	1	1	1
22	1	1	1	1	3
23	1	1	3	4	3
24	4	2	3	4	3
25	1	1	3	1	4
26	3	1	4	3	4
27	2	1	3	3	3
28	1	1	4	3	2
29	1	1	3	2	3
30	1	2	4	4	3
31	1	1	2	3	3
32	1	1	3	2	3
33	2	1	3	3	4
34	2	4	2	3	3
35	1	1	4	3	4
36	1	3	3	3	2
37	3	2	4	3	3
38	3	1	3	4	4
39	2	2	2	3	3
40	2	1	4	4	4
41	2	3	2	2	2
42	4	1	4	4	3

No.	Hacking incident (external)	Installation/ use of unauthorized software	Use of organization resources for illegal communication or activities(porn surfing, email harassment	Spam Emails	Damage by Displeased Employee	Natural Disaster	Human mistakes
1	1	2	2	1	2	1	3
2	3	2	2	3	2	3	2
3	3	4	3	2	1	3	1
4	4	4	3	3	3	2	3
5	1	1	1	1	1	1	2
6	1	1	2	1	2	2	3
7	1	1	1	1	1	1	2
8	1	1	3	1	1	1	5
9	1	3	4	4	4	5	1
10	1	2	2	3	1	1	2
11	4	4	3	3	3	2	3
12	2	2	2	2	2	1	3
13	3	2	3	3	2	4	3
14	4	1	2	4	4	3	4
15	1	3	1	2	1	4	4
16	2	2	1	2	1	2	1
17	1	2	1	1	2	2	2
18	2	3	2	3	1	3	1
19	3	3	2	3	2	3	2
20	1	2	1	1	1	1	2
21	1	1	1	1	1	1	1
22	1	2	1	2	1	1	3
23	3	3	4	4	4	2	4
24	2	3	3	4	2	2	4
25	2	3	1	2	2	1	4
26	2	2	2	2	2	2	4
27	3	3	3	3	2	1	1
28	3	3	2	3	2	1	3
29	2	2	2	3	2	1	3
30	3	4	3	3	3	2	3
31	4	4	2	4	2	1	3
32	2	2	1	3	2	1	3
33	2	2	1	2	2	1	3
34	3	3	3	3	3	2	3
35	4	4	4	4	1	1	4
36	3	3	2	2	2	1	3
37	3	3	1	3	2	1	2
38	4	1	3	4	3	4	4
39	3	3	3	3	2	1	4
40	3	3	2	4	3	2	4
41	2	2	3	2	2	2	3
42	3	3	4	3	2	1	5

Section C: Information Security Policy

No.	4. Have an Information security policy	5. If no, why	6. Is it documented	7. If no, why
1	yes		yes	
2	yes		yes	
3	yes		yes	
4	yes		yes	
5	yes		yes	
6	yes		yes	
7	yes		yes	
8	yes		no	in the process of implementation
9	yes		yes	
10	yes		yes	
11	yes		yes	
12	yes		yes	
13	yes		yes	
14	no	_	_	
15	yes		no	on process to do so
16	yes		no	
17	yes		yes	
18	yes		yes	
19	yes		no	no initiative taken
20	yes		yes	
21	no	_	_	_
22	yes		no	in process
23	yes		yes	
24	yes		yes	
25	yes		no	_
26	yes		no	in process
27	no	_	_	_
28	yes		no	working on having policy
29	yes		no	no clear authority to do so
30	yes		no	_
31	yes		no	in process
32	no	-	_	_
33	no	_	_	_
34	no	-	_	_
35	yes		no	_
36	yes		yes	
37	no	-	_	_
38	yes		no	less effort
39	yes		no	_
40	yes		no	_
41	no	_	_	_
42	yes		no	_

No.	8. How long	9. Distributed policy	10. Effectiveness of the policy	11. Effectiveness at detecting to breaches
1	6	organization intranet	effective	very effective
2	2	Other	Neither	Neither
3	1	staff handbook	Neither	Neither
4	2	None	Neither	Neither
5	5	other-circulation	effective	very effective
6	3	staff handbook	Neither	Neither
7	5	staff handbook	effective	effective
8	_	staff handbook	very effective	effective
9	6	other-circulation	very effective	very effective
10	6	staff handbook	effective	Neither
11	6	staff handbook	effective	effective
12	2	organization intranet	effective	effective
13	5	staff handbook	effective	effective
14	_	_	_	_
15	_	other - awarness classes	effective	somewhat effective
16	_	organization intranet	effective	effective
17	10	staff handbook and other presentations	effective	effective
18	4	staff handbook	Neither	somewhat effective
19	_	_	Neither	Neither
20	5	staff handbook	effective	effective
21	_	_	_	_
22	_	other-verbal briefing	effective	effective
23	5	staff book	Neither	Neither
24	10	organization intranet	effective	effective
25	_	memo circulation	effective	Neither
26	_	Other	Neither	somewhat effective
27	_	_	_	_
28	_	other-memo	Neither	Neither
29	_	other- internal memo	Neither	Neither
30	_	Other	Neither	Neither
31	_	Other	somewhat effective	somewhat effective
32	_	_	_	_
33	_	_	_	_
34	_	_	_	_
35	_	Other	not at all effective	not at all effective
36	1	organization intranet	effective	effective
37	_	_	_	_
38	_	Other	Neither	Neither
39	_	Other	Neither	Neither
40	_	Other	Neither	somewhat effective
41	_	_	_	_
42	_	Other	somewhat effective	somewhat effective

No	12. Legislation is important	13. Rate the success when there is legislation	14. How to check compliance	15. How often to check compliance
1	yes	very successful	from Audit function	monthly
2	no	Neither	Audit	monthly
3	no	Neither	Audit	monthly
4	no	Neither	Audit	unknown
5	yes	successful	logging software	unknown
6	no	Neither	Audit	monthly
7	yes	successful	Audit	monthly
8	yes	very successful	Audit	monthly
9	yes	successful	Audit	unknown
10	yes	successful	sudden visits, system logs, questionnaires during security awareness program	monthly
11	no	Neither	regular check to users workstations and offices	unknown
12	yes	successful	Audit	monthly
13	yes	successful	Audit	monthly
14	_	_	_	_
15	yes	very successful	through network monitoring, network policy (implementing)	monthly
16	yes	successful	Audit	monthly
17	yes	successful	regular audit	monthly
18	no	Neither	normal check	monthly
19	no	Neither	nothing	unknown
20	yes	successful	first by test and then by having checklist done periodically showing some key components of the security policy done and understood	unknown
21	_	_	_	_
22	yes	successful	Random check	quartly
23	yes	successful	using information security audit	quartly
24	yes	very successful	normal audit	monthly
25	yes	successful	normal audit	annually
26	yes	successful	none	unknown
27	_	_	_	_
28	yes	successful	none	unknown
29	yes	successful	by doing the follow up	unknown
30	yes	successful	none	unknown
31	yes	successful	none	unknown
32	_	_	_	_
33	_	_	_	_
34	_	_	_	_
35	yes	successful	audit	less often annually
36	yes	successful	Audit	monthly
37	_	_	_	_
38	yes	successful	none	unknown
39	no	Neither	none	unknown
40	yes	successful	none	unknown
41	_	_	_	_
42	no	somewhat successful	none	unknown

No	16.Do you record the number of security breaches	17.Are all computer regularly tested	18. Are all computers protected	19. How the systems are kept updated
1	yes	yes	yes	antivirus is distributed at routine bases
2	yes	yes	yes	Preventive Maintanance
3	yes	yes	yes	normal/ routine audit
4	No	yes	yes	normalcheck using software
5	no	yes	yes	regular updates through the network
6	yes	yes	yes	regular updates
7	yes	yes	yes	regular updates
8	no	yes	yes	regular updates
9	yes	yes	yes	by dedicating qualified team for each system
10	yes	no	yes	the updates are schedualed to happen automatically
11	no	yes	yes	management software by pushing updates and forcing the instalation automatically
12	yes	yes	yes	using different softwares
13	yes	yes	yes	maintanance
14	_	_	_	_
15	yes	no	yes	automated update through network after downloading new updated patches from internet then upload to our network.
16	yes	yes	yes	maintanance
17	yes	yes	yes	maintanance
18	yes	yes	yes	using different softwares
19	yes	yes	yes	normal update
20	yes	no	yes	updates and apply new versions of softwares
21	_	_	_	_
22	No	no	yes	frequent manual updates
23	yes	yes	yes	maintanance
24	yes	yes	yes	regular check and updates
25	no	yes	yes	regular updates
26	yes	yes	yes	none
27	_	_	_	_
28	No	yes	no	none
29	yes	yes	yes	regular update
30	yes	yes	yes	none
31	No	no	no	none
32	_	_	_	_
33	_	_	_	_
34	_	_	_	_
35	No	yes	yes	none
36	yes	yes	yes	Preventive Maintanance
37	_	_	_	_
38	yes	yes	no	daily check
39	yes	yes	yes	none
40	yes	yes	yes	none
41	_	_	_	_
42	No	no	no	none

20. Using the table below, please indicate the issues covered in your Information security policy. If you do not clearly cover an issue through your policy please leave blank.

No.	Define Responsibilities	Disclosure of information	Viruses, Worms & trojans	Internet access	Use of Organization systems & network	User login responsibilities
1	yes	Yes	yes	yes	yes	yes
2	yes	Yes	yes	yes	yes	yes
3	yes	Yes	yes	yes	yes	yes
4	no	No	yes	no	no	yes
5	yes	Yes	no	no	no	yes
6	yes	Yes	yes	yes	yes	yes
7	yes	Yes	yes	yes	yes	yes
8	yes	Yes	yes	yes	yes	yes
9	no	No	no	yes	yes	no
10	yes	Yes	yes	yes	yes	yes
11	no	Yes	yes	yes	yes	yes
12	yes	Yes	yes	yes	yes	yes
13	yes	Yes	yes	yes	yes	yes
14	_	_	_	_	_	_
15	yes	Yes	yes	yes	yes	yes
16	yes	Yes	yes	yes	yes	yes
17	no	Yes	yes	yes	yes	yes
18	yes	Yes	yes	yes	yes	yes
19	no	Yes	yes	yes	yes	yes
20	yes	Yes	yes	yes	yes	yes
21	_	_	_	_	_	_
22	yes	Yes	yes	yes	yes	yes
23	no	Yes	yes	yes	yes	yes
24	no	Yes	yes	yes	yes	yes
25	no	No	yes	no	yes	yes
26	yes	Yes	yes	yes	yes	yes
27	_	_	_	_	_	_
28	no	No	yes	yes	yes	yes
29	no	No	yes	no	yes	yes
30	no	No	yes	no	no	yes
31	no	No	yes	yes	yes	yes
32	_	_	_	_	_	_
33	_	_	_	_	_	_
34	_	_	_	_	_	_
35	yes	No	yes	no	yes	yes
36	yes	Yes	yes	yes	yes	yes
37	_	_	_	_	_	_
38	no	No	no	no	no	no
39	no	No	yes	yes	yes	yes
40	no	No	yes	no	yes	yes
41	_	_	_	_	_	_
42	no	No	no	no	no	no

No.	Feedback system for suggesting policy improvements	Explain the consequences of violations and breaches	Personal usage of organization resources	Adoption of some standards
1	yes	yes	yes	yes
2	yes	yes	yes	yes
3	yes	yes	yes	yes
4	no	No	yes	no
5	no	yes	no	no
6	yes	yes	yes	yes
7	yes	yes	yes	no
8	no	yes	yes	no
9	no	No	yes	yes
10	no	yes	yes	no
11	no	yes	no	yes
12	yes	yes	yes	yes
13	yes	yes	yes	yes
14	_	_	_	_
15	no	yes	yes	no
16	no	No	yes	no
17	no	yes	yes	no
18	no	yes	yes	yes
19	no	No	yes	no
20	no	yes	yes	no
21	_	_	_	_
22	no	yes	yes	no
23	no	No	yes	no
24	no	No	yes	yes
25	no	No	yes	no
26	no	No	yes	no
27	_	_	_	_
28	no	No	yes	no
29	no	No	yes	no
30	no	No	no	no
31	no	No	no	no
32	_	_	_	_
33	_	_	_	_
34	_	_	_	_
35	no	No	yes	no
36	yes	yes	yes	yes
37	_	_	_	_
38	no	No	no	no
39	no	No	no	yes
40	no	No	no	no
41	_	_	_	_
42	no	No	no	no

Section D: The Success of your Information Security.

21. Using the table below, please indicate the **importance** of each of the following factors and the extent to which your organization is **successful** in adopting them.

(How Important each of the following factors).

No.	security risks	management	organizational culture	clear goals and objectives
1	5	5	5	5
2	5	4	4	4
3	5	4	5	5
4	5	5	4	4
5	5	3	4	4
6	5	5	4	4
7	5	3	5	4
8	5	5	5	5
9	2	3	4	1
10	5	5	5	3
11	5	5	5	4
12	5	4	4	5
13	5	4	5	4
14	_	_	_	_
15	5	5	4	5
16	5	5	5	5
17	4	4	4	5
18	5	5	5	5
19	5	4	5	5
20	5	3	3	4
21	_	_	_	_
22	5	5	3	5
23	5	5	5	4
24	4	4	3	4
25	3	4	5	5
26	5	5	5	5
27	_	_	_	_
28	5	4	4	5
29	5	5	5	4
30	5	5	5	4
31	5	4	5	5
32	_	_	_	_
33	_	_	_	_
34	_	_	_	_
35	5	5	5	5
36	5	5	5	5
37	_	_	_	_
38	5	5	4	5
39	5	5	5	4
40	4	4	4	4
41	_	_	_	_
42	5	5	5	5

No.	IT infrastructure	sufficient budget	training and education	policy in practice	ongoing awareness	security requirement
1	4	4	5	5	5	5
2	4	5	4	4	5	4
3	5	5	5	4	5	4
4	5	5	5	4	5	5
5	5	4	5	5	5	5
6	4	4	5	4	4	4
7	4	4	3	4	5	5
8	4	4	5	5	4	5
9	3	3	4	3	2	2
10	5	5	5	5	5	4
11	4	5	4	5	4	5
12	5	4	5	4	5	4
13	5	4	4	5	5	4
14	_	_	_	_	_	_
15	5	5	4	3	5	4
16	5	5	5	5	5	5
17	5	5	4	3	5	4
18	5	5	5	5	5	5
19	5	4	5	4	5	5
20	4	5	4	4	5	4
21	_	_	_	_	_	_
22	5	5	5	5	5	5
23	4	5	5	5	5	4
24	4	4	4	4	4	3
25	5	5	5	5	5	5
26	5	5	5	5	5	5
27	_	_	_	_	_	_
28	5	5	5	5	5	5
29	4	5	5	5	5	5
30	5	5	5	5	4	5
31	4	5	5	5	5	5
32	_	_	_	_	_	_
33	_	_	_	_	_	_
34	_	_	_	_	_	_
35	5	5	5	5	5	5
36	5	5	5	5	5	5
37	_	_	_	_	_	_
38	4	5	5	5	5	4
39	5	5	5	5	5	5
40	4	4	4	5	5	4
41	_	_	_	_	_	_
42	5	5	5	5	5	5

(How **successful** do the organization has been adopting each of these factors)

No	security requirement	security risks	management	organizational culture	clear goals and objectives
1	4	4	4	3	4
2	2	3	2	3	2
3	4	2	3	2	3
4	3	3	2	3	3
5	3	3	3	3	4
6	2	2	3	3	2
7	4	4	2	3	3
8	3	3	4	4	5
9	2	3	4	3	1
10	3	4	4	3	2
11	4	3	2	4	2
12	2	3	2	3	2
13	3	3	2	3	2
14	_	_	_	_	_
15	3	4	5	4	4
16	3	3	2	3	3
17	3	3	3	3	4
18	3	2	3	2	3
19	3	2	3	2	3
20	3	4	3	3	4
21	_	_	_	_	_
22	4	4	4	4	3
23	4	5	5	4	5
24	3	3	4	3	4
25	5	4	3	4	3
26	3	3	2	3	3
27	_	_	_	_	_
28	3	3	3	3	2
29	2	3	2	2	2
30	2	1	2	2	1
31	2	3	3	3	2
32	_	_	_	_	_
33	_	_	_	_	_
34	_	_	_	_	_
35	3	3	3	2	3
36	5	4	4	4	3
37	_	_	_	_	_
38	1	1	1	2	1
39	3	3	3	3	3
40	3	3	3	3	3
41	_	_	_	_	_
42	1	1	1	1	1

No	IT infrastructure	sufficient budget	training and education	policy in practice	ongoing awareness
1	4	4	5	4	5
2	2	2	2	3	2
3	5	5	4	3	4
4	2	3	2	3	2
5	4	4	3	3	2
6	2	2	2	3	2
7	3	3	2	3	5
8	4	4	4	4	4
9	3	3	5	3	3
10	4	2	2	3	2
11	3	2	3	3	2
12	3	2	3	3	2
13	3	2	2	2	3
14	_	_	_	_	_
15	5	5	4	4	3
16	2	3	3	3	2
17	4	3	2	2	2
18	3	3	2	3	2
19	3	3	3	3	2
20	4	3	3	4	3
21	_	_	_	_	_
22	3	4	5	5	3
23	4	4	4	5	5
24	4	4	4	3	4
25	3	2	1	3	2
26	3	3	3	3	3
27	_	_	_	_	_
28	3	2	3	3	3
29	3	2	2	2	1
30	2	2	2	2	2
31	2	3	3	2	3
32	_	_	_	_	_
33	_	_	_	_	_
34	_	_	_	_	_
35	2	3	3	3	2
36	4	3	3	3	4
37	_	_	_	_	_
38	2	1	2	2	1
39	3	3	3	3	3
40	3	3	3	3	3
41	_	_	_	_	_
42	1	1	1	1	1

Section E: The Criteria of Information Security Policy.

22. In order to have an effective information security policy, an organization should select a set of criteria to be implemented accurately and to give good results.

(How importance of each of the following criteria)

No	fit organization culture	style consistent	use simple language	dynamic to cover changes	solid language	job responsibilities	purpose of the policy	explain what is acceptable and non
1	4	4	4	4	4	3	4	4
2	5	5	5	5	4	5	5	5
3	5	5	4	5	5	5	5	4
4	5	5	5	4	5	5	5	4
5	4	4	5	4	3	3	4	4
6	5	4	4	5	5	4	5	4
7	4	2	3	3	3	4	3	3
8	4	4	4	3	3	4	4	5
9	5	5	5	5	5	5	5	5
10	3	4	5	3	5	4	5	4
11	4	5	5	4	4	4	4	5
12	3	4	5	5	4	5	5	5
13	5	4	5	5	4	5	5	4
14	4	4	4	4	5	4	4	4
15	_	_	_	_	_	_	_	_
16	_	_	_	_	_	_	_	_
17	4	4	5	5	3	4	5	4
18	5	5	4	5	5	5	5	4
19	5	5	5	4	5	5	5	4
20	3	2	4	4	4	4	4	4
21	_	_	_	_	_	_	_	_
22	4	4	5	5	5	5	5	5
23	_	_	_	_	_	_	_	_
24	4	4	4	4	4	4	4	4
25	_	_	_	_	_	_	_	_
26	5	5	5	5	5	5	5	5
27	_	_	_	_	_	_	_	_
28	5	5	5	5	4	5	5	5
29	4	4	4	4	5	5	4	4
30	4	4	4	4	4	3	4	4
31	5	4	5	5	5	5	5	4
32	_	_	_	_	_	_	_	_
33	_	_	_	_	_	_	_	_
34	_	_	_	_	_	_	_	_
35	5	5	5	5	5	5	5	5
36	5	5	5	5	5	5	5	5
37	_	_	_	_	_	_	_	_
38	5	5	5	5	5	5	5	5
39	5	5	5	5	5	5	5	5
40	5	5	5	5	5	5	5	5
41	_	_	_	_	_	_	_	_
42	5	5	5	5	5	5	5	5

(How **successful** in adopting each of the following criteria)

No	fit organization culture	style consistent	use simple language	dynamic to cover changes	solid language	job responsibilities	purpose of the policy	explain what is acceptable and non
1	4	4	4	2	3	3	3	3
2	3	2	3	1	2	2	2	2
3	4	2	3	4	2	2	3	3
4	4	2	5	2	4	2	3	3
5	4	5	3	3	4	3	3	2
6	3	3	2	2	3	3	2	3
7	4	2	2	3	2	4	3	3
8	5	5	5	3	3	4	4	5
9	3	3	4	4	4	3	4	4
10	3	3	3	2	2	3	3	3
11	2	3	4	3	3	3	3	4
12	3	2	3	2	3	2	3	2
13	3	3	3	3	3	2	2	3
14	_	_	_	_	_	_	_	_
15	_	_	_	_	_	_	_	_
16	2	2	2	2	2	3	3	4
17	3	2	2	2	3	2	3	2
18	1	2	2	1	1	1	2	2
19	3	3	1	3	4	4	3	3
20	3	2	3	1	2	1	2	2
21								4
22	1	4	4	4	4	4	3	5
23	_	_	_	_	_	_	_	_
24	4	4	5	3	4	3	4	3
25	_	_	_	_	_	_	_	_
26	3	2	3	2	3	2	3	2
27	_	_	_	_	_	_	_	_
28	1	1	1	1	1	1	1	1
29	2	3	2	3	2	3	2	2
30	3	3	2	3	3	2	3	3
31	2	2	2	1	2	1	2	2
32	_	_	_	_	_	_	_	_
33	_	_	_	_	_	_	_	_
34	_	_	_	_	_	_	_	_
35	2	1	1	1	1	3	2	2
36	4	4	4	4	4	4	4	4
37	_	_	_	_	_	_	_	_
38	1	1	1	1	1	1	1	1
39	3	3	3	3	3	3	3	3
40	3	3	3	3	2	3	3	2
41	_	_	_	_	_	_	_	_
42	1	1	1	1	1	1	1	1

Appendix E

Qualitative Interview Questions *Compliance*

Name of the Organization:
Current Position:
Date/Time of Interview:

<u>Section A</u>: Organization's Security Policy

1. **How long have you been with the organization?**

2. **Does your organization have a security policy? If no go to Q8.**

3. **Do you know what the policy contains? If no go to Q8.**

4. **Can you please give some examples of what your organization security policy contains?**

5. **Does the current security policy, you mentioned to me, work properly?**

6. **Do you think the organization checks employee compliance to the policy, you mentioned to me? If yes how, if no explain please.**

7. **How is this policy enforced in your organization?**

8. **To whom do you report security problems (for example, someone calling and asking about your password)?**

<u>Section B</u>: Organization Culture

9. **I would like to hear your view on the organization itself? What is it like working here?**

9.1 Which of the following descriptions best fits in your organisation?

a. **Employees perform tasks because they must, rather than because they agree with the actions and decisions of senior management.**

b. **Employees will do as senior management wishes because of an incentive system and not because they necessarily agree with senior management.**

c. **Employees identify with the organization and share the same beliefs and values of senior management and they are willingly striving towards the vision of their senior management for information security in the organization.**

10. If a serious information security incident (for example: virus spread in the organization because someone clicked on an email attachment) occurred in a place you have some responsibility for, what are the steps you think should be taken to deal with the situation? Would you deal with it yourself or turn it over to the professionals in the organization?

Section C: Compliance (Skip if no security policy)

I: Questions

11. Do you always comply with the policy you mentioned?

12. In your opinion what is the potential impact on the organization if the employees do not follow the policy you mentioned?

13. Under what circumstances would you not follow the policy you mentioned?

II: Scenarios

14. Can you please give me your opinion in some people's behaviour in different situations? Please tell me, what should they do? Why? What do you predict will happen? Under what circumstances would they be more inclined to do this?

a) Your boss's secretary leaves her PC unattended when she leaves for a lunch break. She shares her office with other colleagues.

b) (Paul/Amanda) receives in his/her office an email with an executable file attached to it. He/She trusts the person the email came from.

c) (Chris/Stacy) is working on a confidential assignment assigned by his/her boss. He/she saved the work on his/her company PC. One day he/she was ill and could not go to work. His/her colleague phoned him/her asking about her password to get some files from his/her machine.

d) (Chris/ Rebecca) have too many passwords and cannot remember them. A friend tells him/her to write them on sticky notes and paste them inside her drawer.

e) (Robin/ Sally) noticed that one of her colleagues was using organization resources for illegal web surfing e.g. (porn surfing, email harassment). What do you think the organisation wants him/her to do? What pressures do you think he/she experiences in making him/her decision?

f) Some people are distributing CDs at central station early morning, saying that the CDs contain a special Valentine's Day promotion. (Chris / Rebecca) also got a CD there. What should s/he do with the CD?

III: Information Security Policy (*show the interviewee a copy of security policy and ask the following*)

15. In your opinion what would make you follow this policy?

16. In your opinion, under what circumstances would you not follow this policy?

In your opinion, what do you think might be the underlying reasons that would explain why employees don’t comply with an organization security policy?

INFORMATION SECURITY POLICY (SAMPLE)

Introduction

This policy highlights to employees what is acceptable use and non acceptable use of the University system and what will happen if the rules are not followed. This policy applies to all University owned equipment.

Purpose

The purpose of this policy is to help the employee to implement the best use of the University computer system. Inappropriate use exposes the University to risks and legal issues.

Scope

This policy is for all employees, consultants of the University.

The employee needs to understand the following:

1. This policy is based on the University information security policies. These policies are available from the employee manager or in the University intranet.
2. University adopts some information security law such as an international standards organization ISO 17799, Copyright, Designs and Patents Act 1988, Malicious Communications Act 1988, Computer Misuse Act 1990, Criminal Justice and Public Order Act 1994, Trade Marks Act 1994, Data Protection Act 1998, Human Rights Act 1998, Regulation of Investigatory Powers Act 2000, Freedom of Information Act 2000 and Communications Act 2003.
3. Employees are responsible for protecting the data, information as well as any resources in their location.
4. Employees are responsible on what they do on the University system.
5. Security is every once responsibility in this University.
6. If there is any uncertainty, employees should consult their manager and in case of observing abnormal behaviour the employees should inform their manager immediately.
7. The employees should recognize what is confidential data and what is not. If they are not sure, they must ask.
8. Information security policies are subject to change. If changes are made employees will be notified by their manager and electronic mail.
9. System, Network and Internet are to be treated as University resources.
10. This policy is affective from the date that the employee sign in the University until terminates their association with the University.
11. Failure to fulfil with the university information security policy may lead to disciplinary actions.

It is the responsibility of every employee using the University computer system to follow the following guidelines:

Responsibilities

- Notify the Chief Security Officer if sensitive or critical University information is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties or if any unauthorized use of University's information systems has taken place, or is suspected of taking place;

Passwords

- DO NOT use familiar names;
- Avoid using commonly known facts about yourself;
- DO NOT use words found in the dictionary;
- Use at least eight (8) characters;

- Utilize both letters and numbers;
- Use special characters, if possible;
- Use upper- and lower-case letters, if possible;
- Combine misspelled words;
- DO NOT share your password with anyone;
- Never write down your password;
- DO NOT store your password in a computer file;
- When receiving technical assistance, enter your password instead of telling it to the technology staff member;
- If you ever receive a telephone call from someone claiming to need your password, report it immediately;
- DO NOT save fixed passwords in web browsers or electronic mail clients when using a system that contains critical or sensitive information or has access to a University critical resource. Anyone with physical access can use the workstations to both accesses the Internet with their identities, as well as read and send their electronic mail;

PC and Laptop Security

- Lock your office door when you leave;
- Logout of the system when you are finished working;
- Logout of the system when you are away from your workstation;
- DO NOT remove any assets tags from University equipment;
- DO NOT use your personal PC or Laptop within the university system without permission by the appropriate authorizing authority.

Software Security

- Install software through approved methods by the appropriate authorizing authority;
- DO NOT establish Internet or other external network connections that could allow non-University users to gain access to University systems with critical or sensitive information unless prior approval has been received by the appropriate authorizing authority;
- DO NOT illegally copy software without written permission by the appropriate authorizing authority;
- DO NOT reproduce copyrighted material without written permission by the appropriate authorizing authority.

Anti-Virus

- Always use anti-virus software on your computer;
- Make sure your anti-virus software is up to date;
- Scan all files downloaded from the Internet;
- Scan all email attachments;
- Scan diskettes, memory sticks and CDs before use;
- Report all virus incidents as soon as possible to your department. If you have a computer virus threat to report, please email security@university.ac.uk.

Document Security

- Maintain a "clean desk" and keep your work space secured; i.e., lock up any sensitive files, diskettes and CD's;
- Shred any confidential documents when you are discarding them;

- Remove papers and wipe boards clean when finished using conference rooms;
- Lock filing cabinets when you leave;
- DO NOT leave documents unattended on the copier or fax machine;
- Employ adequate encryption technology for sensitive or critical information such as educational records, student identification numbers, and credit card numbers to minimize the risk associated with spoofing, eavesdropping, and tampering; Email infosec@university.ac.uk_for specific information regarding encryption technology options;
- DO NOT leave documents unattended on the copier or fax machine;
- DO NOT discuss information security related incidents with individuals outside of the University or inside the University who do not have a need to know;
- DO NOT distribute internal critical or sensitive University communications to external entities that are not affiliated with the University and only distribute to internal entities on a need to know basis;
- DO NOT place University sensitive or critical information in any computer unless the persons who have access to that computer have a legitimate need-to-know the involved information;
- DO NOT post University material such as software, internal memos, or policies on any publicly-accessible Internet computer which supports anonymous FTP or similar publicly-accessible services, unless the posting of these materials has first been approved by the appropriate approval authority.

Email

- You may use the University network to send and receive personal email;
- You are not allowed to spread messages or emails that contain offensive materials;
- You must delete spam emails;
- You are not allowed to open, forward or reply any spam emails;
- You are not allowed to use the organization email for commercial purposes.

Appendix F

Policy A

This document defines the policies to be followed by staff employed by Jacobs and all its subsidiaries (referred to as 'the company' in this document) relating to computer usage, Internet, e-mail and computer security.

This policy is communicated to all employees on joining and should be implemented in conjunction with security awareness training made available to all staff. All staff are expected to bring new security threats, often identified during or as a result of security awareness training, to the attention of management so that this security policy can be updated as appropriate.

The company's IT resources comprise, without limitation, any computer (including laptops issued for off-site use), server or data network, and any telephone handset, video conferencing system, switchboard or voice network provided or supported by the company, and includes interface with and use of public networks in conjunction with the company's IT facilities.

Use of the IT facilities includes the use of data/programs stored on the company's computer systems, data/programs stored on magnetic tape, floppy disk, CD-ROM or other storage media that is owned and/or maintained by the company.

The e-mail facility and access to the Internet and client intranets provided by the company are intended to promote effective communication for the company and its clients on business matters. The company reserves the right to temporarily or permanently limit, withdraw or restrict use of, or access to, any IT facilities if they are used, in the company's sole opinion, in an inappropriate manner.

The purpose of these guidelines is to ensure that all of the company's users use the company's IT facilities in an effective, efficient, and ethical manner, and also to avoid the risk of the company and individual employees facing legal liability as a result of improper use, whether inadvertent or deliberate. Persistent breach of this IT policy and/or misuse of the company's IT facilities is a disciplinary offence and, in appropriate circumstances, will lead to disciplinary action being taken against you, including summary dismissal.

Legal Framework for Information Technology

- Data Protection Act 1998 regulates the use of computerised personal information.
- Copyright designs and Patents act 1998 includes regulations concerning the copying of software and computer programs.
- Computer Misuse Act 1990 defines criminal offences related to the use of computers.

1 Computer system policy

1.1 Software

1.1.1 Attachments which arrive via e-mail are virus-scanned as are software packages installed from the Web or removable media such as CD-ROM. However if you have not connected to the network for some time your virus scanning software could be out of date. Care should always be exercised and if there is any doubt seek advice from the IT service delivery team. (Also see 1.2 below).

1.1.2 All software used on any of the company's computers must be approved in advance by the IT Service Delivery Team. Only personnel authorised by the IT Service Delivery Team or the Head of Systems may load software onto any of the company's computers, connect any hardware or other equipment to any such computers or move or change any such computer equipment.

1.1.3 You must not make any copies of software except where this is expressly permitted by the copyright owner or as permitted by law. It is not permitted to use software for which the company does not own a current user licence. The making of 'extra' copies of software or the introduction of software packages from sources outside the organisation is expressly prohibited. The IT Service Delivery Team retains the legally-permitted back-up copies of all software used in the business and it should not be necessary for you to make copies for back-up purposes. The company has committed itself to obeying the user guidelines accepted in the industry and the company's reputation could be damaged if it were found to have infringed those guidelines.

1.1.4 If you have unlicensed software on a machine for which you are responsible, please remove it. This applies whether or not you actually use the software. If you are unsure whether you have a licence for a particular package, check with the IT Service Delivery Team. Where you are supplied software on a trial basis, you should delete it at the end of the specified time or purchase a licence. The company is committed to operating a fair policy on software purchase and will consider abuses seriously.

1.1.5 If you have a real need for a particular package, consult the IT Service Delivery Team.

1.2 System integrity

1.2.1 It is the responsibility of each user to take all reasonable precautions to safeguard the security of the computer and the information contained upon it. This includes protecting it from physical hazards, including spilling liquids; not allowing unauthorised users access to the machine; and only using approved software.

1.2.2 Our business is vulnerable to computer viruses and to trojan horses. Trojan horses are programs which contain unauthorised instructions, included by the programmer for malicious purposes. While the program performs the action expected by the user, it also has unseen effects (e.g. secretly storing or transmitting confidential information).

1.2.3 An anti-virus software package is installed on each PC in the network and you should run this package to check removable media (such as floppy disks or USB 'pen drives') before you use them. However, please do not totally rely on this software to protect your computer; you must adhere to the other precautions outlined in this policy statement.

1.2.4 Advice should be sought before using any media from a questionable source on your own PC.

1.2.5 Only media supplied by the IT Service Delivery Team should be used. If you are away from the office and need a supply of disks, then buy only branded disks from a reputable manufacturer.

1.3 Passwords and security

1.3.1 You are responsible for the security of your terminal, PC or laptop and for protecting any information or other data used and/or stored on your terminal, PC or laptop.

1.3.2 You must not make copies of system configuration files for your own, unauthorised personal use or to provide to other people/users for unauthorised uses.

1.3.3 You must not allow your PC/terminal to be used by an unauthorised person.

1.3.4 You must keep your passwords confidential and change them regularly. You may not disclose them to anyone, including IT staff.

1.3.5 When leaving your PC/terminal unattended or on leaving the office, you must ensure that you log off the system to prevent unauthorised users using your terminal in your absence.

1.4 Laptops/portable and handheld computers/remote use

Each individual is responsible for the portable computer they use and must ensure that the correct procedures are followed.

1.4.1 You must not disclose dial-up or dial-back modem phone numbers to anyone.

1.4.2 When accessing the company's IT facilities remotely, you must not disclose your passwords to anyone, for any reason.

1.4.3 Do not leave portable computers unattended.

1.4.4 Store portables in secure cabinets when not in use.

1.4.5 Users of portables should be vigilant in public places, as theft is common.

1.4.6 Do not display sensitive information in a public place where the screen could be overlooked.

1.4.7 No sensitive information should be held on the hard disk.

1.4.8 Any removable/transportable media containing sensitive information should not be held with the computer.

1.4.9 Use a carrying case to reduce the risk of accidental damage.

1.4.10 Ensure that back-ups are made.

1.4.11 Never loan the portable computer to anyone, including other employees of the company, without prior approval from the IT Service Delivery Team.

1.4.12 If you are supplied with a loan portable computer, you must sign an acceptance form supplied by the IT Department. If you wish to remove the item from the premises, you must obtain authorisation from the IT Service Delivery Team by completing an IT Equipment Removal Request.

1.5 Unauthorised access

1.5.1 To protect the company's computer systems and records and to preserve confidentiality, access to the company's IT facilities is controlled.

1.5.2 You must not access any part of the IT facilities for which you do not have authorisation.

1.5.3 If you have a legitimate business reason for wishing to access data or programs for which you do not have authorisation, you may only do so with the express authority of the IT Service Delivery Team and/or the Managing Director.

1.5.4 Use on, or in connection with, any part of the company's IT facilities, of programs, utilities and/or any other device designed to:

- circumvent security measures,
- determine or identify passwords, or
- breach conditional access systems, whether belonging to the company or to third parties, will be treated as a serious disciplinary matter which, depending on the severity of the case, could lead to your dismissal from the company.

2 E-mail policy

2.1 The e-mail system is the company's property and the company reserves the right to monitor and to access any messages in the system.

2.2 Never send messages that are abusive, sexist, racist or defamatory. The content of e-mails could be used within a legal action and the same caution should be exercised as with any written medium.

2.3 Improper statements can give rise to legal action against you and/or the company. Remember that advice given by e-mail may be relied upon and contracts may be created by e-mail.

2.4 The mere deletion of a message or file may not fully eliminate it from the system - it may be traced and retrieved at a later date.

2.5 Always remember that e-mail messages, however confidential or damaging, may have to be disclosed in court proceedings if relevant to the issues.

2.6 E-mail messages sent externally may be accessed by others. Confidential information should not be sent externally by e-mail without express authority from the client.

2.7 Please make hard copies of e-mails which relate to client matters or otherwise need to be retained for record-keeping purposes.

2.8 Ensure that you obtain confirmation of receipt of important messages by requesting faxed, e-mail or telephone confirmation using the return receipt facility.

2.9 Bear in mind that due to delays outside our control, the recipient may not receive the message for several hours, depending on the recipient's IT set-up and other external factors.

2.10 Never import file attachments (even what looks like an innocuous TXT file can be a disguised virus or trojan) or messages from unknown correspondents onto your system without first having them verified by the IT Service Delivery Team.

2.11 Whilst it is accepted that you may need to send personal messages from time to time, you should respect the primary purpose of the e-mail system and keep personal use to a minimum. Use of the email system for personal messages is subject to the company's right to monitor the system for its legitimate business purposes, and by choosing to use the company's e-mail system to send a personal message you consent to the company monitoring such message (including when it is sent using a computer or laptop off-site). When you send a personal e-mail, it must make clear that it is not associated in any way with the company.

2.12 Do not create e-mail congestion by sending trivial messages, forwarding 'chain letters' or unnecessarily copying e-mails. Remember that messages posted to the company's Intranet use much less space on the system than lengthy e-mails sent to large numbers of people. Messages posted to the company's Intranet are 'permanent' (i.e. not subject to automatic deletion) and are accessible by everyone in the company.

2.13 In order to prevent the system being overloaded as a result of the space taken by very large attached files (such as drawings, results files and pictures) being received and subsequently circulated, attachments of this kind must not be circulated within the company. They must be forwarded to the IT Service Delivery Team who will advise on the best method of transportation.

2.14 You are expected to maintain your mailbox regularly, deleting unwanted messages and saving attachments.

2.15 Section 3.7 below sets out four different categories of Internet and e-mail use. You should be aware that use of e-mail which falls into the categories set out in (c) and (d) will result in disciplinary action against you, which could include dismissal.

3 Internet policy

3.1 While the organisation is committed to use of the Internet for business purposes, it must ensure that suitable controls are in place to prevent security breaches or other negative consequences.

3.2 The networks used for the Internet are not secure and any communications sent by this means could be accessed or modified by unauthorised individuals.

3.3 There are also threats from obtaining information from the Internet, virus attachments being the most common. Consequently, we must adopt procedures which minimise the risk of using the Internet and follow good practice in the way individuals behave and the Internet sites that they visit.

3.4 We have established our access to the Internet and/or bulletin boards for specific business purposes - to give access to information and facilities relevant to the company's business and the company's clients and prospects.

3.5 You must not use the IT facilities to access Internet sites or bulletin boards which do not meet this purpose, and in particular any sites of an obscene, abusive, sexist or racist nature. The company reserves the right to monitor the system for its legitimate business purposes, and by choosing to use the company's IT facilities, you consent to the company monitoring all Internet sites you access (including those accessed using a computer or laptop off-site).

3.6 You must not, otherwise than in the normal course of employment, trade or attempt to trade or conduct any sales activities (including the solicitation of such activities) which financially commit or could be construed legally to bind the company or solicit the creation, alteration or performance of any legal or contractual obligation unless the express and specific prior written approval of the Managing Director has been obtained.

3.6 Internet activity (including e-mail) is generally grouped into four categories as follows:

(a) Business use: this includes but is not limited to insurance industry reports, economic information, business news, etc.
(b) Non-business but acceptable use: this includes but is not limited to news, weather, responsible brief personal use such as travel information and limited responsible use of web-based e-mail.
(c) Misuse: this includes but is not limited to excessive time, large downloads, games, chat rooms, discussion groups, movies or film clips, advertising personal goods or services, online trading, sending unsolicited e-mail (the practice known as 'spamming') and the introduction of unauthorised software to the system.
(d) Inappropriate use: this includes but is not limited to pornographic or adult-orientated websites or e-mails, racist, sexist or gambling websites or e-mails, sites promoting violence, and illegal software. Disciplinary action (which could result in your dismissal) will be taken against any employee where usage falls into the categories listed in (c) and (d) above.
3.8 Where material is obtained from the Internet, ensure that any copyright restrictions are obeyed and that virus protection procedures are followed. Where material we own is published, ensure that it carries our copyright indications.

4 Telephone system policy

4.1 You are reminded that the use of the telephone for personal calls is at the company's discretion, and is closely monitored. Use of the phone system for personal calls is subject to the company's right to monitor the system for its legitimate business purposes, and by choosing to use the company's phone system to make a personal call you consent to the company monitoring such call.

4.2 Anyone who makes persistent use of the telephone for personal calls will be asked to provide an explanation.
4.3 The company reserves the right, if appropriate, to claim reimbursement for excessive use of the telephone for personal use.

4.4 If you answer a call and need to take a message you should ensure that the caller's full name, telephone number, date, time and pertinent details are recorded and given to the intended recipient as soon as possible.

4.5 Alternatively you should put the call through to the appropriate extension and the caller can leave a message with recipient's colleague.

4.6 Whenever you leave your desk, or leave the office in the evening, you must ensure that your calls are diverted on to an appropriate alternative.

5 Mobile phones and other mobile devices

If you have been issued with a mobile phone, a personal digital assistant (PDA), a palmtop or other such mobile device by the company, you should observe the following good practice.

5.1 Your mobile device contains confidential information. Use any security measures such as the setting of PIN numbers and passwords as are available on the device. When using your device to access the Internet or WAP services, observe the company's Internet policy at all times.

5.2 Mobile devices are particularly attractive to thieves. Use common sense and in particular:
- do not use the device in the open where you may be vulnerable to having it snatched from you
- keep the device in a deep pocket or zipped portion of a handbag.

5.3 Many services available to mobile device users, including text messaging and information services, premium information provider's phone lines, chat services, downloadable games and ring tones are charged to the mobile phone account. You should not use any such services without the express consent of the IT Service Delivery Team, and the company reserves the right to pass on to you any charges incurred by the company for unauthorised use.

5.4 Use of your mobile phone while driving is forbidden.

6 Monitoring

6.1 The company reserves the right to audit, monitor or record any communications component of the IT facilities and systems:

- for compliance with this IT policy
- to establish the existence of facts
- to ascertain or demonstrate standards which are or ought to be achieved (quality control and training)
- to prevent, investigate or detect crime and disciplinary offences
- to investigate or detect unauthorised or illicit use of the IT system
- to secure, or as an inherent part of, effective system operation
- to determine whether communications are relevant to the business or are personal communications.

6.2 The company may monitor any communications at any time and use any type of monitoring it deems reasonable. You will not always be warned in advance of such monitoring. Whilst consideration shall be given to the privacy of certain information about you which may be identified as a result of such monitoring, you should be aware that in appropriate circumstances the company may have access to such personal and private information without your knowledge and consent.

7 Changes to this policy

The company may alter this IT and security policy from time to time where required to reflect changes to the configuration of its systems and applications and to ensure its continued compliance with statutory and other legal requirements. You will be notified of any material changes to this IT and security policy from time to time.

Group Vice President September 2004

Appendix G

Policy B

SHREWSBURY AND ATCHAM BOROUGH COUNCIL

INFORMATION SECURITY POLICY

The Council is committed to using information technology and computer systems in a secure, efficient and legitimate manner. It fully supports compliance with the Data Protection Acts (1984 & 1998), and other legislation relating to the use of computers.

1. INTRODUCTION

1. Shrewsbury and Atcham Borough Council has experienced a considerable increase in the use of information technology since ICT Services became an independent Service in 2000. Usage of its services is set to continue growing in light of the Government's initiatives for Best Value and Electronic Service Delivery.
2. It is essential that all information processing systems within the authority are protected to an adequate level from disruption and loss of service, whether through accident or deliberate damage.
3. This document has been produced in line with the British Standard for Information Security (BS7799 – part 1) which is acknowledged as the appropriate standard for a security policy.
4. The document outlines the Council's policy in relation to the use of computers and especially the areas of:-

- ❑ Fraud
- ❑ Theft
- ❑ Use of unlicensed software
- ❑ Private work
- ❑ Hacking
- ❑ Sabotage
- ❑ Misuse of personal data
- ❑ Use of the Internet and email
- ❑ Disposal of Equipment

2. PURPOSE OF THE SECURITY POLICY

1. The purpose of the policy is to provide a set of rules, measures and procedures that determine the Council's commitment to ensuring that its I.T. (Information Technology) resources are protected from physical and logical risk.
2. The main objectives of the policy are:-
   - ❑ To ensure that all the Council's assets, Staff, Councillors, data and equipment are adequately protected against any action that could adversely affect the I.T. services required to conduct the Council's business;
   - ❑ To ensure that Staff and Councillors are aware and comply with all relevant legislation and Council policies related to how they conduct their day-to-day duties in relation to IT.

3. APPLICATION OF THE SECURITY POLICY

1. The policy is relevant to all I.T. services, irrespective of the equipment in use, or location, and applies to:
   - ❑ All Councillors, employees and agents;
   - ❑ Employees and agents of other organisations who directly or indirectly support or use the Council's ICT Services;
   - ❑ All use of I.T. services within the Council.

4. MANAGEMENT OF THE I.T. POLICY

1. I.T. security is the responsibility of the Council, Councillors and all members of Staff. The Corporate Management Team approves the policy.
2. The policy has been reviewed by Internal Audit in terms of the policy's scope, content and effectiveness. Audit will periodically review this policy as part of their strategic plan.
3. The Authority will nominate an Information Security Officer who's responsibilities will include implementing, monitoring, documenting and communicating information security in compliance with the security policy and legislation.
4. Managers and Administrators are responsible for ensuring that all staff are aware of their responsibilities under the policy and have access to the contents of this document and it's associated 'User guide' ('Good Practice Guide for Computer Users').
5. All providers of I.T. services must ensure the security, integrity and availability of data within the service provided.
6. The I.T. policy document is intended to be a living document, which will be updated, as and when necessary. Sections and appendices can be added to reflect new or amended procedures and guidelines when determined.

5. VIOLATIONS

1. Violations of this policy may include, but are not limited to, any act that:
   - ❑ Exposes the Council to actual or potential monetary loss through the compromise of IT security;
   - ❑ Involves the disclosure of confidential information or the unauthorised use of corporate data;
   - ❑ Involves the use of data, which causes, for example, the law to be broken.
2. Any individual who suspects that this policy is being violated by another individual must report the violation immediately to his or her Manager, who, in appropriate circumstances, must report the matter to ICT Services.
3. A log of all security incidents will be kept by ICT Services. The log is the responsibility of the Security Officer. The log records any reported incidents and action taken.
4. Any breach of the security policy will be investigated and may result in the individual being subjected to the Council's disciplinary procedure. Councillors breaches will be referred to the Councils Standards Committee.
5. Internet use and access to web sites can be monitored. Any unacceptable use of this service may lead to disciplinary action against the individual concerned.

6. LEGISLATION COMPLIANCE

1. The Council has to comply with all UK legislation affecting I.T. All organisations, employees, Councillors and agents must comply with the following Acts and they may be held personally responsible for any breach of current legislation as listed below.
2. The following are brief descriptions on 'key legislation' affecting IT users. Do not assume that this covers all your legal responsibilities. If you are in any doubt about your legal responsibilities ask the Legal Section for assistance.

Copyright Designs and Patent Act 1998

- ❑ Under this Act, any duplication of licensed software or associated documentation (e.g. manuals) without copyright owner's permission is an infringement under copyright law. All proprietary software manuals are usually supplied under licence agreement, which limits the use of the products to specified machines and will limit copying to the creation of backup copies only. However in some instances, site licenses, permitting the use of software on all machines within a specified site are obtainable.
- ❑ To combat the problems of illegal copying, software suppliers have formed their own organisation to police the use of software throughout the UK. The 'Federation Against Software Theft' (FAST) is able to conduct 'spot' checks on organisations, including local authorities, under a court order and without prior warning.
- ❑ According to the Act, individuals found to be involved in the illegal reproduction of software may be subject to unlimited civil damages and to criminal penalties including fines and imprisonment.
- ❑ http://www.fast.org.uk/
- ❑ http://www.hmso.gov.uk/acts/acts1988/

Computer Misuse Act, 1990

- The Computer Misuse Act, 1990 was introduced to deal with three specific offences that were not adequately covered under existing laws:
- Unauthorised access or attempt to access computer material (such as ‘hacking’). Under this offence it is not necessary to prove the users intent to cause harm;
- Unauthorised access with intent. For example, hacking is carried out with the intention of committing a more serious crime such as fraud. Under this offence, if a plan has been hatched which involves the unathourised use of a computer, the unauthorised use will be sufficient to prove an attempt to commit the crime;
- Unauthorised modification. This part of the act makes it an offence to intentionally cause unauthorised modification such as the introduction of viruses.
- The intention of the act is to enable an organisation to take legal action to protect their data and equipment from unauthorised access and damage.
- http://www.hmso.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm

Data Protection Act 1994 & 1998

- Computers are in use throughout society – collating, storing, processing and distributing information. Much of the information is about people - 'personal data’. This is subject to the Data Protection Acts.
- The Council is only allowed to record and use personal data if, under the Acts, there is a legitimate purpose for doing so and if details of the information, its use and source have been registered with the Data Commissioner. There are strict rules about how the information is used and to whom it is disclosed.
- The Act gives rights to individuals about whom information is recorded on computer and in certain manual files. They may request copies of the information about themselves challenge it if appropriate and claim compensation in certain circumstances.
- If there is any doubt about whether the information can be collected, used or disclosed please address queries to the Council’s designated Data Protection Officer.
- A separate policy document covering the responsibilities under the Act is available via the Council’s Intranet site or from the Data Protection Officer direct.
- http://www.dataprotection.gov.uk/
- http://sabc/services/legal/dataprotection.html

Health and Safety Act (1992)

- The Council shall ensure, through the appointed Health and Safety Officer that all IT equipment is located and used in such a way to not impede health of users or others.
- http://www.hmso.gov.uk/si/si1999/19993242.htm

Defamation

Facts concerning individuals or organisations must be accurate and verifiable. Views or opinions must not portray their subjects in any way, which could damage their reputation.

Race Relations Act (1976) & Sex Discriminations Act (1976)

- Accessing or distributing material, which might cause offence to individuals or damage the Council’s reputation, is forbidden. For example pornographic, racist or sexist material.
- http://www.homeoffice.gov.uk/raceact/

Criminal Justice and Public Order Act 1994, and Obscene Publications Act (1959 & 1964)

- To ensure this law is complied with, any use of Shrewsbury and Atcham Borough Council’s computer equipment for viewing, reading, downloading, uploading, distributing, circulating or selling any material which is pornographic, obscene, racist, sexist, grossly offensive or violent is strictly forbidden. This is irrespective of laws regarding the material in the country of origin.
- http://www.hmso.gov.uk/acts/acts1994/

Human Rights Act 1998 (operative October 2000)

- Under this Act, everyone has a right to respect for their private life, their home and correspondence, which is commensurate with the need to protect the Council from fraud, introduction of viruses or breach of other overriding considerations. To this end, the Council reserves the right to monitor usage of PC’s and telephones.

- ❑ Individuals using the Internet, e-mail or telephone should respect the confidence of the Council and colleague’s information in disclosing it to other people. E-mail, in particular, should not be circulated in a tone, which may give rise to a claim of inhuman or degrading treatments.
- ❑ http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Freedom Of Information Act (2000)

- ❑ Any person making a request for information to a public authority is entitled-

  (a) to be informed in writing by the public authority whether it holds information of the description specified in the request, and

  (b) if that is the case, to have that information communicated to him.
- ❑ http://www.lcd.gov.uk/foi/foiact2000.htm

Electronic Communication Act 2000

- ❑ The main purpose of the Act is to help build confidence in electronic communications. The Act creates a legal framework for electronic commerce, It:
  - clarifies the legal status of electronic signatures.
  - gives the Government powers to modernise outdated legislation so that the option of electronic communication and storage can be offered as an alternative to paper.
  - provides a fallback to self-regulatory scheme that will ensure the quality of electronic signature and other cryptography support services.
- ❑ http://www.hmso.gov.uk/acts/acts2000/20000007.htm
- ❑ http://www.dti.gov.uk/cii/ecommerce/ukecommercestrategy/electronicactguide/

Regulatory Investigatory Powers Act 2000

Interception of communications including computer communications such as email, are unlawful unless in accordance with the RIP Act 2000.

- ❑ The Council may monitor and record communications for the following purposes:-
- ❑ To establish facts and monitor performance of standards.
- ❑ In the interests of national security.
- ❑ To deter crime.
- ❑ To detect unauthorised use of the system.
- ❑ To secure a system.
- ❑ http://www.homeoffice.gov.uk/ripa/ripact.htm

7. ASSETS CLASSIFICATION AND CONTROL

1. The Authority positively identifies and keeps documentary evidence of all computer equipment. It is the responsibility of ICT Services to ensure that these records are accurate and continuously maintained.
2. Each inventory item must clearly identify each asset by an identity tag detailing its unique asset number.
3. All equipment is DNA tagged to identify ownership to Shrewsbury Borough Council. All Council buildings have signage to positively display the operation of DNA equipment tagging.
4. The inventory is maintained using a database, including information relating to location, user, asset tag number, and serial number.
5. On receipt of new equipment it must be labeled and recorded on the inventory. No IT equipment should be purchased without prior consultation with ICT Services.
6. No equipment should be installed on the Council’s network without prior consent of ICT Services who must first record the equipment within the inventory.
7. All disposals of equipment should be recorded against its original entry. The Authority actively pursues a ‘green policy’ on recycling IT equipment.
8. An annual audit of equipment should be carried out by all departments and accounted for to ICT Services.
9. No equipment should be relocated without prior consultation with ICT Services.

8. PERSONNEL SECURITY

Security in Job Definition and Resourcing

1. The authority should ensure that there is adequate definition of responsibilities in Job descriptions for security responsibilities.
2. All potential employees should be screened before commencement of employment.
3. All Staff commencing employment with the Council agree to comply with this policy and it's associated 'Email and Internet Policy' and 'Good Practice Guide'.
4. Personnel procedures ensure that all Staff are made aware of these policies during their 'induction process'.
5. Copies of all the policy and guidance notes are available from via the Council's Intranet site.
6. Each new employee is made aware of his or her obligations for security during the Council's induction-training program. This includes Staff being told of the existence of the Security Policy, the Email and Internet Policy and the 'Good Practice Guide for Computer Users'.
7. Training requirements are reviewed on a regular basis to take account of the needs of the individual, and to ensure that staff are adequately trained in the use of technology.
8. Corporate IT training is the responsibility of Personnel Services.
9. Where training is required for a specific application this may be carried out in consultation with the Users Manager.

9. PHYSICAL SECURITY AND ENVIRONMENTAL SECURITY

Physical Access Controls

1. All Staff are issued with identification badges and these should be worn at all times during working hours. The transfer of badges, keys and other security devices is prohibited. Officers leaving employment with the Council must return all badges, keys and portable computer equipment they have responsibility for.
2. Supervising Officers have a responsibility for ensuring that Staff leaving the Council's employment account for their identify badges, keys and portable computer equipment.
3. An identification badge grants access to non-public areas of the authority. All Visitors to Council premises are issued with visitor passes.
4. No member of Staff should take responsibility for a guest or contractor within non-public areas without ensuring the individual has been issued with a visitor pass. Guests should be supervised throughout the duration of their visit.
5. The Council has security-coded access to all non-public areas. Security codes to these areas are changed at periodic intervals.
6. Access to the ICT Services Suite is clearly defined as a security perimeter. Access is controlled by a different sequence of Security coded doors. Codes are changed at periodic intervals. Only staff who have legitimate business and whose jobs require it should be allowed to enter areas where computer systems are located.
7. No staff or Guests are left unsupervised whilst in this secure area.
8. Staff who have suspicion about the identity of an individual within a non-public area are instructed to politely ask them to determine the purpose of their visit. Employees who are uncomfortable with this responsibility are instructed to report the incident to a Senior Officer immediately.
9. Loss of identity badges or keys must be reported to a Senior Officer as soon as the loss is discovered.

Security of Equipment

1. Where possible Computer equipment is sited away from public areas. Where this is not possible the equipment is always supervised.
2. Computer screens and printed output should not be in view of unauthorised persons.
3. All computer screens that are in public areas should be controlled by time delayed screensavers which require a password to access information.
4. Staff should take responsibility for the physical security of their Computer Equipment within their working environment. Windows and doors should be kept shut whilst unattended.

Environmental Controls

1. The Computer Suite is situated away from Public areas and is unobtrusive.
2. All Stationery and hazardous materials are located outside of the Server suite.
3. The Computer Suite has environmental controls including temperature and humidity, power supply, and fire prevention.
4. The Council's Health and Safety Officer is responsible for periodically checking the condition of equipment.

Equipment Maintenance

1. All equipment is maintained to ensure availability. Critical systems are supported by annual maintenance agreements, which provide for Technical support and call out.
2. IT equipment is maintained by ICT Services. Repairs and servicing should only be carried out by authorised Staff and Contractors.
3. A record of all faults is maintained by ICT Services. Staff who wish to report faults of their equipment are able to do so by reporting the incident to the ICT Services Help Desk on Ext 1077.
4. Staff are issued with a 'call reference number' to provide an audit trail for their call.

Security of Equipment off-premises

1. Before equipment is taken out of Council premises a member of ICT Services should book it out.
2. Equipment used outside of the Authority is only to be used for work purposes.
3. Portable computers are very vulnerable to theft; loss and unathorised access when travelling. Personnel who have portable equipment should aquaint themselves with the instructions included in the 'Good Practice Guide'.
4. The high incidence of car theft makes it inadvisable to leave equipment or media in an unattended vehicle.
5. All portable computer equipment is insured with the Council's Insurance Officer, except when left unattended in a vehicle.

Equipment Disposal

1. All items of equipment containing storage media are only disposed of after reliable precautions have been taken to destroy the media.
2. A record is maintained of all equipment recycled.

10. COMPUTER MANAGEMENT

Operational procedures

1. All regular operational procedures are fully documented and have restricted access to authourised personnel.
2. Backup and system procedures are kept of all fundamental systems, including:-
   - ❑ General Operations of ICT Services.
   - ❑ Day to Day operations and work schedules.
   - ❑ Month-end and Year-end procedures.
   - ❑ Recovery procedures.

Incident Management Procedures

1. All system failures are logged and recorded on the Helpdesk. The Deputy Computer Manager is responsible for investigating, resolving the failure, and implementation of remedies to prevent reoccurrence.
2. All hardware failures are logged and recorded on the Helpdesk. The Deputy Computer Manager is responsible for investigating, resolving the failure, and implementation of remedies to prevent reoccurrence.

Segregation of Duties

1. Segregation of duties are in place wherever practically possible. The objective is to minimise the risk of negligent or deliberate misuse of computer systems.

Capacity Planning

Protection from Malicious Software

1. The Council uses antivirus software as a means of protecting itself from malicious attack.
2. All Servers and workstations are installed with upto date antivirus software. Users files are scanned for viruses each time Users log onto the network or attempt to access files from disk.
3. ICT Services periodically check to ensure that all workstations and Servers are updated with the most uptodate version of antivirus software available.
4. Staff are instructed to report all Virus incidents, including 'hoaxes' immediately to ICT Services.
5. ICT Services notify Staff periodically of any relevant procedures for specific virus prevention.

6. No Staff should load or install software on any Council computer without the prior consent of ICT Services.
7. No diskettes should be loaded onto a Council workstation without them first being swept for viruses. No MP3 players or USB/Memory sticks should be connected to Council computers without prior approval from ICT Services
8. All staff are made aware of good practice for virus control including email and Internet protocol (Email and Internet Policy).

Data Backup/Media Storage

1. Back-up copies are taken of all essential data, software and system files daily. The backup procedures ensure that all critical systems can be recovered in the event of a disaster.
2. Backups are checked daily to ensure that they have completed.
3. Records of all Backups are kept securely.
4. All Backups are clearly labeled and after completion are removed off-site each evening. Tapes are stored in fireproof safes. Documented procedures provide for the rotation of backups between two off-site locations at the end of each week.
5. Backups consist of:-
   - ❑ 4 weekly backup sets.
   - ❑ 12 monthly backup sets.
   - ❑ Year-end.

1. Backup procedures are tested regularly. Records are maintained of all successful restores.

Fault Logging - Help Desk

1. The Helpdesk exists for reporting faults to ICT Services. All Staff are aware of the helpdesk and are encouraged to report incidents to the 'desk'.
2. The ICT Officer (PC Support) is responsible for responding to faults reported.
3. The ICT Services Manager is responsible for ensuring the faults are being responded to in accordance with the Services performance targets.
4. The Helpdesk is also used to report 'network' 'systems' faults and 'development' requests.

11. NETWORK MANAGEMENT

Network Security Controls

1. ICT Services have the responsibility for the security of data on the network and protect connected services from unauthorised access.
2. The ICT Officer (Network) has responsibility for security access to the network.

Enforced Path

1. Users are set up with default network contexts. This prevents undesirable 'straying of users'.

Network Access

1. Network access is controlled by ICT Services.
2. Users and their access to resources are created, modified and deleted as appropriate when requested or notified by an authorising Officer. No access or amendment is made unless appropriate authorisation is received from the Data Owner.
3. Access by third parties (Software maintenance) to the Network is only allowed in the following circumstances:-
   - ❑ The Systems Owner has confirmed in advance with ICT Services that maintenance is due to take place.
   - ❑ The identity of the User has been notified to ICT Services.
4. Network modems are only activated on request. ICT Services are responsible for logging third parties onto network resources. ICT Services record access time and details and monitor usage until maintenance is complete, at which point the modems are switched off and Servers locked. Systems owners are responsible for checking that system maintenance is carried out is accordance with action agreed upon.
5. Data that passes outside Council buildings via radiowave transmitters (WAN) is restricted to broadcast to specific network addresses. The data passing between these Council sites is encrypted.

Media Data Handling Procedures

1. See also Data Backup procedures.
2. No data is removed from ICT Services unless it is signed for or collected by an authorised employee or Courier.
3. All data is packaged accordingly to protect it during transit.

Security of System Documentation

1. All systems should be adequately documented. Documentation is kept upto date and matches the state of the system at all times.
2. Systems documentation is physically secured at all times with access restricted to authorised personnel. An additional copy should be kept (hardcopy or softcopy), which will remain secure in the event of the original copy being destroyed.

Media Disposal

1. All hardcopy media containing sensitive data is disposed of in accordance with the Council's corporate policy for disposal of sensitive data.
2. All magnetic data is destroyed if the equipment is to be disposed of. Where the equipment is to be recycled the magnetic data is reformatted or checked with specific software to clear the data. Where a third party Contractor is used to ‘clear data’ a legal disclaimer is required.

Security of Electronic Mail

1. The protocols for sending and receiving email are addressed in the attached appendix - Email and Internet policy.
2. BS7799 - 1 recommends a specific policy for email. An associated policy has been produced and is an appendix to this policy.
3. Email may be used for personal use provided it falls within the guidance defined as 'acceptable use' within the 'good practice guide'.

12. SYSTEM ACCESS CONTROL

Business requirement for system access

1. Systems and Data Owners should have clearly defined access policies, which determine the access rights for users and groups to their Data and Systems. The policy should take account of:-
   - ❑ The security requirements for specific applications and systems.
   - ❑ The policy for disseminating information.
   - ❑ The need for access to carry out the duties as specified in their job description.
2. All Systems and Data Owners should consider the access they want to allow Users. Computers Services will give Users file rights only after they receive a formal documented request (See User Access Management) from the Systems and Data owner.

User Access Management

1. There is a formal user registration and deregistration procedure for access to networked services.
2. No User is allowed access to the network without a formal 'network access request' or 'job request' being submitted to ICT Services. The request authorised by an appropriate Data Owner or Manager should detail the User and the access rights they wish the User to have. There should be an adequate period of notification to ICT Services for new employees (2 weeks minimum).
3. No alteration to User rights is granted without formal written request from an Authorised Officer.
4. System access rights are withdrawn by ICT Services as soon as an individual leaves the Council's employment, changes jobs, or is classed as 'long term sick'. Details of the accuracy of this information reside with the Personnel Section who formally notify ICT Services. Managers and Supervisors are responsible for notifying Personnel.
5. A network account is maintained by ICT Services of each User. The account details the Users access rights and privileges. These are periodically monitored for acceptability by ICT Services.

User Password Management

1. No individual should be given access to a live system unless properly trained. All new Users should be provided adequate training in the systems they will require access to. System Owners are responsible for ensuring that users have the adequate training before requesting User access to the ‘live’ system.
2. All new Users should be made aware of their security responsibilities as defined in their job description.
3. Users should keep their passwords secret and never disclose them to colleagues. It is s breach of this policy for Users to share passwords or sign in other Users and can lead to disciplinary action.
4. All Users should change their passwords periodically. ICT Services include password aging by default when accounts are set up.
5. Where systems permit ICT Services set password length to a minimum of 6 digits for all new accounts.
6. All passwords are conveyed verbally to new Users by ICT Services. Users are immediately prompted to change their password.
7. Passwords are not displayed when entering them.
8. Users who forget their passwords are instructed to contact ICT Services.
9. ICT Services verify the validity of the request before issuing a new password. The identity of the individual is always checked before issuing a revised password.
10. ICT Services maintain a record of previous User passwords. This prevents Users reusing a previous password.
11. High security and system administration passwords are only issued to IT Staff. These passwords are changed regularly.

User Responsibilities

1. Users are issued with guidance on good password management within the ‘Good Practice for Computer Users’. The guidance advocates the following:-
   - ❑ Keep passwords confidential;
   - ❑ Avoid keeping a paper record of passwords;
   - ❑ Change passwords wherever there is any potential compromise in security;
   - ❑ Select passwords with a minimum of six digits;
   - ❑ Avoid basing passwords on potentially guessable formats;
   - ❑ Change passwords regularly
2. Users are instructed not to leave equipment logged on and unattended. Users should ensure that they are logged off systems and sessions.
3. Where Users are in Public areas they are instructed to use Screen Saver passwords. These passwords together with BIOS passwords need to be made available to ICT Services for administration.

Network Access Controls

1. See Network Management

Login Procedure

1. Users accessing the network must comply with the Security Policy. Prior to logging on Users may be prompted with a display notice warning users that 'the computer must only be used by authorised personnel'.
2. Users accounts are disabled after three attempts. Users must notify ICT Services to regain access. A User will be asked to identify themselves before their account is reactivated.
3. Login times are restricted to Office working hours for Staff, unless otherwise requested and authorised.
4. All Users should be prompted for a Username and password. No user should access the system without using their own User ID.

Application Access Control

1. System Owners (See 12.2 - Business requirement for system access) define access and use of application systems.
2. Systems Owners control access to applications and are responsible for ensuring that they support the objective of this security policy.

3. System Owners should strictly control access to System Utilities within applications. Only authorised users should have access to these utilities. Managers are responsible for ensuring that there is adequate ‘internal checks’ carried out on the procedures exercised by these users
4. All unnecessary system utilities are disabled during installation.
5. All application systems should provide adequate audit trails of transactions.

13. SYSTEMS DEVELOPMENT AND MAINTENANCE

New Projects

1. No formal feasibility studies should be carried out without initial consultation with ICT Services.
2. All formal projects should be submitted to the IT Steering Group for consideration.
3. New systems should follow a formal feasibility study of the options prior to selection.
4. All projects for new systems should consider the security requirements of the system to safeguard the confidentiality, integrity and availability of the information assets. This should be considered during the feasibility stage of the project. Consideration should include:-
   - ❑ Control of access to information;
   - ❑ Segregation of duties;
   - ❑ Access to audit trail;
   - ❑ Verification of critical data;
   - ❑ Compliance with legislative requirements;
   - ❑ Backup procedures;
   - ❑ Recovery procedures;
   - ❑ Ease of use
   - ❑ Data Protection

Change Control Procedures

1. Any change to systems, files and data, should be undertaken in a controlled manner. All changes should be documented and tested prior to implementation.
2. There should be a separate 'test' environment set up for new programs. All new programs should be acceptance tested and signed off by the User before going 'live'.

14. BUSINESS CONTINUITY PLANNING

Risks and Planning

1. ICT Services has identified and maintains a record of business critical systems and processes.
2. ICT Services periodically review their Operational risks and their impact on the Authority.
3. ICT Services have identified responsibilities and procedures to follow in the event of disasters for specific Servers and Systems. Documentation of these procedures and processes are kept on file in ICT Services.
4. ICT Services intend to develop a comprehensive Business Recovery plan which includes all IT business processes and recovery action.
5. Staff responsibilities will be determined and conveyed in the Business Recovery Plan.
6. All Staff responsible for Recovery procedures will be trained accordingly.

Procedures are tested and reviewed regularly

Appendix H

Policy C

INFORMATION SECURITY POLICY STATEMENT

The purpose of the information security policy is to protect the HEFCW, its staff and public from all information security threats, whether internal or external, deliberate or accidental.
The information security policy is characterized here as the preservation of:
a) Confidentiality: ensuring that information is accessible only to those authorised to have access.
b) Integrity: safeguarding the accuracy and completeness of information and processing methods.
c) Availability: ensuring that authorised users have access to information and associated assets when required.
d) Regulatory: ensuring that HEFCW meets its regulatory and legislative requirements.
HEFCW has set up an Information Security Team to introduce and maintain policy and to provide advice and guidance in its implementation.
HEFCW requires that all breaches of information security, actual or suspected, will be reported to and investigated by the information security officer (Frances Good ext 2244)
HEFCW undertakes to provide appropriate information security training for all staff.
Third parties are required to ensure that the confidentiality, integrity, availability, and regulatory requirements of all business systems are met.
HEFCW will produce, maintain and test Business Continuity Plans.
It is the responsibility of all users of the network to adhere to the policy.
Members of the Management Team are responsible for ensuring the policy is implemented and adhered to by their staff, third parties and suppliers.
I expect and require all staff to adhere to the policy. Failure to do so may result in the use of disciplinary procedures as appropriate.

Authorised by
Chief Executive

INFORMATION SECURITY POLICY SUMMARY

Introduction

The policy relates to the security of HEFCW's information. Although a high proportion of the measures are concerned with the management of electronic information and associated systems, the policy also covers paper records, personnel matters and issues relating to buildings. The policy itself is detailed and technical in some areas. This summary is intended to enable all staff to gain some understanding of the security policy. However, this summary can only provide an overview. Reference should be made to the full policy to establish exact requirements. The structure of the summary reflects that of the policy document to facilitate cross-referencing. The numbering reflects the ISO 27001 control objectives and controls.

5. Security Policy

This section deals with how staff will be made aware of the policy and how the policy will be reviewed and updated:

- Dissemination of the policy will be through the publication on the intranet together with summaries targeted at specific audiences and by providing training
- Reviews will be undertaken annually and, if necessary, updating will follow organisational changes or the identification of new risks

6. Organisation of Security

The areas covered under organisation of security are the security infrastructure including roles and responsibilities; confidentiality, independent review; and security in respect of external parties:

- The Management Board together with the Information Security Officer will ensure that the policy is implemented. All managers are responsible for ensuring their staff comply and all employees are personally responsible for information security in their own areas.
- Formal authorisation is required for new information systems
- Third party contracts must include clauses relating to information security.

7. Asset Management

This section sets out arrangements for keeping an inventory of assets (hardware, software, systems) and the use of information classification of both electronic and paper records:

- Up to date registers of assets must be kept and all systems should have a named owner who will ensure compliance with the information security policy
- The use of information assets must be in accordance with the Acceptable Use Policy
- Information must be labelled and managed in line with its security classification as set out in the Protective Markings Scheme.
- Sensitive information must be locked up and destroyed by shredding when no longer required.

8. Human Resources Security

Issues covered relate to the security aspects of HR matters including terms and conditions of employment; training; disciplinary proceedings; and procedures for termination or change in employment:

- Job descriptions must include security roles and responsibilities as appropriate; confidentiality agreements must be signed; and declaration of interest forms must be completed as necessary.
- Training will be provided and policies and procedures made available through the Intranet.
- Normal disciplinary procedures apply to violations of the security policy.

9. Physical and Environmental Security

This section relates to the provision of secure areas; the security of equipment; and general controls to improve information security:

- There must be physical entry controls to the building
- Sign in and use of security cards must be enforced for staff and visitors
- Areas within buildings, where sensitive information (eg HR) or equipment (eg servers) are held must be lockable.
- ICT equipment must be installed and maintained by qualified staff according to manufacturers' instructions and be protected from power failure and other damage.
- Equipment will be disposed of in line with the agreed disposal policy.
- Unauthorised access to information is reduced by an enforced clear-screen policy.
- Sensitive documents must be locked away when unattended.
- Equipment is not to be taken off-site without formal approval.

10. Communications and Operations Management

The areas covered in this section are: operating procedures and responsibilities; third party arrangements; systems planning and acceptance; protection against malicious and mobile code; backup; network security management; media handling; exchange of information; and monitoring:

• Change management standards and arrangements for separation of development and operations must be implemented.
• The risks associated with third party contracts must be assessed and contracts should address security issues and should be monitored.
•Demands on systems and storage capacity are to be monitored, acceptance criteria agreed and systems tested before acceptance.
• Systems must be protected against viruses and other malicious software.
• Information must be backed up regularly.
• Information on redundant disks or other media must be destroyed before disposal and steps taken to protect information when a machine is taken off-site for repair.
• Network monitoring must be undertaken regularly and logs kept securely.
• System documentation must be protected from unauthorised access and copies stored securely off-site.
• Formal agreements for information exchange should be established.
• Any sensitive information sent electronically must be protected.

11. Logical Access Controls

This section sets out the rules which limit access to information and systems to that required to discharge business responsibilities covering: user access management; user responsibilities; network access control; operating systems access control; application and information access control; mobile computing and home-working:
• User access is controlled by user identifiers and passwords and the varying level of access rights depending on need as set out in the Access Control Policy.
• Good practice in the use of passwords is mandatory and automatic log outs of PCs are enforced
• Users must only have access to services they have been authorised to use. Appropriate controls on access to the network must be in place and authentication and secure paths must be used for remote access. Shared networks must have appropriate routing controls.
• Secure log-on procedures with user identification and authentication must be used. Access to systems utility programs is restricted. Inactive systems connections will be timed out.
• Use of systems will be monitored and audit logs maintained and reviewed regularly.
• Policies for mobile and home computing will include requirements for security controls.
• Laptop guidelines and mobile phone policy must be adhered to.

12. Development and Maintenance

This section covers security requirements of information systems, correct processing in applications; cryptographic controls; security of system files; and security in development and support processes:
• Data validation and correction procedures must be used
• Encryption of sensitive or confidential information should only be used when authorised by the ICT Team.
• Only approved software and packages will be used.
• Strict controls will be maintained over access to program source libraries
• Change control procedures must be used and application systems testing is to be undertaken following changes
• The information security policy applies equally to any outsourced developments.

13. Information Security Incident Management

• Security incidents and/or weaknesses must be reported to the Information Security Officer (either directly or through line manager) and escalated as appropriate.
• The Information Security Team will record, agree corrective action and monitor incidents
• Advice must be sought immediately from the Information Security Officer following an incident likely to lead to legal action before any further action is taken.

14. Business Continuity Management

This section covers plans for Business Continuity
• All aspects of business continuity are managed by the Business Continuity Group
• The Business Continuity Plan is managed within the Shadow Planner system
• Testing of the plans will be undertaken at least once a year
• All staff are required to undergo training in the use of the system.

15. Compliance

The final section covers compliance with legal requirements, compliance with the security policies and standards and technical compliance; and systems audit considerations:
• The main legal requirements relate to the Data Protection Act (1998); Copyright Patents and Design Act (1988); and the Computer Misuse Act (1990).
• Managers and asset owners will ensure adherence to security procedures in their areas of responsibility.
• Security audits will be carried out periodically.

Appendix I

Policy D

1. Introduction

The information that OCIU holds represents an extremely important and valuable asset. It is essential that this information is suitably protected from a wide range of threats in order to preserve confidentiality and to ensure continuity of service.

OCIU seeks to protect its information by establishing and maintaining an Information Security Management System (ISMS) in accordance with the British Standard BS7799.

Compliance with this standard is required for connection to the OCIU Net.

The standard requires that an Information Security Policy is defined as part of the ISMS. This should aim to address the following key principles of information security:

- **confidentiality** - ensuring that only authorised persons have access to the information
- **integrity** - ensuring that the information is correct and complete
- **availability** - ensuring that authorised persons have access to the information when required. Overall responsibility for information security shall rest with the OCIU Director. All staff shall be made aware of the policy. It is everyone's responsibility to ensure that security is implemented and maintained effectively.

The policy shall be reviewed annually. A review shall also take place in response to significant security incidents, new vulnerabilities or changes to the organisational or technical infrastructure.

This policy is complimentary to other OCIU policies and should be used in conjunction them.

2.Details of the security policy

2.1. Compliance with legislative and contractual requirements

OCIU has legal obligations to maintain security and confidentiality notably under the following legislation:

• Data Protection Act (1998)
• Copyright, Designs and Patents Act (1988)
• Access to Health Records Act (1990)
•Computer Misuse Act (1990)
•EC Directive on Legal Protection of Databases (1996)
•Human Rights Act (1998)
•Electronics Communications Act (2000)
•Freedom of Information Act (2000)
•Health and Social Care Act (2001).
OCIU shall also comply with other guidelines and standards:
•OCIU Security Standards
• Caldicott Report (1997)
• IARC Guidelines on Confidentiality in the Cancer Registry (IARC Internal Report No: 92/003 March 1992)
• Core Contract for Purchasing Cancer Registration (EL(96)7 February 1996).

2.2. Asset classification and control

2.2.1. Register of assets

An up to date register of assets shall be maintained by the IT Manager and reviewed annually. This shall include:

1. information assets: databases and data files, archived information
2. software assets: system software, application software
3. physical assets: computer equipment, magnetic media, other technical equipment.

2.2.2. Classification of information

Information shall be classified to indicate the need, priorities and degree of protection required.

2.3. Working in a secure environment

2.3.1. Secure areas

OCIU shall be based in a locked area, with access using a secure key fob.

2.3.2. Fire doors

Fire doors shall be kept shut at all times. They will unlock automatically when the alarm sounds.

2.3.3. Badges

Identification badges shall be issued to all staff and shall be worn at all times. Temporary staff shall be issued with a badge for the duration of their employment.

2.3.4. Visitors

Visitors shall sign a Visitors Book and wear a visitor badge. All visitors shall be supervised while on the premises.

2.3.5. Leaving the building

Staff shall ensure that on leaving, all windows are closed, blinds drawn and doors closed. The last person out of the building shall ensure all PC's are turned off, doors and cabinets are locked and the lights are switched off.

2.3.6. General tidiness

Desks shall be left tidy and all confidential paperwork and computer media locked away.

2.4. Equipment security

2.4.1. Equipment siting and protection

Equipment shall be installed and sited in accordance with the manufacturer’s specification.

Computer servers shall be sited in a separate locked area with air conditioning. Food and drink shall not be allowed into this area.

Computer servers shall be protected against power fluctuations.

Personal computers shall be physically secured to desks to protect them against theft.

2.4.2. Cabling security

All cabling shall be in conduits or within the framework of the building to protect against interception or damage.

2.4.3. Equipment maintenance

All computer servers shall be covered by third party maintenance agreements.

2.4.4. Remote diagnostic services

Suppliers of systems/software shall be permitted remote access to such systems on request to investigate/fix faults. Generally this will only apply to OCIUnet connected systems and suppliers shall be expected to use the Third Party Secure Gateway for which appropriate approval has been granted.

Dial-in access to systems not connected to the OCIUnet shall be permitted in exceptional circumstances, provided that:

- a strong authentication process is used for connections
- the dial-in connection is physically broken when the fault is fixed/supplier ends the session.

2.4.5. Security of hard disks

Hard disks on any machine may contain sensitive and confidential data. Removal off site of such disks for repair represents a potential threat. Each such case shall be judged on its merits balancing the need versus the risk of breach of confidentiality and then only to approved repairers who will have signed confidentiality agreements.

2.4.6. Security of equipment off-premises

Equipment and data shall not be taken off site without formal signed approval from the OCIU Director.

Portable computers present a high risk to network security as they are very vulnerable to theft, loss or unauthorised access. No such computer shall be permitted to have access to any OCIU network.

2.4.7. Disposal of equipment

Computer hardware shall be disposed in a secure manner. Data storage devices shall be purged of sensitive data before disposal or securely destroyed. All disposals shall be documented.

Computer media shall be given to the IT Team for disposal when no longer required (e.g. floppy disks, tape cartridges, CD-ROMS).

2.4.8. Non-OCIU IT Equipment

IT equipment not owned by OCIU (including PCs, laptops and PDAs) shall not be allowed to connect locally to any OCIU network or system nor shall such equipment be used for the storage or processing of patient identifiable or other OCIU sensitive data. Exceptions will only be allowed with the prior authorisation of the IT Manager and the OCIU Director.

2.5. Access control

2.5.1. Security of third party access

No external agency (OCIU or not) shall be given access to any OCIU information system unless that body has been formally authorised to have access. All external agencies shall be required to sign security and confidentiality agreements with OCIU.

2.5.2. User access control

No individual shall be given access to any information system unless properly trained and made aware of their security responsibilities.

A secure log-on process involving the following passwords shall control user access to information systems.

1. A power-on password: to start machines. The same password shall be used on all machines and shall be changed periodically or when any staff member leaves.
2. A network or operating system log-on password: to access information systems. This password shall be known only to the user. All systems shall include password ageing to force users to change their password periodically.
3. An application password: to access certain applications.
4. A screen-saver password: to clear a screen-saver display.

2.5.3. User password management

Staff shall choose sensible passwords i.e. that have a minimum of seven characters, and that are not easily guessed by others. Staff shall keep passwords secret and never disclose them to anyone.

Staff with authorised access to more than one system may have the same password on all systems to which they have access. This may give different access privileges on different systems depending on job need.

2.5.4. E-mail and Internet access

Staff shall use the OCIU Net for e-mail and Internet access. No computer connected to the OCIU Net shall be allowed to simultaneously connect to any OCIU internal network.

2.6. Network security

2.6.1. Operating procedures

Detailed operating procedures shall be documented and maintained.

2.6.2. Software

Only licensed copies of approved commercial software shall be installed. It is a criminal offence to make or use unauthorised copies of commercial software and offenders are liable to disciplinary action.

The installation of private software, shareware, or any non-standard application e.g. screensavers, games, utilities, etc. onto any computer owned by OCIU shall not be allowed. Exceptions will only be allowed with the prior authorisation of the IT Manager.

2.6.3. Firewall

An approved firewall shall be implemented to protect the OCIU network from OCIUnet and vice versa.

2.6.4. Virus protection

All workstations and servers shall be protected with anti-virus software. On-access scanning shall be implemented on all workstations. Updates shall be applied at least every 30 days or sooner if available from the vendor.

The mail server shall scan e-mail and file attachments on receipt. Certain file types known to be associated with transmitting e-mail viruses shall be blocked and quarantined.

Staff shall report to the IT Team any viruses detected or suspected on their computers immediately.

All newly acquired disks from whatever source shall be scanned for viruses. IT support staff shall provide assistance with this if required.

2.6.5. Patch management

Security updates in the form of patches, service packs, hotfixes etc shall be applied to relevant software at the earliest opportunity. The OCIUIA website shall be monitored regularly for notification of such updates and other security alerts.

2.6.6. Housekeeping

Staff shall save their work on central computer servers. No identifiable data shall be stored on personal computers or on the external network.

All computer servers shall have daily backup regimes. Such backups shall have a minimum of a 5-day cycle before media is overwritten. Secure storage shall be used for 4 of the 5 backups with only the next one to be used being on site. Such storage shall be geographically separate from the system location to protect against building loss.

2.6.7. Network addressing

To safeguard the network from unauthorised connections, static IP addresses shall be used. Dynamic Host Configuration Protocol (DHCP) shall not be implemented.

2.6.8. Upgrades to systems

The development and introduction of new information systems, software, IT projects and IT support activities shall be conducted in a secure and structured manner.

2.7. Data quality assurance

2.7.1. Data input

All systems shall include validation processes at data input to check in full or in part the acceptability of the data. Depending on the system, later validation may be necessary to maintain referential integrity.

Any loss or corruption of data shall be reported immediately to the OCIU Director or to the appropriate line manager.

2.7.2. Monitoring and review

Monitoring and review of data quality shall be undertaken on a monthly basis.

2.8. Security incident management

2.8.1. Security incidents

A security incident is an event that may result in:

- degraded system integrity
- loss of system availability
- disclosure of confidential information
- disruption of activity
- financial loss
- legal action
- unauthorised access to applications

Any security incidents that may have an impact on the OCIU Net shall be reported immediately to the Regional Telecommunications Branch Security Co-ordinator or OCIU Net Security Manager.

2.8.2. Logging security incidents

All security incidents shall be formally logged, categorised by severity and action/resolution recorded. The OCIU IT Manager shall maintain this.

2.9. Security education requirements

All staff shall receive appropriate training and regular updates in organisational policies and procedures.

2.10. Business continuity management

2.10.1. Need for effective plans

OCIU recognises that some form of disaster may occur, despite precautions, and therefore seeks to contain the impact of such an event on its core activities through tested disaster recovery plans.

OCIU recognises that its IM&T systems are increasingly critical to its activities and that the protracted loss of key systems/user areas could be highly damaging in operational terms.

Business continuity plans shall be established and maintained by the OCIU IT Manager and the OCIU Manager.

2.10.2. Planning process

The main elements of this process shall include:

- identification of critical computer systems
- identification and prioritisation of key users/user areas
- agreement with users to identify disaster scenarios and what levels of disaster recovery are required
- identification of areas of greatest vulnerability based on risk assessment
- mitigation of risks by developing resilience
- developing, documenting and testing disaster recovery plans identifying tasks, agreeing responsibilities and defining priorities

2.10.3. Planning framework

Disaster recovery plans shall cater for different levels of incident including:

- loss of key user area within a building
- loss of a key building
- loss of key part of computer network
- loss of processing power

Disaster recovery plans shall always include:

- emergency procedures covering immediate actions to be taken in response to an incident (e.g. alerting disaster recovery personnel)
- fallback procedures describing the actions to be taken to provide contingency devices defined in the disaster recovery plan
- resumption procedures describing the actions to be taken to return to full normal service

3. Security management responsibilities

3.1. Overall responsibilities

Overall responsibility for IT security shall be delegated to OCIU by its host employer, Milton Keynes PCT.

All staff shall be given an annual update on IT security.

3.2. Management responsibilities

Managers shall ensure that:

1. staff are instructed in their security responsibilities.
2. staff using computer systems/media are trained in their use.
3. only authorised staff are allowed access to the unit's information.
4. current documentation is always maintained for all critical job functions to ensure continuity in the event of individual unavailability.
5. staff are aware of the organisation’s Standing Orders on potential personal conflicts of interest.
6. staff sign confidentiality agreements as part of their contract of employment.
7. the relevant systems administrators are advised immediately about staff changes affecting computer access (e.g., job function changes/leaving department or organisation) so that passwords may be withdrawn/deleted.

3.3. Staff responsibilities

1. Staff shall ensure that no breaches of security result from their actions.
2. Staff shall declare any potential conflicts of interest as required by the organisation’s Standing Orders.

3.4. Specific responsibilities

Area of responsibility	Manager
Release of identifiable data	Director/Head of information
Register of assets	IT Manager
Premises security	OCIU Manager
Equipment security	IT Manager
Disposal of equipment	IT Manager
Access control	IT Manager
Network security	IT Manager
Data quality assurance	Head of Information
Security incident management	IT Manager/OCIU Manager
Security education	IT Manager/OCIU Manager
Business continuity	IT Manager/OCIU Manager