EMPLOYEES' INFORMATION SECURITY AWARENESS AND BEHAVIOURAL INTENTIONS IN HIGHER EDUCATION INSTITUTIONS IN OMAN

Mohammed Al-Mahri

A thesis submitted in partial fulfilment of the requirements of the University of Northumbria at Newcastle for the degree of Doctor of Philosophy

Research undertaken in the

Faculty of Engineering and Environment

2018

DECLARATION

I declare that no outputs submitted for this degree have been submitted for a research degree of any other institution. I also confirm that this work fully acknowledges opinions, ideas and contributions from the work of others. Any ethical clearance for the research presented in this commentary has been approved. Approval has been sought and granted by the Faculty Ethics Committee.

Name: Mohammed Al-Mahri

Signature:

ACKNOWLEDGEMENTS

First, I would like to give praise and thanks for the God, the Almighty, the greatest of all, on whom ultimately we depend for sustenance and guidance. I would like to thank Almighty the God for giving me opportunity, determination and strength to do my thesis.

I would like to express my deep appreciation to my supervisors Dr. Paul Vickers and Professor. Lynne Coventry for their support and recommendations, which improved this thesis. They have been a source of continual inspiration throughout my research and without their guidance; comments and encouragement, much of this work would not have been possible.

Finally, my deep and sincere gratitude to my family for their continuous and unparalleled love, help and support.

Abstract

Organisations throughout the world face threats to the security of their information. In most organisations these threats are thought to be a consequence of employees' lack of knowledge of information security, security behaviours and/or understanding of the possible detriments to their organisation of not complying with their organisation's information security policy (ISP). Therefore, empirical research is needed to explore the main threats to information security and the factors that influence how employees intend to behave in relation to information security policies.

The main aims of this research were to investigate employees' ISP compliance behaviour intentions and to explore the organisational and human factors that influence this. Consequently, this research conducted four studies to explore the views of both those responsible for information security (IT staff and system administrators) and non-security employees from a range of higher education institutions in the Sultanate of Oman.

First, interviews were conducted with eight IT staff and system administrators from Omani universities and colleges to explore the common, current information security threats, organisational information security processes and their perceptions of employee information security behaviour in general, and their compliance with ISPs in particular. The findings of this study showed the weaknesses in information security in different organisations and IT staff suggested that employees may not be aware of information security and do not comply with their organisation's ISP. The reported perceptions of IT and staff system administrators were used to design a survey of employee knowledge, awareness and behaviour intentions which was used in the second study.

The second study used a questionnaire-based survey which was designed from the knowledge gained form the first study, a review of the relevant literature and actual ISPs in use at the organisations involved in the study. Data from 503 employees from multiple higher education institutions was analysed. The survey comprised three parts: (i) demographic questions, (ii) 14 information security scenario

questions designed to elicit employee behaviour intentions and (iii) some of the factors influencing their behaviour (underpinned by current theories in psychology). The results show that employees' behaviour intentions vary according to the information security scenario they experience and that the biggest influences on their behaviour are perceived to be trust and authority.

The third study involved 17 IT staff and system administrators from six higher education institutions. Using the same questionnaire from the second study plus qualitative questions, the aim of this third study was to understand what behaviours were seen by IT staff and system administrators as most important and what non-ISP-compliant behaviours they would, nevertheless, also deem to be acceptable. The results highlight the relationship between the behaviours that IT staff rate as important, and whether or not staff intend to adopt that behaviour.

The fourth study used four focus groups (n= 21) from one higher education institution to further explore why employees may not intend to comply with the organisation's ISP and to explore the factors that influence these non-compliance intentions. The focus groups also explored the employees' recommendations for improving organisational information security management. The finding of this study revealed some recommendations for developing information security organisation management and the motivators and barriers that influence employees' security behaviours.

Finally, the results of the four studies were analysed together and it was found that staff consider that communicating the information security policy, ongoing information security risk assessment, ongoing awareness and training, management support and commitment and good communication are important factors in information security compliance intentions. Secondly, it was found that the way organisations manage information security, and human factors in particular (mostly to do with trust and authority), is most important in maximising compliance intentions. Recommendations were provided to improve organisational information security management and to encourage employees to comply with ISPs.

CONTENTS

List of Figures

List of Tables

List of Acronyms

ANOVA: Analysis of Variance

ENG: Engineering Group

ICT: Information Communications Technology

ISP: Information Security Policy

ISS: Information System Security

ITA: Information Technology Authority

ITG: Information Technology Group

KAB: Knowledge, Attitude and Behaviour

PMT: Protection Motivation Theory

SPSS: Statistical Package for the Social Sciences

TPB: Theory of Planned Behaviour

VPN: Virtual Private Network

Chapter 1: INTRODUCTION

1.1 Problem Statement

A major barrier to security is employees' behaviour, particularly non-compliance with their organisation's information security policy (ISP). Many researchers have attempted to explore the factors that influence such non-compliance (Guo et al., 2011; Ifinedo, 2012; Pahnila et al., 2007; Safa et al., 2015; Vance et al., 2012). Failing to comply with the Information Security Policy can leave an organisation's information exposed to theft or modification, however staff may be unaware of these consequences. Nevertheless, these nonintentional internal threats pose a great risk to information. These may arise from a lack of awareness amongst employees, a lack of support from information security management, poor communication and the misuse of data by employees through ignorance (Safa et al., 2016a). However, the enforcement of strict security controls and measures at universities and other higher education establishments is more problematic and complex than other organisations (Drevin et al., 2007; Rezmierski et al., 2002).

In this research IT staff and system administrators' views from multiple higher education institutions are gathered to explore the current information security threats to higher education organisations, management support for security and their perceptions of employees' behaviour with regards to security and compliance with ISPs. This information then helps in the construction of robust instruments (such as questionnaires) to identify employees' information security awareness in general, employees' ISP compliance intentions and important factors that influence employees' compliance behaviour.

The literature on information security suggests that there are few very good tools to objectively measure the behaviours within multiple organisations and understand their ISP compliance behaviour across a range of behaviours that are commonly specified in an ISP. These behaviours include physical security, backup, password management, incident reports, phishing, virus threats, incident report and technical security with privileges. Given this difficulty, psychological theories of behaviour which use behaviour intention as a precursor to behaviour are explored alongside the factors that affect those intentions. In order to statistically explore behaviour

intentions, a large number of participants from different higher education organisations were recruited.

Measuring employees' information security awareness levels and compliance intentions was supplemented with the views of the people responsible for organisations' information security. This permitted consideration of what they consider to be acceptable employee behaviour. This allowed comparisons between employee attitudes and beliefs around acceptable behaviour and those of the security staff.

From this knowledge, recommendations to improve information security in higher education institutions can be proposed.

1.2 Research Question

The aim of this thesis is to explore employees' compliance intention towards information security policies in Omani higher education institutions and to identify the factors which employees believe influence their security compliance intentions. To achieve this, the following research questions were explored through this thesis:

(a) What are the recent information security challenges and threats facing higher education institutions in Oman?
(b) What are the information security awareness levels and ISP compliance intentions of employees within higher education institutions in Oman?
(c) How can we reliably measure actual user information security awareness and compliance intentions?
(d) What factors affect users' intentions (both positively and negatively) toward information security policies within higher education institutions?
(e) What relative importance do IT staff give different behaviours within the ISP and do they permit behaviours which are not written in the policy?

In order to answer the above research questions, a mixed methods approach using both qualitative and quantitative techniques was employed.

1.3 Research Methodology

This study uses a combination of qualitative interviews and focus groups alongside a quantitative questionnaire (see Figure 1.1) to explore employees' information security awareness and ISP compliance intentions. Ethical approval for each study was granted by Northumbria University before starting each round of data collection (see Appendix A).

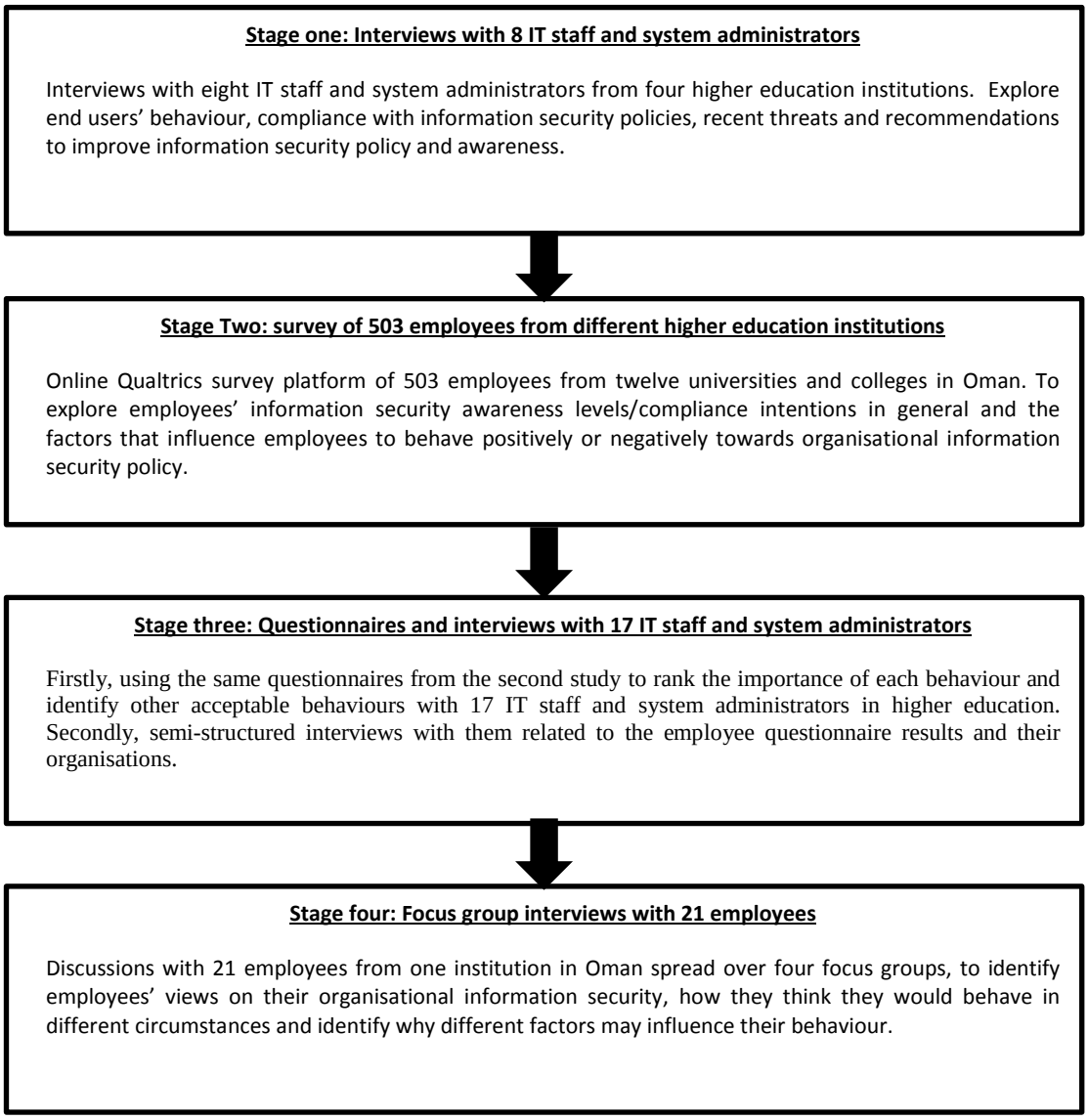


Figure 1.1: Thesis research methodology structure

1.3.1 IT staff and system administrators' interviews

The first exploration used a semi-structured qualitative interview method with IT staff and system administrators in four higher education institutions in Oman. The collected data was transcribed to explore the IT staffs' perceptions of end users'

behaviour, employee compliance with information security policies, recent threats and recommendations to improve information security policy and awareness. Thematic analysis (which assists in exploring and gathering themes and sub-themes) was used to analyse the data.

1.3.2 Employee survey across different higher education institutions

The second study used a scenario questionnaire which was disseminated to several universities and colleges in Oman to explore employees' information security compliance intentions in general and the factors that affect this as well as the impact of non-compliance. In addition, this survey helped identify the specific behaviours within the ISP where more employees had intention to comply and not be influenced by other factors.

The questionnaire utilised indirect scenario questions designed to explore employees' behaviour intentions towards security and possible adherence to their organisation's information security policies. These questions were based on a review of the literature, the universities and colleges' ISPs, psychological theories and results from the first study. 14 scenario questions were developed to explore employees' information security awareness levels in general and information security influence factors in particular and how those factors relate to their organisation's information security policy. Each question had the correct policy-compliant answer and three plausible but non-compliant answers (identified by others as legitimate reasons to not comply with the policy, e.g., at the request of the line manager). The survey also explored eight influencing factors for each scenario: knowledge, response efficacy, subjective norms for organisation and/or manager, compliance, behavioural intentions, and sanctions and rewards. These were identified from psychological theories of behaviour to understand participants' behaviour and to make predictions as to what influences their ISP compliance intentions. Some of these factors were drawn from Protection Motivation Theory (Rogers (1983) and Theory of Planned Behaviour (Ajzen (1991); this allows the exploration of factors that may affect how employees behave towards information security.

1.3.3 IT staff and system administrators' prioritisation study

The previous study identified that intention to comply was not universal across all 14 behaviours, and it was necessary to consider what IT staff considered to be the most important behaviours. It may also be possible that IT staff accepted some behaviours that are not compliant with the ISP. To answer these questions, this third study again took an exploratory, qualitative approach.

First, the IT staff were asked to rank the 14 employee scenario behaviours in order of importance to security in their organisation. They were then asked to explain how they ranked the top and bottom five behaviours. Next, they were asked to provide all answers that they would find acceptable for each of the 14 scenarios to explore what non-policy-compliant behaviours they would also view as acceptable in their organisations. This helped to evaluate IT staff and system administrators' information security awareness and knowledge as well as identifying behaviours they would allow even if not explicitly stated in the ISP. In addition, it helped to evaluate the employees' questionnaire answers in terms of shadow security (Kirlappos et al., 2014), i.e., local behaviours that had become acceptable without updating the ISP.

1.3.4 Employee focus groups

The final stage conducted focus group discussions with 21 employees split into four groups from one institution in Oman to explore their security behaviour intentions in more depth.

The questions were grouped into two parts: scenario questions based on six different scenarios to encourage discussions exploring employees' information security awareness and identifying the underlying reasons for their compliance or non-compliance intentions towards the ISP in different security areas such as sharing passwords, social engineering, physical security, backing up data, incident reports and disabling antivirus protection. The second group of questions focused on the availability of information security policies, employee understanding of the security policy and compliance intentions, the factors that influence whether employees comply with security policies and the employees' recommendations for writing security policies and improving compliance.

1.4 Contribution

The aim of this research was to identify the compliance intentions of staff in Omani universities and colleges towards information security behaviours and to explore the organisational and human factors that influence these intentions in order to mitigate the risks of information security breaches and enhance the security of the information and systems. As such this thesis makes the following contributions:

- A recognition that compliance with security policy is not a single behaviour, and intentions to comply with the individual behaviours within the policy vary. This suggests that research which treats compliance as a single behaviour is flawed. The results of this thesis suggest that employees had awareness and higher compliance intentions for some behaviours, while not others.
- A methodological contribution has been made in the creation and use of indirect scenarios used in questionnaires and the plausible answers derived through qualitative interviews and underpinning psychological theories. The use of indirect scenarios was more likely to discover what participants themselves would do when they are in those situations.
- Understanding the compliance intentions of a large number of employees in multiple higher education institutions in the Sultanate of Oman. The large sample size and involvement of a number of institutions led to results that are more transferrable than previous research. This identified areas of behaviour which should be addressed.
- The findings from the second study (employees' survey) and fourth study (focus groups interviews) show that trust, authority and knowledge are the most important factors in influencing employees to comply with an organisational ISP.

1.5 Research Structure

This thesis comprises eight chapters, the first being this introduction. The remaining chapters are as follows.

Chapter 2: Literature review.

This chapter reviews the literature around information security policy compliance. It highlights and explains several information security areas in management, security policies, psychological theories of behaviour, measurement methods, information security awareness and information security in higher education institutions.

Chapter 3: Semi-structured interviews with IT staff and system administrators.

This chapter describes the semi-structured interviews with eight IT staff and system administrators. The findings are organised into four main themes:

1. Information security processes in the organisation;
2. Types of online information security threats;
3. Perceptions of employees' ISP compliance behaviour; and
4. Recommendations to improve compliance.

The results of this chapter were used to design the employee questionnaires for Chapter 4.

Chapter 4: A large scale employee survey.

This chapter details how the online questionnaire method was used to capture data from 503 employees in multiple higher education institutions in Oman. Moreover, this chapter presents and discusses the participants' background, behaviour intentions and factors that influence ISP compliance.

Chapter 5: IT staff and system administrators' prioritisation of security behaviours.

This chapter presents a study of 17 IT staff and system administrators designed to discover their views on the scenarios used with staff to identify acceptable employee behaviours which are not in the ISP and the relative importance of the different behaviours within the scenarios. The results of this chapter are cross referenced back to the results of the employee survey findings in Chapter 4.

Chapter 6: Qualitative follow on study of employee intentions.

This chapter follows up the study in Chapter 4 to explore in more detail why employees behave the way they reported and the influencing factors that enhance

and/or are barriers to complying with the ISP. The results of this chapter are cross referenced back to the results of the employee survey findings in Chapter 4.

Chapter 7: Discussion.

This chapter synthesises the results of the four studies and discusses findings which may help to improve information security organisational management and motivate employee compliance with the ISP. Furthermore, this chapter provides recommendations for an organisation to implement proper information security.

Chapter 8: Conclusion.

The final chapter concludes the thesis by summarising the main results and discussing the contributions of the research. In addition, this chapter presents the limitations of the research and suggestions for further work.

Chapter 2: LITERATURE REVIEW

2.1 Introduction

Organisations must be constantly vigilant for threats (both internal and external) that put the confidentiality, integrity and availability (in other words, security) of their systems and information at risk. There are serious consequences for an organisation when its information is compromised, which can lead to a loss of trust, money and/or time. In addition, these information security breaches can affect the organisation's reputation significantly (Ahmad et al., 2012; Safa & Ismail, 2013).

Peltier (2005b) defines information security as that which "directs and supports the company and affiliated organisations in the protection of their information assets from intentional or unintentional disclosure, modification, destruction, or denial through the implementation of appropriate information security and business resumption planning policies, procedures, and guidelines" (p.13).

It is impossible to achieve perfect information security even with the implementation of the best available technology. It can be seen from the number of breaches reported in 2017 that there is still a long way to go. For example, in the 2017 UK Cyber Security Breaches Survey, Klahr et al. (2017) reported that 46% of all businesses identified at least one cyber security breach or attack in the previous 12 months and a third of those that experienced a breach reported that senior management saw cybersecurity as low priority. Interestingly, those organisations who say they have a formal information security policy are more likely to have experienced a breach. However, this might just be that those with policies are more aware of breaches within their organisation. Policies are less likely to cover employees' use of mobile, personal, and cloud-based devices and storage of information. While comparative data is not available from Oman, Ramalingam et al. (2016) report that 71% of their respondents from higher education institutions in a survey on security awareness reported experiencing a security problem. Further, the Information Technology Authority (ITA, 2017) reported that in 2016 they stopped 279 million attacks on Omani Government websites. Janes (2012) argues that although many organisations assume that technology alone can solve the

problems of losing their information, because of attackers, insiders or business partners, this is not true.

Janes (2012) advises that to successfully minimise the impact of information loss, the leadership team should effectively combine people skills (awareness and training programmes) processes (proper policies and procedures) and technology (monitor and prevent data leaving a business). These components are shown in Figure 2.1. Those organisations adopting a combination of technical, policy, and behaviour approaches to protect their assets are considered to be more effective (D'Arcy & Hovav, 2007; Li et al., 2010; Vance et al., 2012). However, it is not sufficient to simply have a policy in place, it must be ensured that staff adopt the behaviours outlined in the policy. There is a clear need to understand what motivates employees to adopt such behaviours.

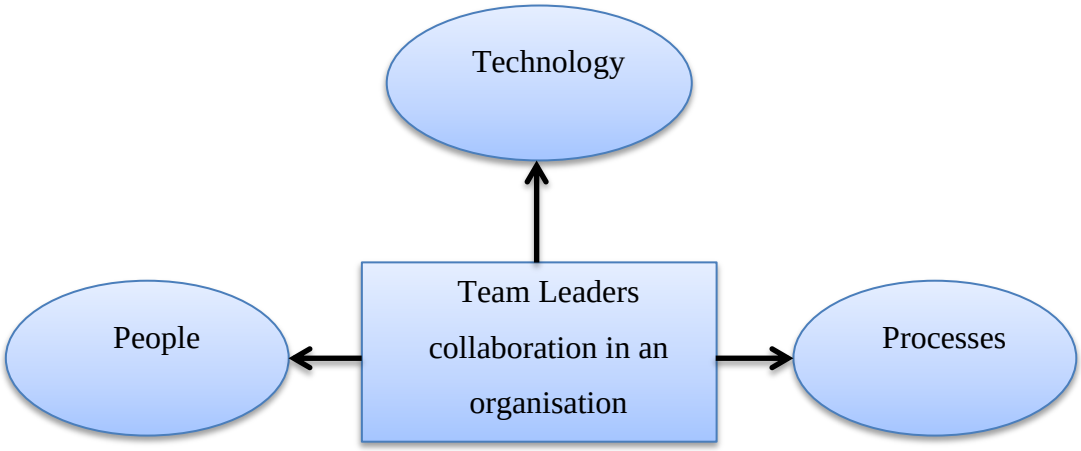


Figure 2.1: Successful information security at organisation

Whitman and Mattord (2012) define an information system as "much more than computer hardware; it is the entire set of software, hardware, data, people, procedures, and networks that make possible the use of information resources in the organisation" (p.16). Information security can be maintained in a number of ways, in particular those aimed at introducing better technological solutions and those aimed at managing and/or changing human behaviour. A technical aspect includes antivirus software, firewalls, cryptography, proxy servers, access control and intrusion detection software. Human aspects include users' knowledge, attitudes, behaviours, and awareness. Technology relies on human behaviour to deliver its benefits.

This chapter focuses on the literature which explores people and their security behaviour intentions within the workplace, particularly how they relate to information security policies. Where possible articles that explore behaviour within a University context are included. It explores theories of behaviour and how behaviour is influenced.

2.2 The Information Security Policy

Employees are the foremost members in any organisation and the most important group of people who can assist in minimising IT vulnerabilities and unintentional errors (Wilson & Hash, 2003).

The increasing level of cyber threats, which have an effect on an organisation's information systems, has compelled companies to establish security programmes. An ISP is the foundation of such organisational security programmes (Knapp et al., 2009). Without ISPs, governance has no substance and no rules to enforce.

Within organisations, the ISP is an internal document that outlines the organisation's expectations, sets rules and outlines behaviours that the organisation wishes to promote in order to protect its information and systems (Bulgurcu et al., 2010). A good policy will outline the roles, responsibilities, reporting processes and penalties that exist within the organisation (Teodor et al., 2014). When an organisation attempts to shape an ISP it must consider the basic rules. For instance, the policy should not conflict with law, should be properly supported and administered, and should be permissible in court.

Bosworth and Kabay (2002); Peltier (2004) outline how to create high-quality policies. These combine to form the following guidelines:

- Use all suitable policy resources from government, industry bodies and commercial organisations in preparation for creating policies
- Policies should be easy for users to understand and use unambiguous language and short sentences.
- The written policies should be applicable so that they meet the needs of the specific organisation.

- When an organisation and its workers practice policies they should meet the organisation objectives and not put the organisation at risk.
- An organisation should make policies which are enforceable.
- Prior to policies being published by an organisation they should allow the employees to comment on drafts.
- Expectations of employees' behaviours towards the policies should be made clear.
- Employees should know they will experience disciplinary sanctions up to and including dismissal when they do not comply with an organisation's policies.
- Give reasons for polices.
- Provide several ways of reading the policies, including printed text, electronic text, and hypertext.
- Review and improve or adapt polices regularly.
- Announce major changes.

The concept of documenting the ISP in an organisation is to clarify the need for information security and furthermore, it provides an explanation to all of the organisation's information resource users. In contrast, Baker et al. (2007) argue for the need to take appropriate action and that organisations need to be aware of the information security risks. In addition, they mentioned that there are many ISP options available, although a number of organisations are not sure about the most suitable method to protect their data from threats. As Karlsson et al. (2017) argue, the availability of an ISP does not necessarily guarantee information security.

Alarifi et al. (2012) suggest that ISPs must be written with due care, as they are one of the most important documents in an organisation and policies should complement the business objectives of the organisation and align with management to operate the organisation in a controlled and secure manner. Unfortunately, organisations often write security policies without considering the goals and the abilities of the employees that must follow them (Beautement et al., 2016). Policies are not easy to write and assistance from outside the organisation may be required. Furthermore, the organisation must be aware that the policies must be suitable for

an organisation's culture. Al-Awadi (2009) summarised different studies and recommended that an ISP must:

- **"Fit the organisational culture:** the security policy of an organisation mostly depends on the common organisational culture. Organisations differ in their security requirements. What is suitable to one organisation may not be suitable to another.
- Have a style which is consistent with the organisation's general communication style: a common format makes the policy easier for employees to understand the purpose of it.
- **Be effective and dynamic:** organisational 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;
- **Use simple 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 organisation:** the policy has to state the reasons for the policy and what the organisation'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" (p.29-30).

Hellqvist (2014) found that the most crucial problems raised by many studies regarding a lack of ISPs in organisations are as follows: there is no clear understanding within the organisation of why it needs an ISP; no clear understanding of the purpose of the ISP; no clear understanding of the resources needed to develop and implement an ISP; no holistic view during the development of the ISP; no consideration or adaptation of the unique environment of an

organisation; and there is no suitable standard to guide the ISP development process and/or it is not clearly established in the organisation.

2.2.1 Policy Infrastructure

An ISP should be in place before technical and non-technical solutions are implemented. For instance, with regards to technical mechanisms, a firewall cannot be installed unless system administrators establish a clear ISP. Furthermore, information security training and awareness cannot commence without agreeing and documenting an in-depth ISP. From organisation to organisation, policies may differ considerably, but they still are important to practice to secure the company's assets. Some organisations use a ready-made ISP established by international information security companies, while other businesses construct their own ISP according to organisational needs.

The aim of the ISP is to ensure that sensitive information within an organisation is protected from destruction, unauthorized access, modification and disclosure, wherever it is stored or handled. Therefore, it is important to classify information to identify the level of sensitivity with regards to the information to ensure proper protection mechanisms and moreover, to identify who is responsible for doing so (e.g., employees, owners, or customers). Employees should distinguish between the internal use of information, for instance, human resources information (personnel data, financial or history) and public information when the organisation is connected to the internet, such as the organisation's web site. For example, Carnegie Mellon University classified institutional data into three levels of sensitivity as shown in Figure 2.2 (Raderman & Markiewicz, 2015).

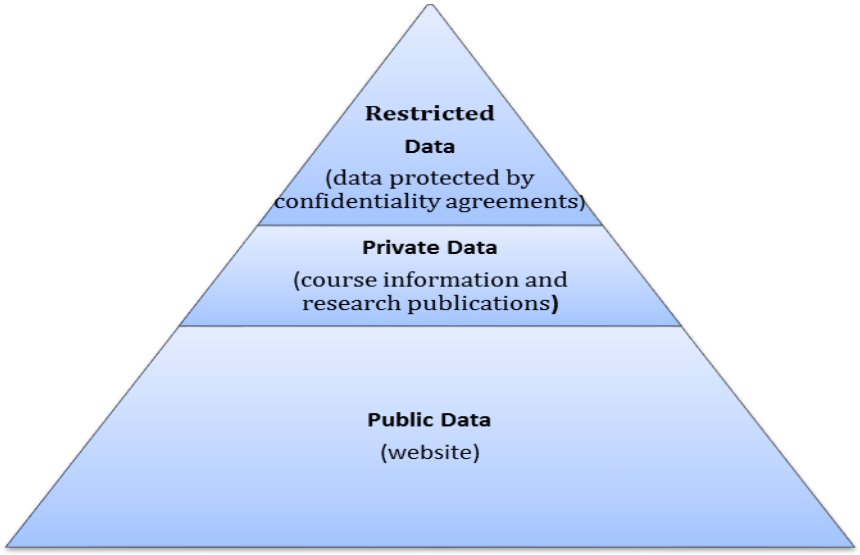


Figure 2.2: Data Classification

Open information such as the university website, which has general information about the university products, international university services and so on, has access enabled for everyone who belongs to the university and for those outside the university. However, no one can change the data except authorised users who can edit data that would present little or no risk to the organisation and its affiliates. Private data can be shared between authorised university employees using the internal network who have rights to read, modify, remove and print electronic files such as course information and research publications. There is a moderate level of risk to the organisation if there was unauthorized access to this data. Finally, data should be classified as Restricted when assets become a significant control issue and pose a significant risk to the organisation if there was unauthorized disclosure, alteration or destruction of that data. This includes confidential information determined by government regulations and data protected by confidentiality agreements.

2.2.2 Policy Implementation

When the ISP of an organisation is documented, in place and available for all staff, those staff need the competence to implement these policies properly. The organisation has the responsibility to train staff in the implementation of information security policies. David (2002) declares that security is based on policy and to make policy effective, it must be enforced.

Procedures explain how staff should implement an organisation's policies. For instance, the policy might state that all data should be encrypted when employees send it outside of the organisation or that staff should use virtual private network (VPN) software to encrypt data. A VPN allows employees to connect securely to internal company resources from a public network via remote access.

Research suggests that the policy alone may not be sufficient. For instance a policy may state that an employee should select a strong password; however, if this is not enforced in some way, then it may not happen (Biddle et al., 2012; Florêncio & Herley, 2010). Consequently, organisations should not rely only on the policy, but should also pay more attention to methods that persuade users to comply (Mwagwabi et al., 2014).

2.2.3 Information security: organisational roles & responsibilities

All companies have employees that work at different levels of responsibility. At the bottom, a company relies on its functions to provide the services or products, whilst at the top team leaders set the strategy and direction for the company as a whole. All organisations have the responsibility of assuring confidentiality, integrity and the availability of sensitive information. Therefore, to prevent employee error the organisation should ensure that all staff are responsible for information security and understand their responsibilities.

Any organisation should know whether their employees understand their roles and responsibilities in the security of the organisation and protecting its information assets. Waly et al. (2012) argue that roles and responsibilities are vital influences that should be the main priority of each employee from senior management to individual staff members.

2.2.4 Information Security Policy Summary

In summary the ISP sets out how employees are expected to behave within an organisation. However, people do not always behave as expected. The following sections explore the literature surrounding the factors that influence behaviour, particularly security behaviour.

2.3 Understanding human information security behaviour

Human information security behaviour is a complex area to study and technology is not the complete solution to information security problems (Kearney & Kruger, 2016). Bulgurcu et al. (2010) point out that an organisation can achieve information security when it considers both technical and socio-organisational factors. In recent years, most studies have paid more attention to the technical aspects of security rather than on security management to investigate the problems created by security breaches (Waly et al., 2012). To reduce the risk of information security incidents in an organisation, human aspects of information security should be considered alongside technological and organisational aspects (Hina & Dominic, 2017; Safa, Von Solms, & Futcher, 2016).

The most frequent reason for information security violations is user behaviour. Karlsson et al. (2017) argue that around half of all security breaches were accidently caused by insiders while other research has estimated about 80% of the risk to information systems comes from insiders (D'Arcy, 2009; Walton, 2006). Others argue that many information security programmes do not spend enough time and effort understanding human behaviour, the costs of human failing and the protection required against it (Liginlal et al., 2009; Parsons et al., 2014; Schultz, 2005; Spruit, 1998).

Most businesses give their employees privileges to access, modify and/or transfer data between computers in the same network or a different network, although of course there is no guarantee of avoiding mistakes that could cause loss to the organisation in terms of time, money and trust. Furthermore, due to lack of information security policies, employees may cause problems to organisational assets by installing software from the internet that has malicious features hidden within it (Kissel, 2009).

ISPs outline the protective behaviours expected from employees. There is a lack of consensus on the recommended behaviours in the workplace. However, there are many different behaviours to consider as outlined in different studies. These include user authentication, the use of security software, keeping all software up to date, being alert to phishing attacks, being alert to actions that reduce privacy and

to maintaining secure internet use. Unfortunately, most IT managers pay more attention to technical problems and solutions (for example proxy servers, intrusion detection systems, firewalls and routers), and pay little or no attention to their end users (Katz, 2005). Research into ISP compliance has also concentrated on security technology and this is insufficient if behavioural and social aspects are ignored (Han et al., 2017). Technical solutions can fail due to human error (Rhee et al., 2009). Therefore, human aspects should be considered as a critical issue (Safa et al., 2015; Safa, Von Solms, & Furnell, 2016; Scholl et al., 2018).

"The security of systems is dependent on the people that use them" points out (Lohrmann, 2014) but unfortunately, people may be the weak link in an organisation (Lebek et al., 2013; Tatu et al., 2018) and their misuse of information system components is a significant threat to organisations (D'Arcy, 2009; Madigan et al., 2004). When employees do not comply with organisational policy, they not only threaten the loss of important information, but it can also lead to the organisation losing money and time working on fixing the problems that they caused.

Before attempting to understand employees' behaviour, it is necessary to explore how security behaviour has been investigated. Quantitative survey explorations tend to explore what factors influence employee intentions to comply with the ISP. However, such research is problematic. First, it fails to recognise that there are many different behaviours listed within such policies, each of which may be influenced by different factors. Posey (2010) lists 67 protective workplace behaviours. Giving a single score for compliance is problematic if some behaviours are followed while others are not. Secondly, this approach assumes that employees have an ISP, and have knowledge of its contents. Third, it assumes that policies are consistent across organisations. These issues may be the reason for inconsistent findings from ISP compliance research (Sommestad et al., 2014).

Given the importance of employee behaviour, the next sections will explore theories of behaviour and the factors that influence behaviour.

2.3.1 Theories of human behaviour used in information security

Beautement et al. (2009) argue that numerous organisations have attempted to influence or change employee security behaviour, but discovered it to be a major challenge. Employee behaviour is affected by social, cultural, individual, and psychological factors (Spender, 1998). These factors are expressed within different theories of behaviour.

It is important for security researchers to be aware of theories of behaviour and behaviour change from psychology. It is important to note that security researchers have not applied these theories consistently; some researchers use only components, rather than the whole theory, while others may use a combination of theories. There are many different theories of behaviour, with many different components, only some of which have been investigated within the domain of security (Coventry et al., 2014). There is no universally correct theory: each theory simply focusses on different aspects. This section reviews the most commonly applied theories in information security awareness and behaviour.

Lebek et al. (2013) and Safa et al. (2015) identified Theory of Planned Behaviour (TPB) and Protection Motivation Theory (PMT) as the most frequently used theories in the literature of information security awareness and behaviour. Both theories incorporate intention to be a precursor to actual behaviour. However, some information security researchers argued that behavioural intention doesn't always lead to actual behaviour (Crossler et al., 2013; Mahmood et al., 2010). The intention–behaviour gap is well established in the behaviour change research but more research is required in security to understand how positive intentions can be translated into actual behaviour.

2.3.1.1 Theory of planned behaviour (TPB)

Ajzen (1991) says that TPB has been the most frequently used and the most productive theory in explaining human behaviours. TPB contains three factors: attitude, subjective norms and perceived behavioural control, as demonstrated in Figure 2.3, which, by their influence on intention, lead to a change in behaviour.

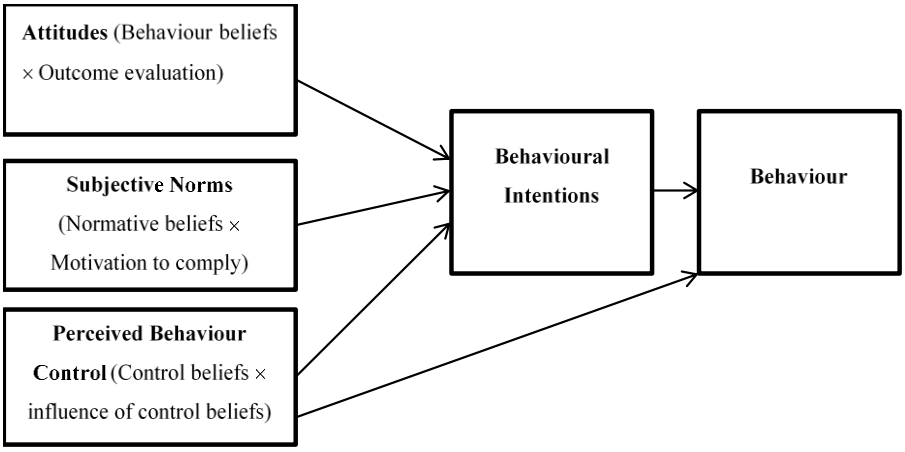


Figure 2.3: The theory of planned behaviour (Ajzen, 1991)

The TPB has been shown to be a good predictor of ISP compliance (Bulgurcu et al., 2010; Dinev & Hu, 2007; Flores & Ekstedt, 2016; Sommestad et al., 2015).

2.3.1.2 Protection Motivation Theory (PMT)

Rogers (1983) developed Protection Motivation Theory and originally applied it to health psychology to understand how "fear appeals" affect an individual's behaviour. This theory says that when people are confronted with a threat, they engage in two types of appraisal: threat appraisal and coping appraisal.

Vance et al. (2012) clarified that threat appraisal contains three factors (see Figure 2.4):

1. Rewards or benefits (any intrinsic or extrinsic motivation for increasing or keeping an unwanted behaviour);
2. Perceived severity (the magnitude of the threat);
3. Vulnerability (the extent to which the individual is perceived to be susceptible to the threat).

Coping appraisal also contains three factors:

1. Response efficacy (the belief in the perceived benefits of the coping action by removing the threat);
2. Self-efficacy (the degree that he or she believes it is possible to implement the protective behaviour) and

3. Response cost (to the individual in implementing the protective behaviour).

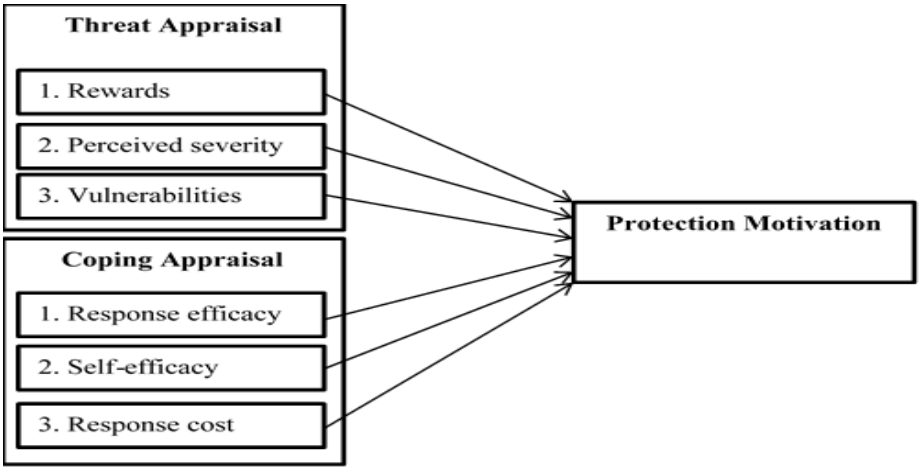


Figure 2.4: Protection Motivation Theory (PMT)

A number of studies in information security behaviour have applied PMT and noted that it is a useful theory to predict a person's intention to engage in protective actions, or protection motivation (Anderson & Agarwal, 2010; Crossler, 2010; Hansen et al., 2018; Ifinedo, 2012; Jansen, 2015; Meso et al., 2013; Tsai et al., 2016).

2.3.1.3 Knowledge, Attitude and Behaviour (KAB) model

Another model that is commonly used in security literature is the Knowledge, Attitude and Behaviour (KAB) model. The model "proposes that behaviour changes gradually. As knowledge accumulates, changes in attitude are initiated. Over some period of time, changes in attitude accumulate, resulting in behavioural change" (Baranowski et al., 2003, p. 28s). For instance, when employees in an organisation know the importance (including the benefits) of complying with the ISP and the possible consequences to them and their organisation of non-compliance then their attitude might change, leading to compliant behaviour (see Figure 2.5). In the KAB model, when researchers want to measure people's knowledge they ask what people know. For attitude they ask what people think about situations. For behaviour they ask what people actually do.

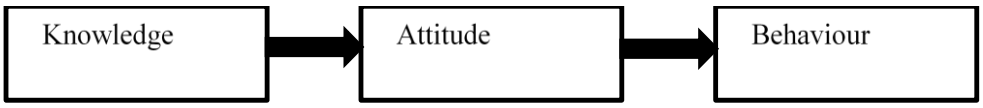


Figure 2.5: Knowledge attitude behaviour model

Several studies on information security awareness such as those by Kaur and Mustafa (2013); Khan et al. (2011); Kruger and Kearney (2006); McCormac et al. (2017) are based on the KAB model to measure the user's information security awareness level. Furthermore, Parsons et al. (2014) applied the KAB model to examine the relationships between knowledge of policy and procedures, attitude towards policy, and behaviour when using computers at work and they found there is a significant relationship between knowledge, attitude and behaviour. Unfortunately, Khan et al. (2011) and Rimal (2001) argue that the KAB model is not always sufficient to change behaviour. Indeed, different research fields such as environmental awareness (Khan et al., 2011), information security awareness (Baranowski et al., 2003), and healthcare show that the KAB model and the theory of planned behaviour (TPB) should be combined to understand the process of behaviour change because knowledge is necessary but not sufficient to change behaviour.

2.3.2 Applying theories of behaviour to information security policy compliance

Many previous studies applied theoretical frameworks to understand employee behaviour intention in relation to information security in general and compliance with organisational ISPs in particular. Thomson and Solms (1998) have shown that insights from social psychology could be used to enhance the effectiveness of an information security awareness programme. Ifinedo (2012) integrated PMT and TPB to understand IS security policy compliance; he found that factors such as attitude toward compliance, perceived vulnerability, self-efficacy, response efficacy, and subjective norms have significant effects on individuals' intentions to comply with organisations' ISPs.

Information security is a fundamental concept for organisations today (Thomson et al., 2006). Research studies have been carried out to identify factors that influence employees' compliance with information security policies and to investigate how

important these factors are. The purpose of the behavioural assessment of security governance is to ensure that employees are practising and implementing the organisation's rules and policies. Vance et al. (2012) note that a number of psychology theories have been used to explain employees' failure to comply with ISPs. Teodor et al. (2014) argue that users' compliance with ISPs will enhance an organisation's information security levels. However, previous studies and field surveys suggest that employees seldom comply with information security procedures (Goo et al., 2013).

Many studies applied psychological theories to understanding employees' behavioural compliance with organisational ISPs. Several attempted to explain why employees do or do not comply with their organisation's ISP by using different psychological theories (Bulgurcu et al., 2010; Ifinedo, 2014; Pahnila et al., 2007). Mishra and Dhillon (2006) argue that criminology and social psychology theories have been frequently utilized to understand and predict employees' security behaviour and awareness.

A number of investigations applied a single theory, whilst others combined two or more theory elements to explain factors affecting employees' compliance with security policies. Siponen et al. (2014) developed a new model by combining elements of the theory of reasoned action, protection motivation theory and cognitive evaluation theory to identify factors affecting employees' compliance with security policies.

2.3.3 Key influencing factors

Many investigations have used different models to recognize and identify effective factors in information security (Waly et al., 2012). There are many factors to measure when considering employees' compliance with ISPs that are incorporated into these different theories.

2.3.3.1 Information security awareness/knowledge

Alarifi et al. (2012), Hasan and Hussin (2010), Khalfan (2004), Rezgui and Marks (2008) and Waly et al. (2012) all argue that lack of information security awareness is one reason why employees behave negatively toward information security.

Organisations must recognise that increasing information security awareness is a key first step in protecting their physical and data assets.

Information security awareness campaigns are designed to attract the attention of users, in order to raise their knowledge and concerns, in relation to information security (Tsohou et al., 2008). Moreover, an ISP should assume that information security awareness is the first priority in development (Ahlan & Lubis, 2011). In addition, the main purpose of security awareness is to ensure that users understand their personal roles and responsibilities towards security (Peltier, 2005a). To reduce the risk of information security breaches an organisation should consider information security awareness to be a very important issue and different training methods are recommended (Safa, 2017).

The development of information security such as the guidelines, procedures, standards and policies is only the beginning of an effective information security awareness programme. Information security awareness encourages users to pay more attention to mitigate human error and comply with an organisation's ISPs and regulations.

Wilson and Hash (2003) declared that awareness is not training and attention to information security is the main aim of awareness and changing users' behaviour. Khan et al. (2011) identified that information security awareness in an organisation is ensuring that all employees are aware of the regulations and rules regarding protection of the organisation's information.

Previous studies have attempted to use different technological and functional awareness and training programmes to improve employees' information security skills, behaviour and knowledge (Albrechtsen & Hovden, 2010; Eminağaoğlu et al., 2009; Khan et al., 2011). This is because lack of knowledge and skills may cause companies to face information security threats (Lacey & James, 2010).

Bosworth and Kabay (2002) state that an organisation should include information security in their policies and focus attention on security by delivering an information security programme that is visible and credible for their employees in order to show that security is paramount and that it is a collective responsibility.

All the employees in an establishment should be involved in an awareness programme, which should begin with new employees and continue throughout the organisation. The organisation should set aside a period for their employees to participate in awareness activities and the employees should sign a statement acknowledging that they understand how to deal with the organisation's material and comply with its ISP and procedures. In addition, the organisation should designate a person or group to manage the programme. The most effective way to enhance users' information security behaviours in their workplace is by raising awareness.

Kaur and Mustafa (2013) examined the effectiveness of knowledge, attitude and behaviour on information security awareness and they found that attitude and behaviour have a significant influence on the availability, confidentiality, and integrity of business information. Furthermore, they argued that lack of information security awareness could cause critical threats to organisational assets and security.

Kruger & Kearney (2006) developed a prototype model to measure information security awareness in an Australian gold mining company by practising three measurements: what employees know (knowledge), what they think (attitude) and what they do (behaviour). The study measured six focus areas, namely actions-consequence awareness, adherence to company policies, careful use of mobile equipment, careful use of the internet and mail, reporting security incidents, and secrecy of passwords along with an awareness of general information security and the ISP. The results showed that the overall score for regional users' information security awareness level was 65%, which related to 77% awareness in terms of knowledge, 76% awareness in terms of attitude and 54% in terms of behaviour. In addition, regarding ISP compliance, users scored 44% overall based on 81% for knowledge, 55% for attitude and 18% for behaviour. They conclude that there are many reasons why organisations have to pay more attention to and spend resources on measuring awareness, which could be useful in security campaigns and return on investments. They established that the information security awareness of employees has a significant influence on the confidentiality, integrity and availability of information, while knowledge showed no significant relationship to

information security awareness. The primary reasons for users' mistakes were a lack of information concerning security awareness, apathy, indifference, carelessness, and misbehaviour, in addition to resistance and ignorance (Safa, Von Solms, & Furnell, 2016). In addition, numerous information security incidents happen because of the unintentional behaviour of and negligence of employees, bringing about a genuine internal danger to the safety of organisational assets (Durgin, 2007; Hina & Dominic, 2016).

2.3.3.2 Management

In any organisation, there are different user positions, responsibilities, and roles requiring different access privileges. The key issue for organisational information security is good management which plays a very important role in enforcing employee compliance with an ISP (Choi, 2016; Lee et al., 2016; Puhakainen & Siponen, 2010). Knapp, Marshall, Kelly Rainer, et al. (2006) identified that top management support is a critical indicator of an organisation's security culture and level of ISP enforcement.

Truss et al. (2006) suggest that one of the most important factors influencing employee engagement is thinking that their manager is committed to the organisation. Furthermore, security studies argue that the role of management practices with security policies is very important for running a successful information security programme (Maynard & Ruighaver, 2006; Siponen et al., 2014). In addition, managers should check employees' information security quality and skills (Safa & Von Solms, 2016).

Straub and Welke (1998) argued that top managers, middle managers and employees continue to ignore information security and that neglect leads to more security breaches in an organisation. Therefore, more studies are needed to explore the role of management in information security and how managers could play a very important role in information security (Soomro et al., 2016).

Top management, immediate managers and IT administrators have the authorisation to interfere and change the information security in most organisations.

The effectiveness of management on employee policy compliance policy needs to be identified.

2.3.3.3 Organisational and national culture

Bates (1990) defined culture as "the system of shared beliefs, values, customs, behaviours, and artefacts that members of a society use to cope with their world and with one another, and that are transmitted from generation to generation through learning" (p.7). Organisational culture is a different concept but is related insofar as it pertains to the shared beliefs, values, customs and behaviours that are present in an organisation. Both national culture and organisational culture will have effects on employees' security behaviour. Several studies have explored employees' information security awareness across different nationalities and organisational cultures. Over time in work environments, trust between employees in the same organisation is built up and helps to get work done and this is a key aspect of organisational culture. But sometimes organisational culture (including factors such as trust between employees) can negatively affect them to not comply with their organisation's ISP such as sharing passwords (Al-Mukahal & Alshare, 2015). For example, an information security survey conducted by Boulder (2010) found that 40% of 2,500 users from Australia, UK and USA shared their password with one or more person in the previous one year. On the other hand, Tang and Zhang (2016) pointed out the positive role that organisational culture can play in encouraging staff to adhere with the ISP by gathering, protecting, scattering and overseeing data to enhance information security.

Walsham (2002) described national culture as shared symbols, norms, and values in a social collective such as a country. National cultures and their relationship to information security may contribute either positively or negatively to employees' information security behaviour. Many studies compared employees' information security awareness and behaviour by different organisational culture fields and nationalities and these studies are described below.

2.3.3.3.1 Organisational culture in different fields

Khalfan (2004) selected several public and private sector organisations in Kuwait to identify the information security considerations in information systems/

information technology and noted security criticalities, loss of control, vendor dependency, cost escalation, and poor service quality. Talib et al. (2010) found that information security knowledge and practice gained from a work environment could be transferred to the home environment.

In a recent study by Waly et al. (2012) questionnaires were disseminated to three sectors (health, business and education). The questionnaires were used to (i) assess the employees' level of information security awareness, and (ii) to evaluate the employees' understanding of the ISPs. They also attempted to tease out (i) what factors influence user behaviour toward information security, and (ii) the impact of the training and awareness programmes on changing the information security management behaviour of the employees.

The study found that when compared to employees in the business and education sectors, health sector employees are better at following and implementing ISPs. The authors of the study suggested that the reason for this is that health sector employees have better awareness along with good communication and reward systems. Moreover, employees in the health sector have a positive attitude to, and belief in the security policy norms as they recognise the significance of security policy. Other studies have shown that the level of information security awareness of employees working in banks in Australia were higher 20% than that of employees working in other industries and this was because of the sensitive nature of their organisation's information (Pattinson et al., 2017).

Alfawaz (2011) investigated the relationship between national, organisational and technological values to understand how they might affect the development and deployment of an organisation's information security culture in Saudi Arabia and found both dimensions of national and organisational culture to be underlying determinants of individuals' behaviour and this extends to information security culture, particularly in developing countries.

The question is how to apply appropriate ISPs in different cultural environments. Each organisation has different priorities, and the current organisational culture

may decide the desired level of information security culture (Tipton & Krause, 2006).

2.3.3.3.2 National culture

Alarifi et al. (2012) conducted a survey of 462 members of the general public in Saudi Arabia and found that information security awareness is very poor due to the highly-censored, patriarchal and tribal nature of Saudi culture compared to Western pluralistic democracies. In addition, they compared their study with research undertaken by Kruger et al. (2010) by using the same questions for users shown in Table 2.1.

Table 2.1: Password management

Response	South Africa	Saudi Arabia
I never change my password	27.3%	65.7%
I choose a simple and easy password	9.1%	45%
I share my password with others	0%	35.8%

The results showed that there was a significant difference between the two countries, and that South African users were more aware than Saudi Arabian users regarding password practices. Furthermore, Lang et al. (2009) found that 74% of users surveyed in Ireland said they never change their passwords. Karjalainen et al. (2013) conducted selective interviews with employees who were working in companies located in Finland, Switzerland, the UAE, and China. The findings show that employees in the UAE, and China are affected positively by administering punishments and rewards to comply with the ISP but not in Finland or Switzerland. In addition, monitoring ISP compliance had a negative effect on employees in Finland and Switzerland. The results suggest that different cultures require different information system security interventions.

Hovav and D'Arcy (2012) used the deterrence theory on employees' information system misuse in the U.S. and Korea. They found that the impact of perceived certainty of sanctions on IS misuse intentions for Koreans was stronger whereas the impact of perceived severity of sanctions was stronger for the U.S. However, regulations and rules are different from country to country and the studies above

showed that different factors influence employees' security behaviour positively, negatively and/or have no effect. Therefore, investigations into employees' security awareness and behaviour need to be in one country as they have the same regulations and roles.

2.3.3.4 Sanction and rewards

A number of studies have argued that sanctions and rewards have a significant impact on users' compliance with ISPs (Karjalainen et al., 2013). Furthermore, Bulgurcu et al. (2010) and D'Arcy (2009) applied ISP behaviour compliance models to investigate the role of sanctions on compliance and found that sanctions play a very important role in motivating firmer compliance with ISPs. In addition, Siponen et al. (2010) discovered that sanctions have a significant effect on actual ISP compliance and they strongly recommend that managers and information security staff establish sanctions for non-compliance. Furthermore, rewards do not appear to have a significant effect on employees' compliance. Knapp, Marshall, Kelly Rainer, et al. (2006) argue that one way to enforce the ISP is to use severe sanctions such as termination when employees regularly breach organisational security policy.

Siponen et al. (2014) argue that employees' vulnerability, normative beliefs, self-efficacy and attitude had a significant impact on their intentions to comply with ISPs. On the other hand, employees' rewards and response efficacy did not have a significant effect on compliance.

Conversely, Herath and Rao (2009), in analysing the penalties, identified that certainty of detection was found to be significant while, surprisingly, severity of punishment was found to have a negative effect on security behaviour intentions. Similarly, Pahnila et al. (2007) argued that sanctions do not have a significant effect on intention to comply with an ISP and rewards do not have a significant effect on actual compliance. Moreover, attitude, normative beliefs and habits have a significant effect on intention to comply with IS security policies.

Of course, not all the factors identified in this study will be useful for all organisations to improve employees' compliance with ISPs because each

organisation has different business functions, objectives, culture, and other characteristics.

2.3.4 Measuring information security awareness and compliance intentions

Some organisations measure their employees' information security awareness level regularly using different methods such as questionnaires of vocabulary (i.e., asking users to identify the meanings of key security terminology), scenario questions, qualitative interviews, and/or practical measurement by observing behaviours such as password strength. Employee awareness measurement identifies important factors which influence employees' behaviour.

Several researchers have conducted surveys to measure employees' information security awareness levels. Employee information security awareness can be measured by different models and psychological theories and those measurements can be categorized into three groups:

1. General information security awareness.
2. Information security awareness toward ISP compliance.
3. Information security awareness in different organisational and national cultures.

Vroom and Von Solms (2004) argue that monitoring or auditing ISP compliance behaviour is very difficult and an alternative auditing tool needs to be found. In addition, observing users' behaviours under laboratory conditions are not the same as actual users in the real workplace (Podsakoff & Organ, 1986). Therefore, behaviour (or, at least, behavioural intention) can be measured through scenario questionnaires, especially indirect questions (i.e., questions that do not directly ask participants what they would do in a given situation). In addition, Caulfield and Parkin (2016) argue that to explore how individual and organisational factors in the work environment affect security behaviours, scenario-based questionnaires can be used. Gross and Rosson (2007) investigated users' knowledge of security and threats and how they manage their security concerns. The results demonstrated that all users were able to deal with important information to which they had access but that their knowledge of the technical components of security such as firewalls and

virus scanners was low. Kruger et al. (2010) applied a questionnaire that consisted of two sections. The first contained a vocabulary test which included basic and generally known terms (e.g., what is phishing, spam, etc.). The second section contained scenario-type questions to evaluate respondents' behavioural intentions independently of their vocabulary knowledge. The findings confirmed that a lack of information security knowledge (vocabulary test) correlated with intended behaviour (scenario test) indicated by scenario-type questions. It is worth noting that the participants in the study were students and the sample size was small (n=44).

2.3.4.1 Scenario measurements

Alexander and Becker (1978) asserted that scenario questions provide researchers with something that closely approximates real-life decision-making situations. In particular, scenario questions have become more common in measuring ethical/unethical and anti-social behaviour (Hovav & D'Arcy, 2012).

Trevino (1992) commented that it is difficult to measure individual behaviour by direct questions because respondents are likely to answer questions in socially desirable ways. The scenario method allows indirect questions to be used to measure a person's likely intention to commit unethical behaviour.

Scenario questions have been applied in quantitative studies to measure users' information security behavioural intentions (see Table 2.2). All the studies in Table 2.2 used survey scenario questions. Interviewing participants leads to lower levels of self-disclosure of socially undesirable behaviour so in the current study online scenario questionnaires were used because they can make participants more comfortable disclosing personal information (Locke & Gilbert, 1995). Furthermore, the quantitative results can be generalised to a large population, which is randomly selected (Carr, 1994).

Table 2.2: Studies using scenario questions

Authors	Scenario questions	Scenario answers	Population	Number of questions
Farooq et al. (2015)	Direct	Direct (multiple-choice options)	614 students from University of	10

			Turku	
Kruger et al. (2010)	Direct	Direct (multiple-choice options options)	Two different class groups of small population of students (44 responses) at a university	9
D'Arcy (2009)	Indirect	Direct (point scale)	269 computer users from eight different companies in the USA	4
Vance et al. (2012)	Indirect	Direct (point scale)	210 employees from an organisation in Finland	6

Most studies used scenario-based questionnaires to measure users' intended security behaviours, for example, see D'Arcy (2009), Farooq et al. (2015), Kruger et al. (2010) and Vance et al. (2012). These studies differed in terms of the scenarios used, populations and the number of questions. When participants are presented with direct scenario questions they tend to select the best answer which does not necessarily reflect the way they would actually behave. Farooq et al. (2015) and Kruger et al. (2010) used direct scenario questions. For example, in Farooq et al. (2015) participants (university students) were asked to answer the question:

"Once a password is allotted for your university's email account, you do the following: (Select One most suitable)

a. I never change my default password
b. I change it when system asks me to change it
c. I usually change it
d. I always change it" (p.245).

Similar direct scenario questions were used in the Kruger et al. (2010) questionnaires but participants were allowed to choose more than one answer. In

both studies the participants would give the best answer (if they knew it) to show that they are doing well even when they were not. In this case, the researchers could measure knowledge and attitude of users but not their real behaviour.

D'Arcy (2009) and Vance et al. (2012) used indirect scenario questions in an attempt to measure information systems misuse behaviours. For example, D'Arcy (2009) included the following scenario:

"Scenario 1: Taylor received an e-mail from a friend that contained a series of jokes. Many of the jokes poked fun at the stereotypes that people often associate with different ethnic groups. Taylor found the jokes very funny and decided to send the e-mail to several co-workers."

Participants were then asked to select their agreement level for that action as if they were in that situation. That is, "If you were Taylor, what is the likelihood that you would have sent the e-mail? (very unlikely to very likely)". However, as the question is still asking participants what they would do it will still elicit direct responses leading participants to give what they think is the expected response rather than what they might actually do in that situation.

Given the variety of approaches to scenarios – using indirect or direct questions, giving a single answer or multiple answers etc. – and that the populations are general students from a single organisation, there is a research gap to consolidate and improve the use of scenario questions to measure behavioural intentions.

Indirect scenario questions followed by options identifying how a third party might behave enables assessment of employees' likely compliance with an ISP and identification of factors that might stop them complying with policy. In addition, much security research uses populations of employees and different organisations in different sectors (such as the medical sector), yet little work has been carried out exploring staff within Higher Education.

To address this gap, this thesis uses indirect scenario questions offering several behavioural options. These questions are put to staff within Higher Education

Institutes. In each question, participants are asked what the person named in the scenario should do. For example, (the current study):

"Ali is having a day off. His co-worker phones him and asks for Ali's password in order to access an important email he has received. What should he do?

a) He should give him his password because his co-worker is a trustworthy person.
b) He should not give him his password.
c) He should give him it if the email does not contain sensitive information.
d) If he is a close friend it is fine to give it to him."

Each scenario has four different answer-options based on a literature review, organisational ISP and IT staff interviews (what users' information security behaviour is considered to be like). The answers relate to reasons that have been given for noncompliance. Participants must select only one of the four possible answers. While Beautement et al. (2016) conducted an indirect scenario survey based on employees' security behaviour and attitudes, their survey did not systematically use influencing factors in the answers to explain why the participants might not choose the policy-compliant answers. In addition, that study had only eight questions, which is smaller compared to the current study, which used fourteen questions.

2.3.5 Higher education measurement and investigation methods

Katz (2005) pointed out that colleges and universities have enormous computing power and have open access to their clients and the public, which makes them susceptible to attacks. In addition, the IT infrastructure of universities and colleges allows geographically distributed academics to share large amounts of data and virtual computing resources (Rezgui & Marks, 2008). Furthermore, universities and colleges over the world have national and international students and staff and hold personal and educational records for these staff and students (Hina & Dominic, 2016). The ISP in the university is frequently ineffective at protecting information because of the lack of awareness amongst students and staff, less understanding with regards to the importance of information, lack of response in anticipating the

current issues, and a lower prioritisation of information security than other organisations (Ahlan & Lubis, 2011). Higher education institutions significantly depend on security controls and apparently ignore the compliance of end users with the ISP executed to guarantee institutional assets wellbeing (Hina & Dominic, 2017).

Kyobe (2010) examined factors influencing users' compliance with security policies and regulations in universities and ascertained that policy compliance remains a major challenge. He recommended that to guide users' compliance in universities, framework alignment requirements should be developed with control standards. Likewise, Hina and Dominic (2016) argued that the enhancement of information security awareness to keep information confidential, with integrity and available in higher education institutions is a challenging task.

Marks and Rezgui (2009) compared end users' information security awareness levels between different higher education institutions in different countries (UAE, UK and USA). They recommended that to establish enhanced information security in universities, elements such as having an ISP, campaigning and promoting, training, rewards and sanctions, and assessing and readjustment should be delivered sequentially.

Waly et al. (2012) studied three different organisational sectors (education, health, and business) to explore the factors that influence information security behaviour. In contrast, this thesis investigates multiple institutions in a single sector (higher education) in a single country (Oman).

Al-Awadi (2009) undertook interviews with 25 employees of the University of Glasgow in the UK as one part of a study. The investigation comprised two parts. The first used semi-structured interviews to elicit employees' views on the organisation' ISP, organisational security culture and ISP compliance. The second part was based on six indirect scenario questions to identify barriers to non-compliance with the ISP and to understand opinions about employees' behaviour based on those scenarios. The scenario questions covered leaving a computer without logging out, opening an unknown attachment, sharing passwords, writing

down passwords, illegal or immoral web surfing, and opening a CD from an unknown source in work machines. Her investigation centred on the effectiveness of the security policy in reducing security breaches within an organisation. The study revealed that employees do not comply with an ISP for several reasons: they are unaware of the security policy, they are affected by poor organisational security culture, they believe that it is someone else's problem, and are affected by individual values and beliefs and work pressure.

Several academic and industrial researchers have attempted to measure information security awareness in higher education sectors and have focused only on students and not on employees, such as Aliyu et al. (2010), Eyong (2014), Farooq et al. (2015), Fatani et al. (2013), Kruger et al. (2010), Masrom and Ismail (2008), Ngoqo and Flowerday (2015), North et al. (2006) and Zhang and Li (2015). Moreover, those studies that used employees as participants focused on only one university, such as Mahabi (2010), Rezgui and Marks (2008) and Marks and Rezgui (2009). However, the aim in this thesis is to investigate employees' behavioural intentions in multiple higher education institutions in Oman rather than one organisation in order to give a big picture of Omani organisations. While a focus on single institutions is helpful, there are differences across institutions in terms of reputation, size, location and policies. Looking at a range of institutions allows a better understanding of Omani institutions more generally.

Al-Kalbani (2017) conducted a survey of 294 employees in public organisations in Oman (18% working in the education sector) to explore the factors that affect their information security compliance. This survey focused on high level policy and management issues, improving information security management, awareness and training and discovering what employees wanted management to do to support them. The study did not explore specific concrete security behaviours such as password management, backup, incident reporting, etc. In addition, Parsons et al. (2014) argue that many survey studies of computer users in higher education focused only on one issue of information security awareness such as password-related behaviours, mobile computing or security features within specific applications. The studies on higher education above focused on a few specific

security behaviours, so the study in this thesis uses 14 different indirect scenario questions and each one has four different employee behaviours (totalling 56 behaviours) to identify employees' ISP compliance intentions and overall awareness level. Furthermore, these scenario questions will help to identify factors that influence employees to behave positively or negatively with regard to the ISP. While it is difficult to identify the most significant factors (Alotaibi & Furnell, 2016) this study will focus on eight factors: knowledge, response efficacy, subjective norms for organisation and/or manager, compliance, behavioural intentions, and sanctions and rewards in order to predict employees' ISP compliance intentions (for each scenario there will be direct agreement questions).

2.4 Summary

This chapter has reviewed the background of information security awareness and behaviour intention studies. It described the previous findings of information system security threats and vulnerabilities at different organisational environments and specifically in higher education environments. The chapter has highlighted measurement tools to measure organisations' information security awareness levels and the compliance intentions of employees. In addition, this chapter showed the role of information security awareness on employees' ISP compliance. The chapter reviewed the importance of exploring human factors and their role in influencing ISP compliance.

The literature showed that information security challenges still remain and research is needed to explore and understand the organisational and human factors that affect employee compliance with security policies especially in higher education environments.

Previous studies showed that even when an organisation has a good ISP, information security awareness programme, and software and hardware security, if they do not study employees' knowledge, attitude and behaviour the organisation will miss some critical issues.

Researchers have attempted to identify and explore the factors that affect employees' behaviour and found that challenges remain. An organisation cannot

guarantee that all employees will understand their roles in protecting information assets, even though an organisation may have an information security awareness programme (Kruger & Kearney, 2006).

The literature review showed the limitations and gaps in current knowledge about information security awareness and employees' ISP compliance. To the best of our knowledge, the direct and indirect roles of information security awareness on an employee's compliance have not yet been studied. The literature shows that none of the previous research studies applied indirect scenario surveys with answers derived from influencing factors, for large numbers of employees of different nationalities and different higher education institutions in the same country, and nor did they attempt to measure overall employees' information security awareness and behaviour intentions.

It should be noted that interesting and important research exists, but there are few studies dealing with employee behaviour intentions in higher education. To address this gap, the next chapter details a study with administrators and IT staff about their perceptions of the employees' behaviour and the threats this creates to information security. This helped to explore their perceptions of employees' information security behaviours in general and how these related to their understanding of information security threats and specifically, helped to explore what IT staff expect employees to do in the context of information security.

This information then fed into the design of a scenario questionnaire which was subsequently disseminated to employees within several universities and colleges in Oman (Chapter 4).

The scenario questions are based on several areas of information security designed to explore employees' information security compliance intentions (e.g., logging off or locking their computers when leaving their office, keeping passwords secret, backing up important data files.). In addition, this study aimed to identify factors that are perceived to influence employees to behave positively or negatively towards information security.

Chapter 3: UNDERSTANDING IT STAFF AND SYSTEM ADMINISTRATORS' PERCEPTIONS OF INFORMATION SECURITY

3.1 Introduction

This chapter presents research into the implementation of information security policies in higher education institutions in Oman. There are more than thirty of these universities and colleges in Oman. The study is based on an exploratory approach using a semi-structured qualitative interview method with IT staff and system administrators in four different Omani higher education institutions. Data were collected, recorded, transcribed and subsequently analysed to explore IT staff's perceptions of end users' behaviour, compliance with organisational information security policies, behaviours they believe are important, recent threats and recommendations to improve information security policy compliance. Figure 3.1 shows the chapter structure and overview.

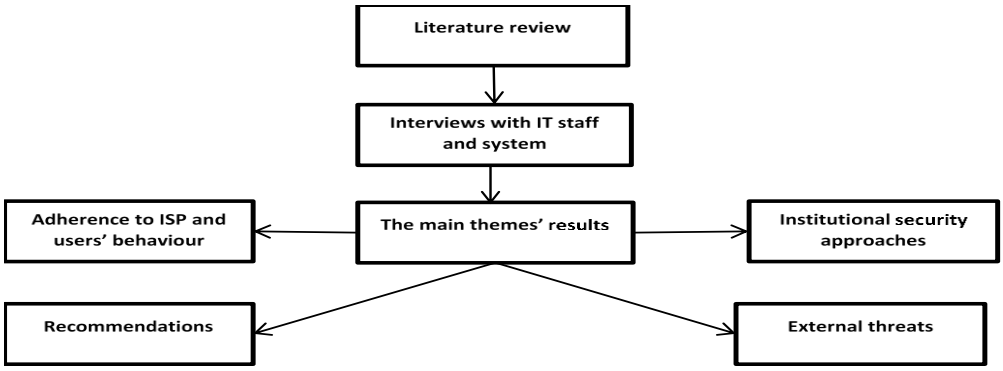


Figure 3.1: The chapter structure and overview

Organisations throughout the world face threats to the security of their information. These threats may arise from employees who, for whatever reason, do not comply with some or all of an organisation's ISP (see literature review for factors affecting employees' security behaviour). Users can find the security policy inconvenient, time consuming and generally a hindrance to getting on with what they want to use a system for (Chipperfield & Furnell, 2010) and so may not comply with it.

To ensure that employees can behave appropriately we must understand the threats that IT has to defend against, if policies exist and, moreover, if they are complied

with. To this end, interviews were carried out with eight IT staff and system administrators in four higher education institutions in Oman to identify threats that these staff considered the most prevalent and discuss their understanding of users' behaviours, either positive (promoting security) or negative (breaching policy and posing potential problems). The reason for conducting the interviews with IT staff and system administrators is because they are the people responsible for making decisions regarding information security in their universities and colleges. They are responsible for security, troubleshooting any problems, installing and configuring new hardware and software, meeting the needs of users and assisting them. Albrechtsen (2007) recommends the interview method in research to build an understanding of users' experiences in relation to information security. In the current study, the interviews with IT staff aim to elicit what issues are faced by the organisation rather than why users behave insecurely.

3.2 Methodology

After ethical approval was received from the university, participants were approached to take part in the study. First the study was described to all participants via the Participant Information Sheet (see Appendix A). This covers the purpose of the study, how confidentiality was ensured and the right to withdraw from the study at any time. It is important to ensure that participants feel that the information they reveal will not be used against them (Myers & Newman, 2007).

3.2.1 Interview questions

The semi-structured interview questions were designed to explore users' behaviour, which may contribute to information security threats and breaches, ISP compliance with and recommendations relating to information security in an organisation. In addition, the questions explored any recent security issues, the consequences of those issues and how concerned staff were about these issues. The initial questions are listed below:

a) What online security problems do you believe are caused by the behaviour of staff and students?

b) What external threats do IT staff defend the university network from? (What is the most frequent type of attack on the system and employees?)
c) Has the university experienced a security issue recently? If so, what do they think caused it and what were the consequences of that issue?
d) What areas of the IT security policy/end user computing policy do the staff and the students adhere to?
e) What parts of the IT security policy/end user computing policy do the staff and the students not adhere to?
f) Do IT staff have concerns about online security which are not covered in the current policies?

The qualitative approach was flexible and understandable and allowed the participants to explore the topic in depth. The questions were open-ended to encourage participants to speak freely, explore their own experiences, users' behaviour and improvement factors relating to information security. Questions 2 and 3 could have been combined but it was very difficult in the interviews to answer the third question, which is why they are separated.

3.2.2 Participants and Procedures

Eight IT staff and system administrators were interviewed using a one-to-one, face-to-face method. The information security policies of each organisation were collected before and during each interview. All the participants had a university degree and at least three years' work experience. These individuals are the persons responsible for network and information security in their respective offices or colleges and for that reason it was important to obtain detailed information from them.

The interviews were organised at a time convenient for the participants and took place in their own offices and meeting rooms at their own organisation. The interviews were conducted in English. The interview lasted approximately thirty minutes. Data was collected via note taking and voice recordings. The recordings were transcribed and a thematic analysis of the data completed. As shown in Table 3.1, five participants were from universities and three from colleges.

Table 3.1: Participants from each Organisation

No	Organisation	Number of Participants
1	A (Large size, university)	4
2	B (medium size, university)	1
3	C (medium size college)	2
4	D (small size college)	1
Total	4	8

To ensure that the findings were not idiosyncratic of one organisation participants were recruited from different sizes of institution (both colleges and universities) and from different geographical locations. Of the eight interviewees, four were Omani and the others were originally from other countries. The number of interviews depended on the number of employees in the organisation. For example, organisation A has the largest number with B the second highest number of contributors. At the start, several participants were not happy about recording the interview when they responded to the questions; however, after explaining how the data would be saved and used, they became relaxed and gave genuine answers.

3.3 Data analysis

The interviews were designed to determine the perceptions of IT staff and system administrators regarding security threats and their views on the role of employees' security behaviour. The interviews explored the problems that arise when employees do not comply with an organisation's ISP. Furthermore, the interviews provided an opportunity for IT staff to recommend any changes they wanted to see in security management at their institution.

Bogdan and Biklen (1992) identified data analysis as the

> *Process of systematically searching and arranging the interview transcripts, field notes and other materials that you accumulate to increase your own understanding of them and to enable you to present what you have discovered to others. Analysis involves working with data, organizing them, breaking them into manageable unites, synthesizing them, searching for*

patterns, discovering what is important and what is to be learned, and deciding what you will tell others (p.153).

After collecting the data, analysis began with the transcription of the interviews into written form. Thematic analysis was chosen for the analysis of the semi-structured interview data. Four main themes were identified from data. Based on the data, certain themes emerged which are related to internal and external threats to organisational security, staff's adherence to information security policies, and recommendations to enhance information security. Through coding and analysing the data the themes that emerged are shown in Figure 3.2.

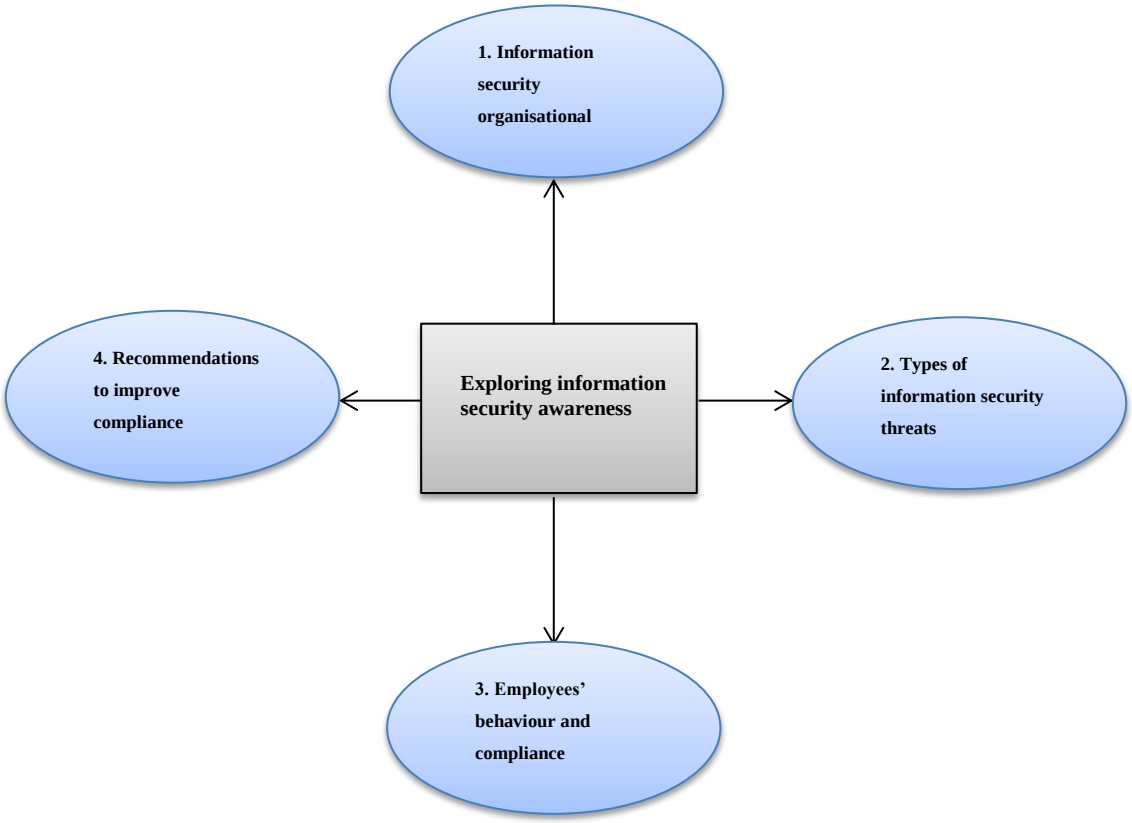


Figure 3.2: The four emergent themes

As shown in Figure 3.2, four broad themes emerged from the data analysis (1) organisation's information security, (2) types of information security threats, (3) employees' behaviour and compliance and (4) and recommendations. Within the major themes, sub themes were identified, such as password policy, not reading an email, etc. Subsequently, quotations from the interviews were used to directly

clarify each of these main points. The qualitative findings are supported by verbatim quotes from the participants.

3.4 Results

Technological security is an important issue and employees have access to sensitive information. The IT & system administrators from the four higher education institutions are described by presenting their work tasks of the organisation's information security. All organisations have a service centre to support the systems and other business areas, and furthermore, each one has a different name. The findings summarised in Table 3.2, shows the four main themes and their associated sub-themes. These themes represent the IT staffs' views of what is going on in their organisation.

Table 3.2: Summary of themes and sub-themes

Theme	Sub-theme	Description
1. Information security process in the organisation	Technology tools form a strong defence	IT staff depend on technology to secure their network, devices and applications. In addition, they have up-to-date hardware and software.
	ISP and regulation is not universal	Only two organisations have an ISP available and these do not cover many security issues and are not updated.
	The ISP is communicated via emails	All organisations mostly use emails to disseminate the ISP to users and to communicate with them.
	Access and operating privileges' are excessive	Staff have excessive privileges which causes more information security problems than are caused by students. Because of the culture staff believe that they should have higher access and operating privileges (e.g. have administrator privileges, downloading software from internet, disable antivirus, etc.)
2. Types of online information security threats	Email phishing, spam and viruses are the most common threats	Phishing and spam emails are the most common particularly if employees respond inappropriately such as providing usernames and passwords

		on request and clicking on links.
	Employees' behaviour is perceived to be problematic	The biggest threat to organisations' information security were employees' behaviours such as opening and downloading internet files and attachments that contain viruses.
3. Employees' ISP compliance behaviour	Compliance with ISP is perceived to be low	According to IT staff very few employees comply with the ISP because of a lack of knowledge and experience.
	Non-compliance with ISP is common	Most employees do not comply with the Organisational ISP because of a lack of awareness and factors related to organisational culture.
	The ISP should be readily available	ISP should be available, up-to-date and cover all relevant security issues.
	Communication to raise awareness	An organisation should use alternative ways to raise employees' information security awareness such as e-learning, videos, text mobile, face to face meeting etc.
4. Recommendations to improve compliance	Join the domain and limit the employees' privileges	Minimise employees' privileges and force them to join the domain network by strict policy and management support.
	Awareness and training	Ongoing awareness sessions, workshop and training to all employees.
	Sanctions and benefit	All users should know the benefits and consequences of following/not following the organisation's ISP.

3.4.1 IT staff and system administrators' views on their organisational information security

Organisations in the Middle East increase their security technology by using the latest software and hardware (Aloul, 2010). In the current study the semi-structured interviews showed that all the organisations involved believed they had adequate and up-to-date hardware (e.g., firewalls) and software (e.g. antivirus, firewall) to

protect their own information and the organisations' services. IT staff consider that most problems encountered are due to users causing breaches in the security of their organisation which IT staff believe is because of carelessness and being uninformed, and a lack of strict punishments. IT staff either did not have (because such statistics are not maintained by the organisation) or were not willing to divulge (for reasons of organisational confidentiality or concerns over reputational damage — see section 3.4.2 below) specific numbers of security incidents whether caused by employees or system problems. Therefore, it was only possible to use the evidence reported by the IT staff.

In the interviews, the majority of the participants said that there was good hardware and software in their organisations and they depend on technology to secure their network and devices and applications. Most organisations are using firewalls, antivirus software, and operating system patches and actively block ports which are not used in the network. According to one participant:

> *We [system administrators] are just going to make some policies even staff connect using the firewall and no one can access our server before they pass our security policies. And for that policy we make them update antivirus. They will update with security patches when they are applicable and accepted. After that they will connect to our network. Before this they are not allowed to get connected to our network or get any IP from that one [P7]*.

All organisations depend on their mail server to filter incoming and outgoing emails to protect the network from viruses:

> *We [organisation] have a mail server which is very good software that can protect our environment and our emails. It can filter the malicious software and it can scan all the emails going and coming and if some of staff have spam on their PC it can block him[employee] [P6]*.

3.4.1.1 Information security policy and regulation

In most organisations there are two types of information security policy: one for networks and computers and a user policy supplied by system administrators and IT staff. Firstly, computer policies are set up by system administrators on the

network and operating systems that allow users privileges to perform certain tasks on computers and access university information and devices such as printers, scanners, emails and websites. User information security policies (regulations and rules of the organisation which all staff and students are required to comply with) were discussed by participant 3:

> *First of all, we have two types of policies, computer policy and users' policy. The computer policy (implemented at the system level by system administrator) which applies on the computer system itself the operating system and applications and things like the user cannot control it so everything control by us [P3].*

However, not all organisations have an information security policy. The interviews identified that two organisations in the sample have a documented information security policy ISP which is available on the website, as one participant said:

> *They [end users] can read also the policy in the website [P1].*

Two organisations do not have a formal documented ISP but all organisations send emails to all users to inform them what to do and not to do with regards to information security. One organisation presents small policy notes when users log in to the organisation networks. These emails and notes tell users what is expected of them. Another participant mentioned that users are presented with very small sets of guidelines or policies when they log in to the organisation's network:

> *We [the organisation] haven't policy documented but we have some small notes when you switch on the computer you find small notes that guide you about what is computer and what password and what network is [P8].*

It is unclear which is the best approach: leaving a document on a website for users to view or actively sharing specific pieces of information. But clearly there are differences in practice that warrant further investigation.

Unfortunately, policies are often not updated for long periods of time. For example, participant 5 said:

It [policy] should be updated because here long time I mean it is the same policies [P5].

In addition, the information security policy is not complete and not understandable to the users in the organisation as one of the participants says:

Mobile services and wireless network access — these have not yet been implemented and the policy of those services which I mentioned are still an ongoing implementation and right now it is still in the development stage [P2].

3.4.1.1.1 Email communication of policy:

The four organisations send email rules and regulations to all their users and that was the most frequent method to disseminate an organisation's policy. For example, participant 1 said:

We [system administrators] have email policy, always sending them [end users] the policy of the email so they can read, they aware of what they must do when using email account for the college [P1].

In addition, if there are any problems or threats such as spam email in the network they use email alerts:

We [system administrators] always send email to the whole users in university academic, staff and students to make them aware of these kind of security threat [P6].

Most participants (n=7) thought that despite their efforts their employees are not aware of information security policies and therefore don't follow them which could result in security breaches. One participant said:

We network [administrators] are asking them [users] to follow the email policy most of them are not aware of those policy which results as I have mentioned earlier, in a security breach in our system [P2].

Even when an organisation has an ISP clearly located on its website, IT staff perceive that employees are not necessarily reading it.

From the site [website of the organisation] most of the staff they are not going and reading all these [ISP] [P5].

The findings suggest that IT staff believe that it is very important for information security policies to be accessible, documented and updated and their absence or poor quality could impact negatively on the organisations' information security. However, they also note that staff are not reading them.

3.4.1.2 Staff have potential to cause more problems than students

All of the interviewees said employees cause more problems than students because they have more privileges when using the organisations' networks. As one of the administrator said:

Staff have some permission but student don't have that permission they have limited permission to access the computers. Student cannot install software from the internet but staff can install but they are not aware about what is the purpose or they only use Microsoft then it will create problem because which staff give him some permission to install software that will create problem [P7].

This was confirmed by another participant from a different organisation:

Actually students' accounts have very limited access to computer [P8].

The culture in higher education institutions in Oman allows employees to have full control of their computers. The participants' comments above suggest that information security management staff do not have the power to force their employees to comply with their information security policy. For example, employees can disable antivirus software which is installed in the organisation's computers and install programs downloaded from the internet. The employees believe that this is one of their rights. As one participant said:

The most problems we [system administrators] are facing with staff is that they are prevented from joining the domain so this join to domain which is the main problem facing with the staff and without join the domain they will use the administrator so they have full control which they can install any

software which cause many viruses like third party software. ... They [academic staff] said I do not want work as limitation I want full control of my PC [P5].

This problem seemed especially true of those who have a higher position in the organisation:

Some academic staff according to their position they push IT staff to open computer in administrator account to download some programs from Internet in that case the IT under the pressure of this academic staff he can open the computer in administrator password by his account or he change his account academic staff to administrator…. Sometimes like high position people push IT staff to give him administrator [P8].

3.4.2 Types of online information security threats

Interview question: What online security problems do you believe are caused by staff and students?

Wiant (2005) points out that most companies fear bad publicity and don't talk about incidents that occur as a result of security breaches. Most of the surveyed literature reports finding difficulty in obtaining logs of security incidents from their participants and many incidents are underreported or undetected. Organisations might be afraid about loss of reputation if the media discover and then report an incident.

Most of the IT staff and system administrators believed that users are not aware of or do not care about security when they are using the internet in their organisation. The interview analysis shows that the majority of participants agreed that email phishing, spam and viruses are the biggest external threats particularly if employees respond inappropriately. In addition, breaches occur when the employees reply to spam or download attached files. Sometimes attackers use different methods such as spam advertisements as one participant notes:

We [IT staff and system administrators] are facing many problems as normal spams, phishing emails like general attack from outside ... most of them are

phishing that we are system administrator and we need your account and sometimes like this or sometimes from a company and we are winning hundred million Omani Rials and like this [P8].

Another participant from a different organisation added:

Online security problems we have actually encountered here - some malware attacks, and some phishing, also the problem of the email spambot which is external senders that send too many messages in our servers [P1].

Some participants shared the story of an attacker who has a valid username and password from an organisation, and what the consequences are, for instance, blocking an organisation's domain to other websites. As one of the participants, in a remark about phishing emails, said:

Say we need your password because we are doing maintenance some staff actually send their information without knowing those emails are not coming from the college, it comes from outside [P2].

And he mentioned the consequences that when hackers use usernames and passwords to access other servers then the domain of the university gets blocked:

Sometime we [organisation domain] are been blocked from outside or from like the main email provider such as like Google or Yahoo sometimes they would block our mail servers and those accounts sends spam again to others that's why we are been blocked [P2].

Another participant stated:

So then the hackers use these username and password to send huge of emails and this cause us problem like we are going to blacklist so our domain will be in blacklist in most of organisation [P5].

Another consequence is that attackers can use a username and password given by employees through replying to phishing emails and as a result, get access to the organisation's information system resources to steal data. One participant said:

A small hacker or a hack with a bit knowledge can get username and password and login remotely in somehow pretending that he is in the university and then use that person credentials and then access all the local information [P3].

Spreading viruses in the organisation (via USB sticks, CDs and opening attached files) was also perceived to be a direct result of staff behaviour. Viruses tend to spread through organisations' networks through employees downloading files from the internet, attaching their own laptops to the network, or inserting USB memory sticks and disk drives or CDs as all of these can carry viruses:

Sometime this virus attack that most came from USB some time they bring CD drive [P7].

In addition, employees tend not to scan their USB devices when using them in the organisation:

Flash memory also we [system administrators] are facing some of the problems because they [employees] are using flash memory without scanning [P5].

Employees are using external email services and opening attached files which gives viruses access to the organisation. One participant said:

Some of the staff is using Hotmail or Gmail which is not hosted in our environment they open attachments and this kind of things which have viruses [P6].

Regarding problems associated with installing software on their computers one participant said:

The staff is not aware when they are install [software programs from the internet] in their computers so there is some program install in their PC it has phishing software [P2].

3.4.3 Employees' ISP compliance behaviour

The interview findings showed that IT staff perceive that employees comply with some areas of information security and not with others, but the majority of interviewees agreed that their employees do not comply with the ISP. The administrators believe that users' behaviours cause many of the problems they face, including being blocked from email servers and viruses.

The majority of participants (n=6) believe that most of their employees are not aware of the organisation's information security policy and, hence, are also not aware of the consequences of their organisation's policy.

However, the picture is not uniform; two administrators mentioned that their employees follow certain parts of the organisation's specific ISP. As one participant said:

> *They [employees] are following some of the policies we apply [P4].*

For specific rules some employees could comply with ISP when they want to get new equipment or move system from one area to another they follow the procedure of the organisation as one participant says:

> *Most of employees here once they want a new system for example they follow the right procedure, they ask our director then he will forward it to the responsible department [P4].*

IT staff believe that the employees' security knowledge affects their compliance level and that those employees who have an IT background or knowledge of viruses would check emails and delete them:

> *Sometimes some employees have experience and know this virus different information level they have because some of them have already IT background and they know this is viruses and must delete it [P8].*

The participants stated that their employees do not comply with their ISP for different security behaviours such as physical security and password usage. In addition, they felt that most employees do not act responsibly when they have more

privileges for operating the antivirus system on their computer and installing software. With respect to physical security, sometimes employees leave the doors to their offices and their computers unlocked when they are not there. One participant said:

> *Plus, leaving the door office open which allow physical access to the computer… there is computer sometime they do not lock their computers [P3].*

3.4.3.1 Password policy

Participants reported that most users in the organisation do not follow the password policies relating to a strong password, for example:

> *I am very sorry to say that regarding to the password policy they [students and employees] are not really following what organisation recommended as they have to use strong password [P6]*

Additionally, they reported that employees write passwords on paper and save it on their computer, especially non-academic employees who come from the public sector as one participant says:

> *Most of the student or staff exactly I mean those who are old age coming from public sector [non-academic] they are writing the password in the papers [P5].*

The system administrators perceive that their employees often experience problems with passwords and do not comply with password information security. With regards to the changing of passwords, when employees were requested to change their password they often just changed one character. For example, the password "W3man123" gets changed to "W3man125":

> *The changing of password, the password has period of time they need to change and whenever they change they always use similar password they just a letter or number and unfortunately using like obvious password [P3].*

System administrators also noted that employees share passwords with other employees. Sharing usernames and passwords is not allowed by information security policies but unfortunately some academic staff share their IDs and passwords with their colleagues. As one system administrator points out:

> *We [IT staff and system administrators] have been announcing always [by email] telling them [users] please do not share your password please keep changing your password and these kind of things but unfortunately they are not following this policy [P6].*

3.4.3.2 Privileges for employees

Participants were concerned that employees were not taking responsibility for information security when they had increased security privileges. For example, they cited employees disabling antivirus software on their workstations and installing software downloaded from the internet as particular problematic behaviours. Staff were known to disable antivirus software to improve their computer speed.

IT staff and system administrators believe that this undesirable behaviour was because the employees are not aware of information security that they do not see security as being their responsibility, and they believe that applications such as antivirus software slow down their computers. One interviewee summarised the problem thus:

> *Staff complaining that their system is very slow, and this is because their system is compromised with virus, so what they did or what they are doing they are disabling their antivirus that are been installed in their computers…I [staff] will disable the antivirus to make my system work faster [P1].*

In other words, maintaining productivity was proposed as one reason for insecure behaviour.

Another problem facing system administrators was that staff would download software directly from the internet without asking for permission from the IT staff

and without running virus scans to ensure the software is free from malware. In addition, some staff holding senior positions in the organisation ask for administrator privileges. As one participant remarked:

> *Most of them [academic staff] say that they need that software urgently for teaching like this we need software to download from internet but maybe this software is free and it is open source software but he didn't download before and check it by make scan by antivirus he need download direct from inside direct to his computer and he push technician to do that job and sometimes he said I am in hurry and no have time he make many problems to open his computer in administrator and he feel that if he is in higher position so he must have full facility full access to the network [P8]*.

Interviewees claimed that some employees open emails which have a virus attached even though IT staff send emails to all users in their organisation warning them not to open particular spam emails. One participant said:

> *Sometime when we found this spam before it becomes an employee issue, I made general email to all university that is one email coming from company or from this source please when you found this email direct delete it without open that. Sometimes some employee opens and he is attacked by virus [P8]*.

Of course, such warning emails are often sent after the phishing emails have already been received so IT staff are too late in responding for some users.

Several of the administrators commented that most employees do not even check the source of emails. While this is not a reliable method for avoiding trouble, not checking it at all is problematic. Some emails could have attached files containing viruses. Some (written by hackers) could pretend to come from system administrators in their organisation and ask for a username and password. Unfortunately, employees open these emails and supply the requested information or download the attached file which has viruses:

> *Unfortunately, they [employees] are not reading the email they receive an email they [hackers] ask for username and password and directly they give*

the username and password so later on this hacker will use this username and password and they are using emails we are facing a lot of these [P5].

One interviewee mentioned that users do not check emails that they receive even if this is explicitly required by their organisation's policy. As one interviewee noted:

A lot of people when they receive phishing email when they asking for username and password they are kind of personal information they do fill the form or they click on the link and they go to those and that is why a lot of problems we are facing [P3].

3.4.4 Recommendations to improve compliance

Participants recommended that management should enhance information security and try to increase information security awareness in order to improve ISP compliance. In addition, they mentioned important factors which could change employees' behaviour regarding compliance with information security policy.

3.4.4.1 Information security policies and regulations

All participants confirmed that information security policies are very important for their organisation. They believe that policies should cover all areas, be up-to-date, easy to understand and available on the organisation's website. One participant commented:

The policy should be improved every year up-to-date because the IT improvement every day and IT change every day [P5].

Another advised that the information security policy should be on the organisation's website:

Policy must be clear for student for staff for everybody in website [P8].

In addition, system administrators believed that an organisation's regulations should be known and strictly enforced. For example, all employees should sign an information security agreement that he/she is responsible for their behaviour regarding security issues and moreover, that there will be appropriate action taken

against those who disobey the regulations, legislation and/or organisation's information security policy.

With regards to changing passwords from time to time, one participant says:

> *I think it should be forced by the administrators – to have to change their [users] password periodically which means every three months every six months I think we should follow this policy [P6].*

While users may make minor changes (e.g. one letter change) to get around this, the system could be designed to force more significant change. Of course, recent advice from the UK government's National Cyber Security Centre (NCSC, 2015) recommends not requiring regular changes to passwords at all but, instead, choosing a memorable but very strong password and keeping it.

3.4.4.2 Communication to raise awareness

When the information security policy is written and in place in an organisation, participants felt that communication and sharing of knowledge between IT staff and all users in the organisation should occur. Organisations have many ways to disseminate the ISP and to raise awareness of it but they would be more effective for all users when there is effective communication:

> *I think increasing awareness and these by emails like posters visiting [employees in] the colleges for awareness policies... I think is changing the way I mean like visiting these colleges and meeting staff and increase the awareness just to show to everyone [P5].*

3.4.4.3 Minimise employees' privileges and ensure they all join the domain network

Most organisations implement different privileges related to different employee roles and responsibilities. For instance, the results show that each organisation has assigned IT staff and system administrators to have direct responsibility for the organisation's overall information security and were required to maintain security policies, install and configure new hardware and software, add and remove system users, set up initial passwords, provide education and training to the end users, and

so forth. On the other hand, system administrators would prefer if end users were not be able to make system changes and did not have administrator privileges.

One participant stated that it would be easy for him and his team to control and monitor employees' computers and the network when they are in the domain:

> *The computers were in domain it is easy for us it is centralized and easy for us to adapt to push any breaches, any update and control them and to monitor if there is any kind of weird or strange behaviour in those computers so at least really we can monitor what is happening [P3].*

In addition, the same participant suggested that information security management should be centralised when all employees join the organisation domain which would help them to apply the proper policy:

> *We can apply for proper policy because once all the computers on the domain applying policies for those in the domain is easy to apply any other systems and control it centralised and everything through this kind of things [P3].*

The most important finding was with regards to user privileges; in all four of the organisations involved, some employees insist on having full control of their own machines to enable them to download and install files from the internet, disable the antivirus, etc. System administrators believe that the ISP should restrict user privileges:

> *If they [employees] are not joining to the domain, they should have the administrator but we are trying now to join most of them to the domain PCs. It is easy for us to make policies to reduce these viruses and spam [P5].*

All four organisations complained about employees' access privileges stating that most of them can get workgroup administrator privileges which allow them to install programs from the internet and run it on their work computer:

These staff's computers are not connected with our domain they are working in a workgroup so sometimes they are able to remove the antivirus on their computes [P7].

3.4.4.4 Training and awareness

All eight participants believed that the best way to reduce the number of security incidents is for their organisation to provide regular awareness and information sessions for their employees.

We [system administrators] can minimise the threats which we have by giving them awareness and giving them [employees] sessions the right way… So my recommendations first of all to increase the awareness sessions for students and staffs and introduce them to the new technologies and services that centre providing for the university to minimise the threat of viruses and things like that [P3].

For my recommendation there should be awareness for staff and students so regular symposiums regular workshop for staff and students to be able for them to know or realised the important of those policy with proper training to them proper information to be able to see the importance of implementing those policy [P2].

Once we get our staff and students educated in IT. I mean we got some pain of headache getting this problem in our environment [P6].

Two participants indicated that employees will change their information security behaviour for the better when an organisation puts awareness programmes in place. When one participant was asked whether staff lock their office door and PC when they leave their office he answered:

Majority now yeah, previously was not because since we started the awareness the improvement we can see the trend [P3].

While ISP awareness is not necessarily sufficient to increase compliance, it is nevertheless, one of the ways that IT staff felt would increase compliance.

3.4.4.5 ISP compliance: sanctions, benefits and responsibility

One participant suggested that employees could be influenced to follow the ISP if they knew the benefits of policy compliance, and there should be sanctions for non-compliance:

> *When he [new employee] joins the organisation it must be in clear place for users to read security policy and regulations and know what are the benefits and the punishments if they did not follow this [P8]*.

He mentioned that employees feel that information security is not their responsibility and they do what they want because they know that IT staff will fix their security problems when they occur.

> *Others [employees] are not aware because they know that IT will replace his computer [P8]*.

3.5 Summary of IT staff and system administrators' views on information security

The results showed that higher education institutions have numerous technological practices available to protect the IT infrastructure. The organisations use security technology such as firewalls, antivirus, security patches, etc. The IT staff at the four organisations stated that information security is a very important issue for them and their organisations. This study indicated that IT staff believe that the major reasons for information security breaches were not to do with technology as all the organisations involved had up-to-date hardware and software. Rather, the study revealed that the IT staff and system administrators were mostly concerned with information security threats related to employee behaviour. Six out of the eight participants believed that most employees do not follow their organisation's ISP. They offered a number of recommendations for a better information security environment.

Participants believed that users should be provided with well-written ISPs, training, regular communication and awareness because these, they felt, play a very significant role in the process of enhancing information security behaviour in the organisation.

There was concern that the organisations suffered from a lack of user awareness of information security which was linked to poor information security behaviour. The participants admitted this because there is no ongoing and proper training, campaigning, strong communication or sanctions system regarding information security in their organisations. Participants from two organisations stated that they are giving awareness sessions for students and employees and they were improved but that was not continuing because of management. Yet very few universities are known to offer IT security awareness sessions to students and staff (Rezgui & Marks, 2008).

In general, the findings have shown that email and website phishing, spam, viruses and denial of service were perceived as the most substantial threats to information systems. Interviewees believed that employees were not familiar with external threats and they were not aware of the consequences of security breaches which affect their organisation. In contrast, the findings indicate that employees with IT background and knowledge avoided these external threats.

IT staff perceived employee mistakes, such as responding to spam or phishing emails to be particularly problematic. The interviews indicate that how employees behave in terms of in information security depends on their knowledge, background and experience of using computers. According to the participants, employees were replying to phishing emails and had bad password practices and this result agrees with the results of a study of employees at the Zaid University in UAE (Marks & Rezgui, 2009). Participants across the four organisations stated that their employees did not follow basic information security practices such as not writing or sharing and changing their passwords. This is particularly problematic for organisations, as Safa, Von Solms, and Furnell (2016) point out "hackers target people, rather than computers, in order to create a breach". They point to poor password, email and download behaviours as particularly problematic to organisations.

Moreover, employees in all the organisations surveyed have different qualifications, with some of them having academic experience and others not. In addition, some of them have lengthy experience of dealing with computers, whereas others do not. Furthermore, organisational cultures, job positions, different nationalities and staff

joining from different organisations were judged by participants to play a significant role in employees' information security behaviour.

All the IT staff and system administrators interviewed believe that users should only have limited privileges to access their organisation's software and hardware but the interview findings showed that all the organisations have provided most of their employees full control of their workplace computers and that this has caused many problems for the organisation. For example, employees download and install files from the internet which have viruses and they also disable the antivirus in their computers because they think it will make their computers faster. Eining and Christensen (1991) found that participants believed a person's behavioural intentions would be influenced significantly by knowledge of the consequences. Similarly, the current interviewee suggests that bad behaviours result from a lack of knowledge about the consequences for their computers and the organisation.

However, Wiant (2005) investigated whether the presence of an official information security policy impacted the number of security incidents and found that the presence of a written policy did not reduce the number of computer abuse incidents. Universities today need to find other ways to improve behaviour. Relying on end users to read the policies is less effective (Rezgui & Marks, 2008).

Moreover, participants believed that organisations should provide ongoing education and training for employees to increase awareness. Overall, these results indicate that IT staff believed that employees do not feel that they are responsible for information security issues, as most participants stated that employees are not aware of information security and they believe that if anything happens to the organisation that only IT staff are to blame, despite the employees in the education sector revealing information that should not be disclosed to an unauthorised person and making their machines vulnerable to malicious code by opening attachments.

Finally, all participants recommended ways to build successful information security management and improve employees' ISP compliance. They suggested that organisations should have an up-to-date ISP which is available for everyone to see. Training should be provided to explain the ISP to employees and avoid the problem

of staff not reading the ISP. Furthermore, information security management should build good communication with their employees to share knowledge regarding information security to protect them from threats and meet with them face to face to introduce them about organisational information security policy. In addition, information security management should minimise the privileges of employees and force them to join a domain network that would help them to have good control over the security of the networking environment.

3.6 Summary

This chapter presented an overall discussion of information security problems, challenges and solutions perceived by IT staff in four higher education institutions in Oman. The findings indicated participants' experiences with their organisations' information security threats, incidents, consequences and their perceptions of employees' information security behaviour in general, and specifically information security policies.

The investigation established that the results from this study matched findings from previous studies by confirming that human behaviour is perceived to be a frequent cause of information security breaches. IT staff discussed a number of non-compliant behaviours and ways in which users justify these behaviours. Therefore, the next step is to investigate these behaviours and explore factors that influence employee compliance with organisational information security policies.

IT staff and system administrators recommended that the organisations should establish clear, strict rules in an up-to-date ISP, and provide regular workshop training for employees. There are a number of important changes which need to be made in organisations' policies and strategies for information security and user behaviour. Moreover, more all organisations should undertake regular training and make proper information security available to all users. None of the institutions participating in this research offered information security training or awareness campaigning despite all participants identifying the importance of having employee awareness programmes. IT staff also expressed a belief that enforcing sanctions for non-compliance would make a difference, however, Aurigemma and Mattson

(2017) point out that employees' perceptions of the usefulness of sanctions is dependent on their previous experience with sanctions.

It was not possible to get concrete data about the extent of security incidents in the organisations involved. Some organisations did not keep such records and others were not willing to divulge such information. However, the IT staff and system administrators interviewed were responsible for their organisations' information security and were sharing their views and impressions based upon their experience of what happens in their organisations. Clearly, administrators believe employees are responsible for most security problems in their organisations. To explore the validity of these beliefs the next chapter presents a questionnaire survey that was distributed to a number of different education institutions in Oman to investigate the behavioural intentions regarding 14 different security behaviours extracted from ISPs. The survey also investigates what factors staff believe influence those intentions, in a range of information security scenarios. The results are then compared to the interview findings to see whether the IT staff and system administrators' perceptions were accurate.

Chapter 4: UNDERSTANDING EMPLOYEES SECURITY BEHAVIOUR INTENTIONS

4.1 Introduction

Previous studies (e.g., Bulgurcu et al. (2010)) have treated ISP compliance as a single behaviour, when in fact an ISP incorporates many different behaviours. This study examined employee intention to comply with ISPs in the Omani higher education sector. The aim of this study was to measure employees' security and policy compliance intentions for each behaviour and likely. Online behavioural scenario questionnaires were used to identify factors that affect employees' intentions regarding information security policies.

The literature review has shown that both direct and indirect questions have been used previously. A drawback of using direct questioning ('what would you do in this situation?') is that participants are likely to give the answer they think the researcher is looking for rather than indicating their actual intentions. The literature suggests that giving participants indirect questions in which they advise a third party on what they should do leads to answers which more reliably reflect what the participant would, in fact, intend to do in that situation (Trevino, 1992).

Each of the 14 scenarios used in this study provided four possible behaviours from which participants were required to choose which they thought the person in the scenario description should do. The scenarios and their four possible behavioural responses were designed to present participants with genuine situations in order to measure how they would intend to behave in the situations. Although only one of the responses for each scenario was policy-compliant (i.e., derived from the actual ISPs) the others were all plausible behaviours (some of which had been identified as being carried out by employees during the IT staff interviews discussed in Chapter 3).

It is worth mentioning that only a few studies employing scenario questions to measure employees' reactions have been conducted on information security in the workplace and do not utilise plausible answers as distractors. The questions and answers were drawn from the literature review, the interviews with IT staff and

system administrators in different educational sectors in Oman, and most scenario behaviour questions were drawn from the information security policies of several Omani academic organisations. The fourteen scenario questions were designed to test employees' awareness and knowledge of their security behaviour.

This chapter explores behaviour from three angles: demographics, scenario questions and social factors, as shown in Figure 4.1.

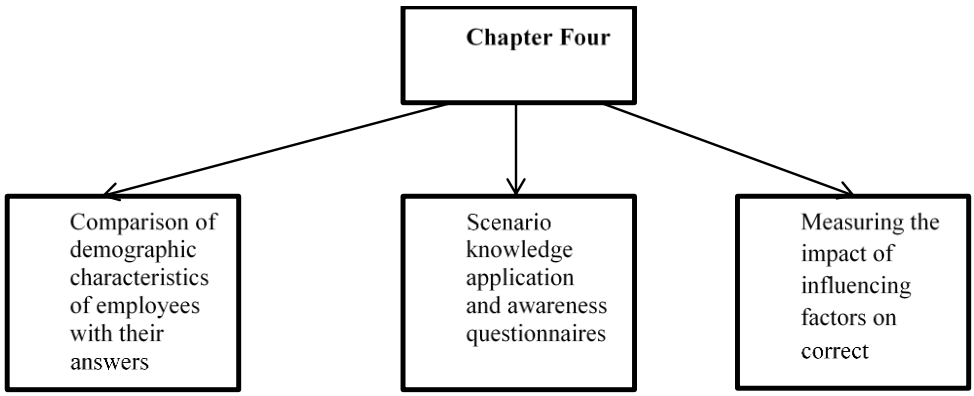


Figure 4.1: Structure of Chapter 4

The first identifies the relationship between demographics and compliance intention, identifying if any difference in compliance is related to demographic differences. The second identifies the behaviours that employees chose in response to security scenarios. The third section explores the factors that participants believed influenced their decisions about how the fictional characters in the scenarios ought to behave.

These factors have been drawn from a number of theories of behaviour. Protection Motivation Theory is particularly relevant to Information Security as it is based on assessing threats, in this case cybersecurity threats, and people's ability to cope with the threat, i.e. are there responses, that people have the skills to employ, which will effectively remove the threat. In addition to this assessment of threat and ability to cope, they must also have knowledge of the expected behaviour (KAB models). In addition, the Theory of planned behaviour brings in the idea of social norms and that people are influenced by how others around them behave (both peers and influential others such as managers). This approach to behaviour is also recognised in Social Learning Theory which is frequently used in crime studies (Akers 2017). Lastly, it is

important to note that behaviour is influenced by rewards (positive reinforcement to encourage a behaviour) and sanctions (negative reinforcement to reduce a behaviour) (Skinner 2014). These factors will be utilised in Chapter 4 to explore which ones employees perceive to influence their behaviour.

4.2 Methodology

The questionnaire was based on knowledge gaps highlighted by the literature review and the results of the interviews conducted in Chapter 3. The survey, which was designed to explore employees' information security compliance intentions in general and to identify specific information security issues around what employees consider to be appropriate behaviour in the light of their organisation's information security policy, was disseminated to several universities and colleges in Oman. In addition, the survey was used to explore what factors impact employee information security behaviour intentions both positively and negatively.

4.2.1 Questionnaire design and analysis

The questionnaire was administered online using the Qualtrics survey platform (see Appendix D). The questions were based on a review of the literature on psychological theories which have been applied to security behaviours, colleges' information security policies, psychological theories and analysis of the interviews conducted in the first study (Chapter 3). The survey comprised two parts:

1. The first section dealt with general questions (demographic) such as name of organisation, job title (optional) academic/non-academic job role, nationality, gender, age group, employment period (years), qualifications, admin privileges, availability of ISP (and, if yes does he/she claim to understand the ISP).
2. The second part comprised 14 indirect scenario questions. Each scenario contains three plausible but incorrect answers and one policy compliant answer, and rating scales for 8 different behavioural influencers.
    a) Each scenario has four behaviour options and participants were required to select the one option that they believed to be correct. The 14 scenario questions focus on five main security issues: backup,

password management, physical security, phishing and virus threats, data leakage, work environment and privileges. The 56 security behaviour options (14 scenarios × 4 options) were based on the literature review, information security policies and the results of the interviews with the IT staff and system administrators (Chapter 3). In addition, the scenario questions were designed to measure five influence factors: trust, authority, productivity, responsibility and curiosity.

b) In each scenario, participants were asked to rate their beliefs about influencing factors across the different scenarios. In this part, participants' perceptions of influencing factors, knowledge, response efficacy, subjective norms for organisation and/or manager, compliance, behavioural intentions, and sanctions and rewards, which may influence employees to comply with an organisational ISP were measured using a five point Likert scale running from strongly agree (=5) to strongly disagree (=1).

4.2.2 Pilot Study

An initial version of the questionnaire was designed and piloted with 16 randomly selected employees (male and female) from different higher education institutions and different nationalities. The participants were between 26 and 65 years of age and came from a range of nationalities. After completing the questionnaire, participants gave their feedback on face validity (what did participants think each question was trying to achieve, and did they make sense) and provided suggestions as to how the questions might be made easier to understand. The survey was then revised to improve its comprehensibility to participants and correct any spelling and grammatical errors.

4.2.3 Participants and procedures

The revised questionnaire was then loaded onto the Qualtrics system to allow online data collection. Invitations to take part were sent by email to all employees in a number of higher education institutions in Oman. The invitations were sent by system administrators from the organisations to employees. 898 members of staff

responded, 395 were excluded from this study due to incomplete questionnaires. The remaining 503 complete responses were provided by participants from twelve universities and colleges across Oman which is 56% of the targeted sample. The average time taken to complete the questionnaire was 18 minutes.

The first set of questions focused on demographic information about the respondents, such as the name of their organisation, age, gender and qualifications to enable the results to be categorised. Statistical Package for the Social Sciences (SPSS) was used to collate and analyse the responses.

4.3 Results

Fourteen scenario questions were designed to test employees' security behaviour intentions; only one participant out of 503 scored 100% correct answers, as shown in Figure 4.2. This figure also illustrates the spread of overall individual compliance intentions, i.e., some participants chose the compliant answer more than others. In this study, as measured by the number of correct answers, 88 participants (17%) scored 1-5 (poorly), 290 (58%) scored 6-9 or (average) and 125 (25%) scored 10-14 (good). The average score was only 7.7, which indicates employees provided the correct answer just over 50% of the time. That is, for each question, only half the participants gave the policy-compliant correct answer with the others choosing one of the three plausible but incorrect answers. Approximately half the participants achieved an average score.

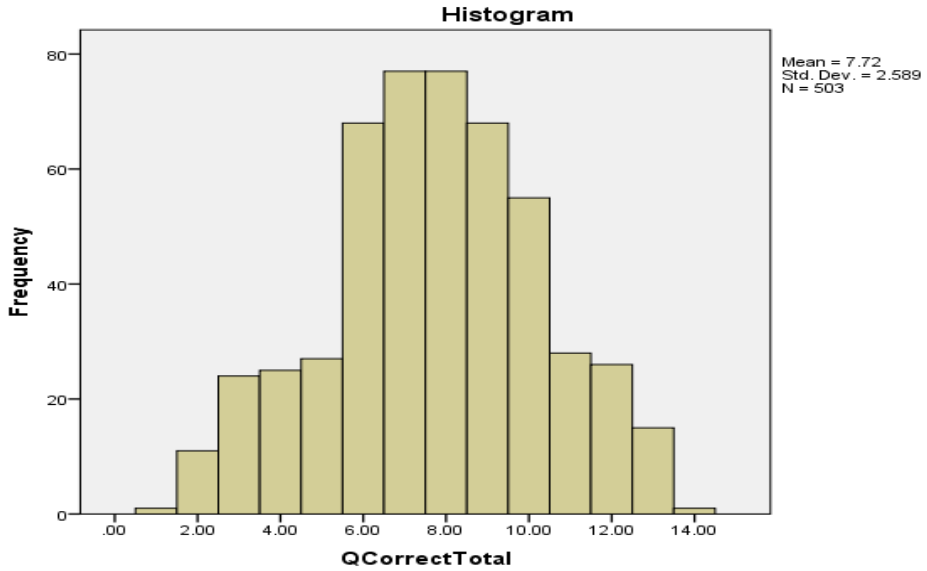


Figure 4.2: Overall awareness level

Kruger and Kearney (2006) classified awareness for a region or sector of a business in three levels: poor (0-59%), average (60-79%) and good (80-100%). In this data, the sector is higher education in Oman. Table 4.1 shows the frequency of correct scores achieved by this sector. This table highlights that behaviours should be considered individually as the number of employees making policy-compliant decisions, in the sector, varies by scenario.

Table 4.1: Results grouped according to Kruger and Kearney (2006) awareness levels

% Participants who intend to comply with ISP behaviour	Behaviour scenario number
Good (80-100)	9, 12, and 13
Average (60-79)	4, 10, 11 and 14
Low (59 and less)	1, 2, 3, 5, 6, 7 and 8

In the following sections, the results for each type of behaviour are discussed. The following section is divided into three parts. The first looks at employee score by demographic characteristics. The second looks at the answers to the 14 scenario questions and the third part looks at the ratings for the eight influencing factors

(knowledge, response efficacy, subjective norms for organisation and/or manager, compliance, behavioural intentions, and sanctions and rewards).

4.3.1 Survey data analysis demographic details

Respondents came from twelve universities and colleges; five are combined as 'other' as they consisted of very small numbers of respondents. Table 4.2 presents the summary statistics for the responses in numbers and their percentages in relation to the demographics. All questions are compulsory except organisation name and job title which were optional to provide further anonymity (job titles see Appendix B). As can be seen in Table 4.2, the highest number of participants came from organisation A (36%).

Table 4.2: Demographic characteristics of participants

Demographic/Group	No. Responses	Total of Responses (%)
Organisation (University/College)		
A	181	36
B	90	17.9
C	87	17.3
D	68	13.5
Others	26	5.1
E	20	4
F	18	3.6
G	13	2.6
Category of staff		
Academic	385	76.5
Non-Academic	118	23.5
Staff nationality		
Egypt	7	1.4
India	222	44.1
Oman	170	33.8
Other	33	6.6
Pakistan	15	3
Philippines	48	9.5
United Kingdom	7	1.4
Gender		
Male	324	64.4
Female	179	35.6
Age group		
18-25 years	16	3.2
26-35 years	172	34.2
36-45 years	247	49.1
46-55 years	50	9.9
56-65 years	18	3.6

Employment period (years)		
Less than 1 year	50	9.9
1-5 years	264	52.5
6-10 years	125	24.9
11-15 years	38	7.6
16-20 years	15	3.0
21 years or more	11	2.2
Qualification level		
High school	9	1.8
Diploma	16	3.2
Bachelor's degree	110	21.9
Master's degree	263	52.3
Doctorate	105	20.9

The majority of the respondents (76%) are academic staff, 44% are from India and 34% from Oman. The majority (64%) are male. Half of the respondents are from the 36-45-year-old age group. Moreover, in terms of years working in organisations, more than half of the respondents (52%) have worked from 1-5 years. The results demonstrate that the majority of the respondents are well-educated as 95% have university level education.

To analyse this information, independent-sample t-tests and one-way ANOVA tests were employed to identify if there are significant differences in the mean value in the respondents' security decisions. An independent-samples t-test was conducted to identify significant differences in the mean values of the respondents' knowledge of the correct behaviour (the fourteen scenarios scores) in the staff category, gender and admin privileges groups, which comprise two different groups.

Table 4.3 shows the relationship between compliant answers and the demographic variables with the results of a series of one-way ANOVA tests (Field, 2009) to assess whether demographic characteristics are linked to participants' security behaviour intentions. The effect of ten demographic variables was examined: organisation, staff category, country, gender, age group, employment period, qualification, admin privileges and the availability and understanding of an ISP. Organisation, nationality, gender, age group, employment period, qualification and administrative privileges exhibit a significant effect on security decisions.

In addition to the significance tests, effect sizes were also estimated. An effect size is a way to measure the magnitude of any significant effect (Coe, 2002). According to Cohen (1992), effect size values of 0.1 signify small, 0.3 medium and 0.5 large effects, respectively. The second test was the ANOVA which was applied to the remaining variables from Table 4.3 , (A, C, E, F, G, I and J), which have more than two different groups. Table 4.3 confirms that six mean values were significantly different: nationality, gender, age, employment period, qualification and administrative privileges.

Table 4.3: Comparisons of participants' characteristics and correct responses

Variable	Group	N	Mean	p-value	Effect size
Organisation	A	181	7.3315	0.06	-
	B	90	8.4000		
	C	87	7.6437		
	D	68	7.6765		
	Others	26	7.6154		
	E	20	8.2500		
	F	18	7.6111		
	G	13	8.7692		
Category	Academic	385	7.6805	0.52	
	Non-Academic	118	7.8559		
Nationality	Oman	170	7.7824	.000**	-
	India	222	7.3964		
	Pakistan	15	8.2667		
	Philippines	48	8.5833		
	Western	18	9.8889		
	Other	30	6.8333		
Gender	Male	324	7.9568	0.006**	0.13
	Female	179	7.2961		
Age Group	18-25 years	16	6.8750	0.001**	-
	26-35 years	172	7.2733		
	36-45 years	247	8.0364		
	46-55 years	50	7.7800		
	56-65 years	18	8.2778		
Employment period (years)	less than 1 year	50	7.2200	0.000**	-
	1-5 years	264	7.4318		
	6-10 years	125	8.0400		
	11-15 years	38	9.2632		
	16-20 years	15	6.8667		
	21 years or more	11	9.1818		

Qualification level	No university	25	6.4400	0.006**	-
	Bachelor's degree	110	7.9818		
	Master's degree	263	7.9240		
	Doctorate	105	7.2476		
Admin privileges	Yes	105	7.0667	0.008**	-0.15
	No	398	7.8945		
Availability of ISP	Yes	352	7.7955	0.599	-
	No	22	7.4091		
	I don't know	129	7.5736		
Understanding of ISP	Strongly Agree	89	7.7865	0.160	-
	Agree	211	7.9953		
	Neither Agree nor Disagree	41	7.1463		
	Disagree	8	6.5000		
	Strongly Disagree	3	6.3333		

***Note:** Degree of significance = *p <0.05 or highly significant = **p<0.01.

Independent-samples t-tests regarding respondents' compliance intention answers reveal that there is no significant difference between academic and non-academic staff. Conversely, significant differences were identified between different gender groups and moreover, who has or does not have administrative privileges.

There was a significant difference between male employees (M=7.96, SD=2.66) and female employees (M=7.30, SD=2.41), t (501) =2.75, p<.01; however, the effect size (0.13) was extremely small. Furthermore, employees who did not have administrative privileges (M=7.89, SD=2.48), were significantly more knowledgeable about the ISP than those who have administrative privileges (M=7.06, SD=2.85), t (501) =-2.93, although the effect size is very small (-0.15).

ANOVAs were run for characteristics that have more than two groups. There were no significantly different compliance scores for different organisations, and the availability and understanding of ISP. Conversely, there are significant differences between means for nationality, age, employment period and qualification levels.

The results indicate that there are significantly different levels of awareness/compliance intention (p<.01) between employees from various countries.

The countries with the largest numbers of participants in this survey are India (N=222), Oman (170), the Philippines (N=48), Western countries (18), Pakistan (N=15) and other (most of the countries in this group had only one participant). There is no significant difference between the two largest national groups: Indian (M=7.4, SD=2.5) and Omani (M=7.78, SD=2.58). In contrast, there are significant differences between Western countries (M= 9.89, SD=2.05) and Indian and Omani employees. That is to say, the average score of participants from Western countries is higher than the Indian and Omani participants but they are a small group (18).

With regards to age, five age groups demonstrate a significant difference between employees' awareness scores ($p<.01$). The result shows that the 56-65 age group (N=18) scored significantly higher (M=8.277, SD= 2.585) and the 18-25 group age (N=16) scored the worst (M=6.8750, SD= 2.418) but these two groups have the lowest number of participants of all the age groups. Regarding the two largest groups, the 26-35 group age (N=172) with (M=7.273, SD= 2.595) scored less than the 36-45 group age (N=247) with (M=8.036, SD= 2.547).

The sixth grouping, work experience, demonstrates significant differences in means and the overall p-value is zero. When we compare the two largest groups (1–5 years, N=264 and 6–10 years, N=125) we see a significant difference between their performance (1–5 years, M=7.431, SD= 2.528; 6–10 years, M=8.040, SD= 2.553).

Respondents' qualification levels show a significant difference ($p<0.01$). Participants with a bachelor's degree scored significantly higher (M=7.981, SD= 2.756) than those with doctorates (M=7.247, SD= 2.786) and those with no university qualification (M=6.440, SD= 2.599). The finding that those with doctorates scored worse is unexpected and difficult to explain. Conducting several one-way between-groups ANOVA tests with a range of hypothesised interaction variables showed that while there was no significant interaction of qualification on age, gender, experience working with the organisation, or privileges, there was an interaction effect of qualification with nationality such that the effect on the scores of having a higher degree depends on nationality ($F(12) = 2.44$, $p=0.004$). For Omanis, there was a consistent pattern of improvement in scores along with increasing qualifications; this was not the case for any other nationality.

4.3.1.1 Summary of employees' demographic information

The majority of employees (N=290) scored 6-9 from a maximum of 14 correct answers, which means their knowledge of good information security behaviour is average. The study examines whether or not there are differences in relation to employees' awareness of the correct behaviour regarding information security, based on individual demographics. The fourteen scenario outcomes measure the difference between the mean scores of employees' knowledge of ISP-compliant behaviour and their demographics. The results show that from ten demographic characteristics, six of them demonstrate significant differences: nationality, gender, age group, work experience, qualification level and whether they have computer administration privileges or not. Further work is needed in the future to investigate why these differences exist.

It is interesting that there was no significant difference for availability of ISP suggesting that the presence of an ISP did not influence security awareness/compliance intention. In addition, there was no significant difference between those who said they understood the ISP and those who did not.

However, gender did display a significant difference with men scoring higher than women. In addition, employees who are older and have acquired more years working in an organisation made significantly more policy-compliant choices than younger colleagues who have fewer working years. Moreover, employees (N=18) from Western countries scored better than Omani and Indian employees. Furthermore, the lower an employee's qualification level, the less likely they are to score correct answers (although holders of bachelor's degrees achieved better scores than holders of doctorates). The effect size between two-variable groups (category, gender and administrative privileges) with correct answers is extremely small.

4.3.2 Analysis of employees' compliance intentions

The scenarios covered several areas of security behaviour from organisations' information security policies based on the major security issues of any information system, such as backup, password management, physical security, phishing and virus threats, data leakage, work environment and privileges as shown in Figure 4.3.

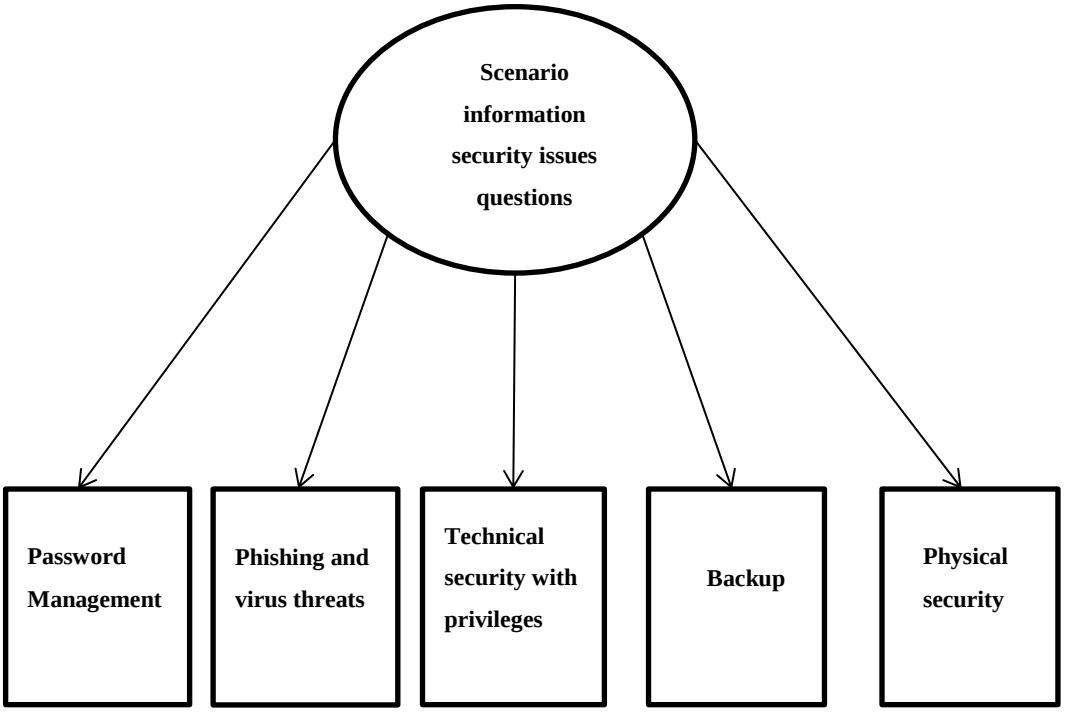


Figure 4.3: Scenario information security issues questions

4.3.2.1 Employees' information security policy compliance

Figure 4.4 shows that employees do not intend to comply equally with all aspects of the ISP. For example, 94% of employees chose the correct answer in scenario 13 which dealt with incident reporting (missing files), while only 29% correctly responded to scenario 3 which dealt with the issue of sharing their password with their managers. This suggests that it is inappropriate to talk about policy compliance as if it is a single behaviour.

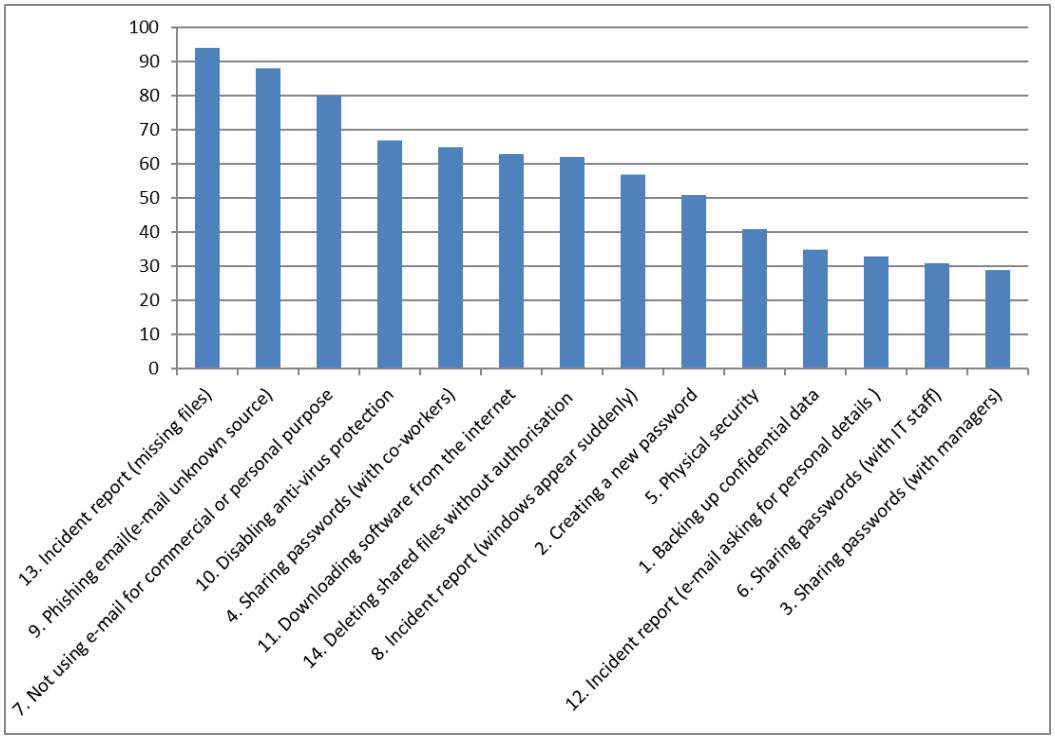


Figure 4.4: Result of employees' compliance with information security policies

4.3.2.1.1 Password management

Table 4.4 illustrates the circumstances in relation to employees sharing their passwords with other employees in different positions in their organisations. Sharing passwords is a particularly problematic area in this Omani data set and achieved the lowest score regarding security awareness, as can be seen from answers to scenarios 3, 4 and 6.

Table 4.4: Sharing password

Scenario No	Circumstances	Share password with	ISP-compliant response	%
3	When manager is extremely busy and needs to retrieve some files from employees' accounts.	Managers	Decline the order and remind their managers it is not allowed.	29
6	IT staff want to perform some troubleshooting.	IT Staff	Delete the email without replying to it.	31
4	When employees are on a day off their co-workers need to access an important email they have received in their email accounts.	Co-worker	Not provide co-workers with their password.	65

In scenario 3, only 29% of employees indicated they would decline their manager's order and remind him/her that password sharing is not allowed, while 71% of them would share their password with their managers if they requested it. The findings from scenario 6 reveal that only 31% of respondents would delete the email without replying to it. In contrast, 54% of employees would send their username and password through email if IT staff asked them to. In contrast, scenario 4 shows that 35% of employees are willing to share their username and password with their co-workers via the phone while they are off work in order to allow co-workers to access important emails. This highlights an important message effect, that is, the outcome is influenced by who asks employees to share their passwords. While happy to say no to co-workers, participants were less willing to refuse a request from someone in authority such as managers or IT staff.

- Creating a new password

Scenario 2 was about creating a new password and almost half of the respondents (49%) had difficulties in remembering new passwords when asked to create a new strong password.

4.3.2.1.2 Phishing and virus threats

Occasionally, employees receive suspicious emails which purport to come from people within their organisation, such as administrators, co-workers, IT staff and/or managers (hijacking emails) asking employees about their username and password, personal details and/or to click on a link or visit websites. Table 4.5 shows the scenarios with the highest number of policy-compliant responses. Scenario 13 has the highest correct response rate, revealing that 94% of employees would inform IT staff immediately they discover that files are missing or other changes to their computers. Most employees will report the incident because it may negatively impact their productivity or ability to get on with their work.

Table 4.5: Phishing and virus threats

Scenario No	Circumstances	ISP-compliant response	%
13	A number of files are missing from their computers and several changes have occurred.	Inform IT staff immediately.	94
9	Opened attachment email which unknown source.	Delete the email immediately without opening the attachment.	88
12	Employees want to use their email for their own commercial purposes.	Not use their accounts for personal or commercial purposes.	80
8	Applications windows start to move around on employees' computers and several new windows suddenly appear.	Disconnect their computer from the network and inform IT staff.	57
7	Personal details by logging in to a specific web link.	Phone the administrator to report the email.	33

It is interesting to compare scenario 13 and 7 which both require employees to report the situation to IT staff. However, in scenario 13, the harm has already been realised, and the employee is being reactive, whereas in scenario 7 the employee is potentially less sure if they have been phished and the effect is not immediate. Consequently, fewer employees are likely to report the incident and be proactive (i.e., put in effort to prevent future harm) and assist the administrator.

One of the highest correct actions is noted in scenario 9, where 88% of employees would delete a phishing email they received from an unknown source asking them to open an attached file. In scenario 12, a similar number of respondents (80%), would not use their work email account for personal or commercial purposes.

However, 48% employees would verify the source and click on the link if they think it is safe. Unfortunately, currently there are many hijacked email accounts and it is difficult for an individual to know if the source is reliable and, even if the source appears to be legitimate, it could be spoofed. In addition, personal details are extremely important; thus, if an unauthorised person obtains them, it may possibly result in harm or financial loss to an employee.

With regards to identifying employee level soft skill in recognising a computer infected with a virus, scenario 8 confirms that more than half of the workers (57%) would disconnect from the internet and inform IT staff of the incident. However, only 29% of them would make sure that the antivirus is on, which indicates that they do not have adequate skills to deal with these types of viruses, and moreover, that they rely on the settings of the computer.

4.3.2.1.3 Technical security with privileges

Table 4.6 shows how employees' ISP compliance intentions when they have elevated privileges on their workplace PC allowing them, for example, to disable antivirus software, or install software from the Internet.

Table 4.6: Technical security with privileges

Scenario No	Circumstances	ISP-compliant response	%
10	Employees want to disable antivirus software in their computers when they are very busy because they think it slows down their computers.	Not disable the antivirus software.	67
11	Employees urgently need to install free software that they have downloaded from the Internet for work purposes.	Ask a technician to install the software.	63
14	When the project is finished employees want to delete the files because they no longer require them.	Ask permission from all the colleagues they work with.	62

In scenario 10, 67% of respondents said they would not disable their antivirus when working on their computer, even when they are busy; however, this leaves the institutions vulnerable as a third of employees think that switching off the antivirus may speed up their computer, and they may be tempted to do this to improve productivity. Similarly, in scenario 11, 63% of employees would ask for permission to install software from the internet when there are urgent situations, whereas 26% of workers would install it without permission, once they had verified there was no virus. In scenario 14, 62% of employees would ask for permission to delete files

from organisations' hard disks when they finish a project. In contrast, 38% would delete the files in different circumstances, which is an unauthorised modification.

4.3.2.1.4 Backup

In scenario 1 only 35% of respondents would not send their confidential work file to personal email accounts for back up (e.g., Gmail), while 30% of them would. Furthermore, 31% would do this after asking their manager for permission. In addition, in scenario 14, 28% of employees would save their files to a USB as backup when they finished a group project and delete the files from the organisation's hard disk. While participants may believe they are supporting the university, these behaviours increase security risks continues by saving company data to personal or external devices.

4.3.2.1.5 Physical security

In scenario 5, 41% of respondents would lock-up the office or work area (doors, windows) and their computer screens when they leave their workplace for only a few minutes. In contrast, 30% believe that it is not their responsibility to lock up their offices or workplace. However only, 5% of employees would not lock their computer screens when there are co-workers in the office. Furthermore, 25% of employees would only lock their computer screen and not the office door if they leave the office for a few minutes. This shows that the risk from the physical environment is ignored by the more than half the staff.

4.3.2.2 Summary of employees' applied knowledge

In general, most employees would not intend to comply with some aspect of the organisations' information security policy or they are not aware of the security policy in their workplace. Only three of the fourteen scenario questions had correct response rates of 80% or more. It should be mentioned that on occasion hackers send emails to employees and pretend to be an administrator asking for employees' usernames and passwords. Even if the email appears to be from an administrator, employees should not send the information, for the reason that it is not permitted under any circumstances, as is written in organisations' information security policies. However, the results are surprising and indicate that 71% of employees would share this confidential information with their manager, whilst 35% would

share with co-workers. In addition, the results show that almost half of employees have a lack of motivation when they are requested to create new passwords.

It is important to point out that sending a password by phone or email via text or voice could expose the password to the public which is unacceptable behaviour. In the questionnaire, numerous employees indicated that they would share their password with their managers and administrators. In this case, managers and system administrators should not request login passwords from employees, under any circumstances. It is possible that the results observed here are due to Omani culture in which employees defer to their bosses.

4.3.3 Exploring human factors in information security

The principal aim of the study is to explore what factors affect compliance with ISPs. When positive and negative factors that influence employee behaviour are identified, this may assist an organisation to better understand how to motivate employees to comply with information security policy. The results showed that the overall employee information security awareness was approximately 57% across the 14 scenario questions.

Employees can be influenced by organisational and social factors that distract them from complying with an ISP. Employees are also affected by personal factors such as trust in co-workers and IT staff, authority, productivity, responsibility and curiosity. The following sections discuss the wrong answers chosen by participants. These wrong answers reflect different ways that people may be influenced to behave in a noncompliant way. The factors explored in the answer set are trust, authority, productivity, personal responsibility and curiosity.

4.3.3.1 Trust in co-workers and IT staff

Trust was the highest factor influencing employees to disregard complying with the ISP, as they think they are safe. For example, in scenario 7, 58% of employees would try to verify the source and clicking on the link, or click on the link to substantiate what is there, when they receive an email that appears to have been sent by an administrator asking them to visit a specific web link to confirm their personal details. Unfortunately, this is more than those who comply with the ISP

(33%). In addition, in scenario 1, 34% of employees trusted personal emails and co-workers to send confidential files; 30% of them would send their confidential files to commercial emails and 4% of them think it is alright to send confidential files to trusted co-workers. 35% of respondents gave the ISP-compliant answer.

Similarly, in scenario 6, 47% of employees would send their username and password via email if IT staff ask them to once they had ensured that the email is from IT staff. This is strictly against policy which does not allow username and password sharing and furthermore, is more than those who comply with the ISP (31%). These two cases reveal that employees believe that they are not doing anything wrong because they trust IT staff.

Trust, such as sharing important information for work purposes, can be developed between employees at the same organisation. This in group-trust is due to belonging to the same group organisation. In scenario 4, 65% of employees would refuse to give a co-worker their username and password but 35% were willing to share their username and password with co-workers via the phone because of trust while they are off work. Furthermore, scenario 3 showed that 17% of employees would give their username and password to their manager if they need to access confidential files. This is probably influenced by Omani culture in which trust in superiors is high.

4.3.3.2 Authority

The results show that employees would likely not adhere to the ISP if their managers ask them for their password or give them permission to do what they want, even if that action is incorrect. Instead, in scenario 3, the result indicates that 71% of employees would share their usernames and passwords with their managers in different circumstances, seeing as they believe that their managers have the authority to ask for and obtain them. 43% of employees would provide their managers with their password when the managers agreed to take responsibility for using employee passwords and 17% of them would perform the request if the files involved are not sensitive. This means that authority is followed more than ISP compliance (29%).

Furthermore, in scenario 1, 31% of employees would ignore the policy by asking for permission from their managers to send their confidential work files to a commercial email service, such as Gmail.

4.3.3.3 Productivity (work pressure)

Regarding the work environment, employees in scenarios 5, 10 and 11 are not willing to comply with information security when they are busy with work, seeing that they want to complete the work and complying with the ISP will be time consuming. In scenario 5, 25% of employees would only lock their computer screen and not the office door if they leave the office for a few minutes.

In scenario 10, 33% of employees would disable the antivirus on their computer for a short time when they have privileges on their computers or by asking the IT staff to do it. Similarly, in scenario 11, 37% of employees would install software downloaded from the internet when they administrative privileges on their computers, asking the IT staff to do or asking the technician for their username and password, in order to install it themselves.

4.3.3.4 Responsibility

In scenario 5, 30% of employees say they would lock their computer screens, although they believe that it is not their responsibility to lock up the office or work area (doors, windows) during the working day because they trust people in the organisation to close doors and windows and not to try to access their computers.

4.3.3.5 Curiosity

Most organisations recommend their employees do not open emails attachments if they are not sure about the source of the message, but unfortunately they are often curious to open the attachments anyway and are not concerned about who it is from (Madigan et al., 2004). Although source information may be unreliable (the email may appear to come from a reliable source), it is nevertheless an important signal that users sometimes disregard, even when they do not recognise the source. In the current findings, in scenario 6, when employees receive an email that appears to have come from the administrator asking for username and password to perform some troubleshooting, 15% would reply to the sender to ask who they are.

Furthermore, in scenario 7, 10% of employees would click on the link to verify what is in an email when they receive one that appears to have come from an administrator asking them to go to a specific web link to confirm their personal details. However, the link may have a virus.

4.3.3.6 Summary of human factors plausible distractors

Trust, authority, productivity, responsibility and curiosity drive respondents to non-compliance with information security policy, although they chose an incorrect action when they were under social, organisational and environmental conditions. Furthermore, work pressure may possibly force them to make a mistake and decrease their intention to comply with ISP. The results confirm that trust and authority appear to have a stronger influence than rules on non-compliance with information security policy.

4.4 Understanding factors of influence

In addition to the distractor (wrong) answers, eight questions were used to identify what participants believed influenced their ISP compliance and participants were asked to rate their level of agreement using a five point Likert scale from strongly agree to strongly disagree. The factors identified were: knowledge, response efficacy, subjective norms for organisation and/or manager, compliance, behavioural intentions, and sanctions and rewards. The purpose of this section is to understand whether participants' scoring high or low in compliance hold different beliefs about why they behave the way they do.

4.4.1 Study Analysis

For each of the fourteen scenarios discussed above, participants were asked to rate eight influencing factors. A 2 (high/low ISP compliance) × 14 (scenarios) × 8 (influencing factors) ANOVA was carried out to look at whether there were differences in the ratings of influencing factors for those with different overall levels of compliance across the different behaviour scenarios.

The 503 participants were grouped into two groups (high and low compliance). The higher group scored from 8 to14 (N = 270) questions correct (i.e., they chose the

policy compliant answer) and the low compliance group scored from 1 to 7 (N = 233), as shown in Table 4.7.

Table 4.7: Employee group scores

Participant's group	No. policy compliant answers	No. of participants
Participants scored high	8 to 14	270
Participant score low	1 to 7	233

The analysis of variance (ANOVA) test was designed to determine how the entire collection of group means is spread out and compares that to how much those means might be expected to vary if they were all sampled from the same population (that is, if there were no true differences between the groups). The result, given as the F ratio specifies the ratio of how much variability there is between the groups relative to how much there is within the groups. ANOVAs with repeated measures (within-subject factors) are particularly susceptible to the violation of the assumption of sphericity. Sphericity is the condition where the variances of the differences between all combinations of related groups (levels) are equal. Violation of sphericity (Mauchly's test) is when the variances of the differences between all combinations of related groups are not equal. The violation of sphericity is serious for the repeated measures ANOVA, with violation causing the test to become too liberal. If violations of sphericity do occur, corrections (Greenhouse-Geisser) are used to produce a more valid critical F-value.

4.4.2 Results: Influencing factors

A repeated measures ANOVA was carried out for eight factors across fourteen scenarios, with a between-subjects' variable of compliant answers (high or low). Mauchly's test indicates that the assumption of Sphericity had been violated. Sphericity occurs when the variances of the differences between all group combinations are equal. When the condition is violated Sphericity must be estimated. Therefore, the degrees of freedom was corrected using Greenhouse-Geisser estimates of Sphericity; $\varepsilon = 0.74$ for the main effect of scenarios, 0.505 for

the main effect of the factors and 0.547 for the interaction effect between scenarios and factors (see Table 4.8).

Table 4.8: Mauchly's Test of Sphericity

Within Subjects Effect	Mauchly's W	Approx. Chi-Square	df	Sig.	Epsilon[b]		
					Greenhouse-Geisser	Huynh-Feldt	Lower-bound
Scenarios	.153	931.608	90	.000	.741	.758	.077
Factors	.026	1811.006	27	.000	.505	.510	.143
Scenarios * Factors	.000	16953.248	4185	.000	.547	.610	.011

4.4.2.1 Main effect of compliance level

There was a significant difference (F (1, 501) = 14.20, p = 0.000) between the high (M= 4.165), and low (M=4.007) compliance score groups; however there was only a small effect size (r = 0.028). This suggests that those who score well and badly hold different beliefs about how their behaviour is influenced, however that actual difference between the scores is very small.

4.4.2.2 Main effect of scenario

The result of a repeated-measures ANOVA test with a Greenhouse-Geisser correction reveals that there is a significant main effect of scenario (F (9.633, 4826.04) = 56.86, p = 0.000) with small effect size (r = 0.102). Table 4.9 highlights the mean agreement rating across the factors for each scenario. Thus the level of agreement with the influencing factors was different for different behaviour scenarios.

Table 4.9: Means Factor scores for scenarios

S	1	2	3	4	5	6	7	8	9	10	11	12	13	14
M	3.86	3.92	3.84	4.03	4.07	4.12	4.13	4.07	4.21	4.14	4.15	4.20	4.25	4.16

*** Note:** Scenario=S; Mean=M.

4.4.2.3 Main effect of factors

The result of a repeated-measures ANOVA with a Greenhouse-Geisser correction corroborates that there is a significant main effect with regards to factor F (3.54, 1771.44) = 174.99, p = 0.000) with medium effect size (r = 0.259).

Table 4.10 provides the mean agreement level for each factor. Participants most strongly agreed that knowledge (M= 4.37), was the reason for their behaviour, while they were least likely to believe that there would be sanctions (M = 3.63) if they did not comply.

Table 4.10: Means for influencing factors

Factors	K	RE	SNO	SNM	C	BI	S	R
Mean	4.37	4.29	4.02	4.09	4.04	4.19	3.63	4.03

***Note: K:** Knowledge; **RE:** Response Efficacy; **SNO:** Subjective Norms Organisation; **SNM:** Subjective; Norms Manager; **C:** Compliance; **BI:** Behaviour Intention; **S:** Sanctions; **R:** Rewards

The pairwise comparisons illustrated in Table 4.11, show a significant difference between the two means of each factor, for the majority of influencing factors. This suggests that participants felt as if each factor had a different level of influence on their choice of answers.

Table 4.11: Difference between each two means of the influencing factors

Factors	K	RE	SNO	SNM	C	BI	S	R
K								
RE	.084*							
SNO	.358*	.274*						
SNM	283*	.198*	-.076*					
C	.329*	.245*	-.029	.047*				
BI	.188*	.104*	-.170*	-.094*	-.141*			
S	.744*	.660*	.386*	.461*	.415*	.556*		
R	.349*	264*	-.010	.066	.019	.160*	-.396*	

***Note: p**< 0.05; **Bold:** not significant**; K:** Knowledge; **RE:** Response Efficacy; **SNO:** Subjective Norms Organisation; **SNM:** Subjective Norms Manager; **C:** Compliance; **BI:** Behaviour Intention; **S:** Sanctions; **R:** Rewards**.**

4.4.2.4 Interaction Effects

The primary purpose of the repeated measures ANOVA is to explore the interaction effects between levels of compliance decisions, scenarios and

influencing factors. While a significant interaction was found between compliance level (low and high) and the scenarios (F (9.633, 6513) = 4826.04, p = 0.001) there was only a small size effect (r = 0.006) using Greenhouse-Geisser correction. Figure 4.5 illustrates how the mean agreement level for the influencing factors varied across the scenarios and between the two groups.

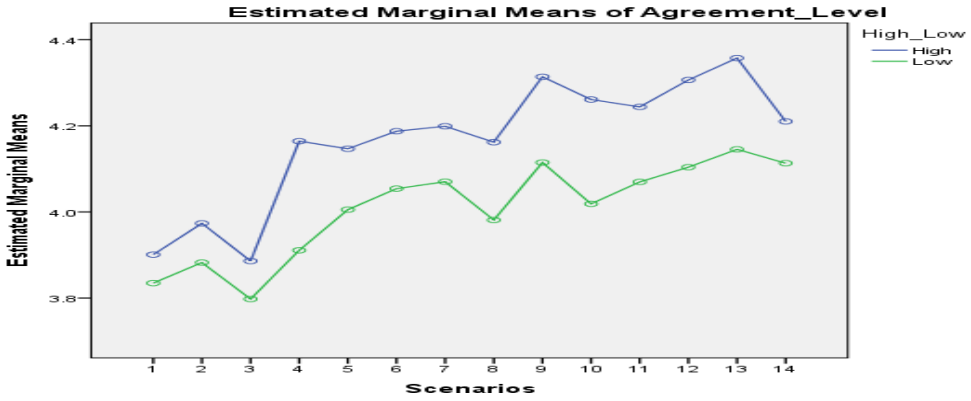


Figure 4.5: Interactions between scenarios and compliance score (high and low)

There was also a significant interaction effect between the influencing factors (mean across all the scenarios) and compliance score (F (3.536, 1771.44) = 5.069, p = 0.001) but again only with a small size effect (r = 0.010) using Greenhouse-Geisser correction.

Figure 4.6 illustrates the mean score for each influencing factor (across all scenarios). The pattern is generally the same for both groups (high and low compliance scores), however there are larger differences between some of the factors.

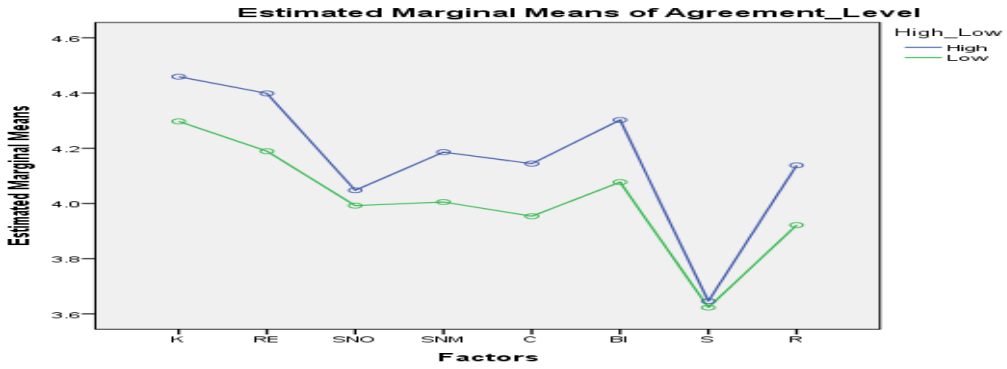
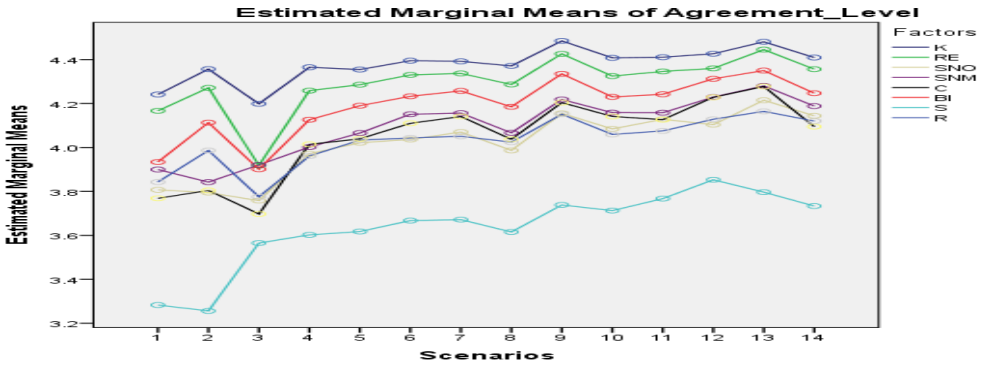


Figure 4.6: Interactions between factors and compliance score (high and low)

The result of the repeated-measures ANOVA with a Greenhouse-Geisser correction suggests that there is a statistically significant interaction effect between the scenarios and influencing factors (F (50, 24942.58) = 0.996, p = 0.000) with a small effect size (r = 0.019). Thus, this indicates that factors are rated differently depending on the individual scenario. However, it is clear from the graph the main effects are more compelling than the interaction effects. It is interesting to note that sanctions are consistently rated as the least influencing factor (see Figure 4.7).



***Note: K:** Knowledge; **RE:** Response Efficacy; **SNO:** Subjective Norms Organisation; **SNM:** Subjective Norms Manager; **C:** Compliance; **BI:** Behaviour Intention; **S:** Sanctions; **R:** Rewards

Figure 4.7: Interactions between scenarios and factors

There is no significant three-way interaction between compliance level, group factors and scenarios. The repeated-measures ANOVA with a Greenhouse-Geisser correction explains that there is no significant interaction effect between the high and low scores of both groups, in relation to the factors and scenario F (50, 24942.58) = 0.482 , p >0.05.

4.4.2.5 Further investigation of influencing factors by scenario

To more fully understand the relationship between the influencing factors and each individual scenarios a number of further analyses were conducted. Firstly, for each scenario a T-test was carried out to ascertain if there was a significant difference in ratings of influence factors between people who chose the compliant answer for that scenario, and those who did not. This analysis highlighted that different influencing factors were found to be significantly different in different scenarios.

This is summarised in Table 4.12. Those cells marked with "sig" highlight where a significant difference was found in the influencing factor rating between those who chose the compliant answer and those who did not.

Table 4.12: Influencing factors by scenario

Scenario	K	RE	SNO	SNM	C	BI	S	R
1		sig	sig		sig	sig		
2	sig	sig		sig	sig			
3	sig	sig	sig		sig	sig	sig	sig
4	sig	sig	sig	sig	sig	sig	sig	sig
5	sig	sig		sig	sig		sig	sig
6	sig	sig		sig	sig	sig		sig
7						sig		
8	sig	sig		sig		sig		sig
9	sig	sig	sig	sig	sig	sig		sig
10	sig	sig	sig	sig	sig	sig		sig
11	sig	sig		sig	sig	sig	sig	sig
12	sig	sig	sig	sig	sig	sig	sig	sig
13	sig	sig	sig	sig	sig	sig	sig	sig
14								
Total	11	12	7	10	11	11	6	10

***Note: K:** Knowledge; **RE:** Response Efficacy; **SNO:** Subjective Norms Organisation; **SNM:** Subjective Norms Manager; **C:** Compliance; **BI:** Behaviour Intention; **S:** Sanctions; **R:** Rewards

Following this, a step wise regression was undertaken for each scenario, the aim was to see which factors were useful in predicting if a person would choose the compliant answer or not. Those factors that were significant in predicting the scenarios are presented in Table 4.13 . This highlights that the predictive factors vary by scenario, with response efficacy (belief that the behaviour will keep information secure) being the most frequent factor across the scenarios. Interestingly from this knowledge and sanctions are only part of a significant regression on one occasion and rewards are never part of the significant regression equation.

Table 4.13: Regression analyses for individual scenarios

	Influencing factors														
	K		RE		SNO		SNM		C		BI		S		R^2
	B	SE	B	SE	B	SE	B	SE	B	SE	B	SE	B	SE	
S1			.07*	.03	-.12**	.03					.08**	.03			0.05
S2					-.12**	.03	.15**	.04	.08*	.04					.09
S3			.14**	.03	-.06*	.03	-.07*	.03	.13**	.03					.19
S4	-.12**	.04	.18**	.04	-.07*	.03			.11**	.03	.13**	.04			.22
S5			.16**	.04	-.08*	.03			.15**	.04	-.10*	.04			.08
S6			.11*	.04	-.07*	.03					.13**	.04	-.06*	.02	.08
S7											.04*	.02			.01
S8			.16**	.04	-.12**	.04	.17**	.05	-.09*	.04					.08
S9			.13**	.03											.06
S10			.20**	.03											.07
S11			.18**	.04	-.12**	.03			.14**	.04					.11
S12			.12**	.04					.07*	.03					.08
S13			.12**	.02											.10

***Notes:** **a) K:** Knowledge; **RE:** Response Efficacy; **SNO:** Subjective Norms Organisation; **SNM:** Subjective Norms Manager; **C:** Compliance; **BI:** Behaviour Intention; **S:** Sanctions
b) *P<.05; **P<.005
c) Scenario 14 had no significant predictors; and Influencing **factor 8** was never a significant predictor

A regression was also ran for the dependent variable of total correct answers for the average score of each influencing factor (see Table 4.14).

Table 4.14: Regression analysis for average factor scores as a predictor of total questions correct

	Influencing factor														
	K		RE		SNO		SNM		C		BI		S		R^2
	B	SE	B	SE	B	SE	B	SE	B	SE	B	SE	B	SE	
No. Scenario	1	2	3	4	5	6	7	8	9	10	11	12	13	14	
All Scenario Average			.14**	.05	-.10**	.02									.17

***Notes:** **a) K:** Knowledge; **RE:** Response Efficacy; **SNO:** Subjective Norms Organisation; **SNM**: Subjective Norms Manager; **C:** Compliance; **BI:** Behaviour Intention; **S:** Sanctions.
b) *P<.05; **P<.005
c) Scenario 14 had no significant predictors; and Influencing factor 8 was never a significant predictor

4.5 Summary of compliance influence beliefs

The aim of this section was to evaluate if participants who scored well and badly differed in their beliefs about the influence of knowledge, response efficacy, subjective norms for organisation and/or manager, compliance, behavioural intentions, and sanctions and rewards on their behavioural intentions to comply with organisational information security policy.

This section has presented a number of analyses in order to determine the factors that have the most influence on employees' compliance with ISP. The findings indicate that knowledge is the factor which employees believe is the reason for their choice of answer, while sanctions are thought to have the least influence.

4.6 Summary of the chapter

This chapter presented findings from a study of 503 employees in different institutions in the higher education sector in Oman in order to identify employees' awareness and the factors they believe influence their behaviour. The questionnaires were divided into three sections: general questions, security questions and questions on influencing factors. Overall, 57% of participant answers were in line with policy. This means that approximately half of the time non-policy-compliant decisions were being selected as acceptable responses with regards to security behaviour. However, compliance level was not consistent

across all scenarios. For example, in scenarios 9, 12 and 13 high levels of compliant decisions were made, whereas other scenarios had very low levels.

The results from the fourteen scenarios show that trust, authority, productivity, responsibility and curiosity are main influencing factors that prevent employees from complying with the ISP. The most influential factors are authority and trust (for example, more than two-thirds of employees would give their usernames and passwords to their managers and IT staff).

The findings also confirm that participants believe that their behaviour is influenced differently by the eight factors investigated and their agreement that their behaviour was influenced by each factor varied across the scenarios. Knowledge is perceived to have the highest effect on employees' intention to comply with an organisation's ISP, whereas the presence of sanctions is perceived to have the lowest effect. The employee findings confirm the perceptions of the IT staff and system administrators reported in chapter 3, that knowledge is the most important for employees' compliance with ISP and that because sanction systems were not present in these organisations the employees did not perceive sanctions to have a strong effect. In addition, this highlights the importance of not thinking of information security policy compliance as a single behaviour. Each behaviour (as illustrated by a scenario) needs to be considered individually for factors that influence it.

Given that for each behaviour, different numbers of staff intended to comply it is important to understand how important the behaviours, where more staff do not intend to comply, are to IT staff. The following chapter presents a study which presented the scenarios to IT staff and asked them to rank their importance. The same questionnaires that were used with the employees were given to the IT staff to draw out what behaviours (including non-policy-compliant ones) the people responsible for IT security considered to be acceptable in their own organisations. In addition, interviews were carried out to explore the reasoning underpinning the IT staff and system administrators' views and their thoughts about why employees might behave in non-compliant ways.

Chapter 5: REVISITING IT STAFF AND SYSTEM ADMINISTRATORS' PRIORITISATION OF POLICY BEHAVIOURS

5.1 Introduction

In the previous chapter, 14 behaviours were examined and it was found that more staff had intentions to comply with some behaviours and less with others. Given that some behaviours are less likely, it is important to understand a) how IT staff prioritise the 14 different behaviours and b) to find out whether IT staff condone the non-compliant behaviours. This chapter presents a study of 17 IT staff and system administration staff views of employee behaviour intentions and the importance they place on each behaviour. First, the study utilised the same scenario questionnaires presented to university staff in the previous study, and IT staff were asked to first identify the policy compliant answer then rank by level of importance for each scenario behaviour. In addition, participants were asked to select all the accepted behaviours in their organisations for each scenario or provide any alternative behaviour which would be acceptable. This would help to identify other acceptable behaviour which is not in the organisational ISP. This would suggest acceptance of some shadow security behaviours (Kirlappos et al., 2014), i.e., behaviours that have become accepted within the organisation but are not formally written into the ISP.

This was followed up by a second stage which used semi-structured interviews to explore in more depth information, IT staff perception of the employees' behaviour, intentions. In addition, the interviews aimed to identify barriers and motivations that technical staff believe influence employees' compliance with their organisations' information security policies.

As shown in Figure 5.1, the results are presented in six main sections: ranking important employees' behaviour, acceptable and unacceptable employee behaviour; information security incidents and reports; factors which affect compliance with the ISP; barriers to compliance with the ISP; and recommendation for successful information security management and increased employees awareness. Finally, the

17 IT staff and system administrators' importance ranking was compared with results of the survey of 503 employees in Chapter 4.

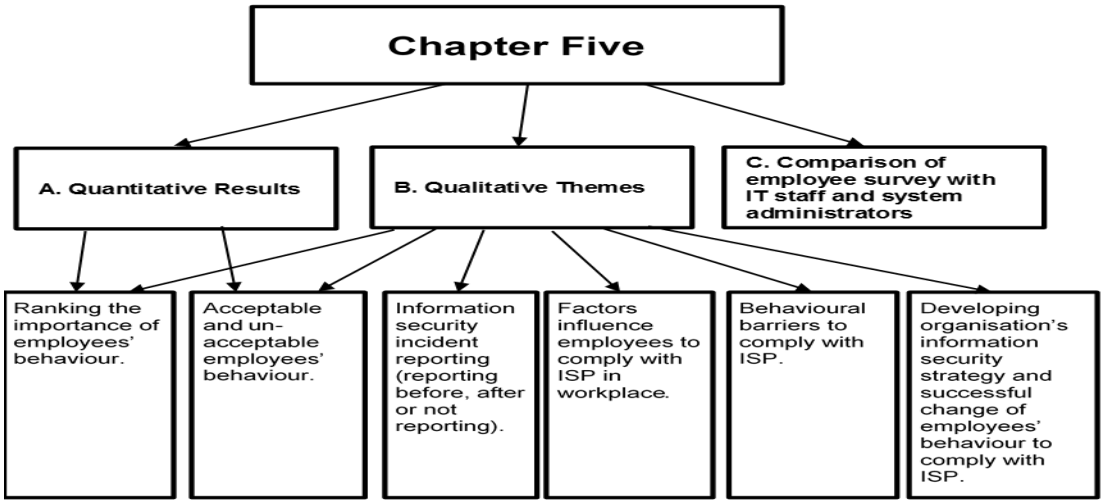


Figure 5.1: Structure of chapter five

5.2 Methodology

After receiving ethical approval from Northumbria University, 17 IT staff and system administrators agreed to take part and were given the same 14 scenarios as employees were given in Chapter 4 (four multiple choice) and interviewed using a one-to-one, face-to-face method.

5.2.1 Participants

17 participants from five higher education institutions took part in this study (see Table 5.1). Three of the participants from two organisations (A [1], and C [2]) also participated in the first study (Chapter 3). Therefore, participants were numbered from 1 to 17 in the second interviews. Organisation E was added because of the large number of participants in the survey study from this organisation (Chapter 4).

Table 5.1: Organisations and participants

No	Organisation	Number of Participants
1	A (Large size, university)	4
2	B (medium size, university)	1

3	C (medium size college)	6
4	D (small size college)	1
5	E (Large size college)	5
Total	5	17

All the participants had a university degree and at least three years' work experience. Of the 17 participants, six were Omani and the others were originally from other countries. These individuals are the persons responsible for network and information security in their respective offices or colleges and for that reason, so it was important to obtain detailed information from them.

5.2.2 Procedures for data collections and analysis

For this study, both quantitative and qualitative data were gathered via a questionnaire which used both open and closed questions. The questionnaire was administered first followed by the one-to-one interviews. The questionnaire was divided into two parts, employee behaviours in order of importance (see Appendix C) and highlighted the acceptable behaviours from each scenario. The qualitative aspect was administrated via a one-to-one, face-to-face session with the researcher. The interview procedure was the same as in the first study (Chapter 3) except that participants were allowed to hold the interview in either English or Arabic depending on their preference. The interviews were recorded and transcribed. The questionnaire and interview portions of the study were structured into steps and each step was divided into several sub-steps as below.

I. Quantitative method:
    a. Each participant was asked to order the employee behaviour scenarios from most important (1) to least important (14). This time the scenario was presented with the ISP compliant behaviour included in the description and participants were asked to rank these employees' behaviours in order of importance to the security of their organisation. The rankings for the employee scenarios were then totalled. This provided a ranked order of importance of employee behaviour. The purpose of this ranking was to find out which scenario behaviours are given top priority by IT staff and whether the ranking is consistent

across different staff. The ranking of security behaviours may help an organisation to focus on its priority areas to improve staff behaviour.

b. Next, IT staff were asked to provide all answers that they would find acceptable for each of the 14 scenarios thereby highlighting whether they would accept non-policy-compliant behaviour. In addition, they were allowed to supply free-form text answers if they wanted to add alternative acceptable behaviours. The data were collected individually face-to-face. This provided scores for ISP compliance and for non-compliant options that they find acceptable.

II. Qualitative method:

a. After the quantitative task, participants were then asked to provide the reasons for their rankings and to explain how they had chosen their top five (most important) and bottom five (least important) behaviours.

b. Participants were asked if employees reported information security incidents. Furthermore, the participants were asked what factors (knowledge, managers, co-workers, sanctions and rewards) they think influence employees to comply with ISP in their organisations and, where possible, to give examples from their own experience. This study identifies the barriers that IT staff believe influence whether employees comply with an ISP.

c. Finally, participants were asked to rank the factors that they believe affect employee compliance intention in order of importance. These factors were rewards, sanctions, awareness, knowledge, and managers. This aspect allowed differences to be identified between staff about how to influence intentions and recommendations to be made that could help organisations to deal with these barriers in an appropriate way in order to improve organisations' information security management and employee security behaviour.

A framework analysis was used for the open answers to the questions (Ritchie et al., 1994). Framework analysis was chosen for the analysis of the semi-structured

interview data because it is better suited to research that has structured questions (Srivastava & Thomson, 2009).

5.3 Results

The 17 participants were from different countries, organisations and positions and gave different views on some points and similar views on others into their organisations' information security management.

5.3.1 Ranking the importance of employees' behaviour:

Kruger and Kearney (2008) found that asking decision makers to rank security issues according to perceived importance led to "a better understanding of the relevance and importance of those factors influencing an ICT security awareness program" (p. 259). In this study all participants ranked employee behaviours in order of importance (Table 5.2) from most important (1) to least important (14). This provided a total importance score used to rank the policy behaviours.

Table 5.2: Ranking the scenarios' behaviours in order of importance to security

Ranking the importance	Employee behaviours in the 14 scenarios
1st	7. Incident report (email asking for personal details)
2nd	13. Incident report (missing files)
3rd*	9. Phishing email(email unknown source)
3rd*	4. Sharing passwords (with co-workers)
4th	6. Sharing passwords (with IT staff)
5th	2. Creating a new password
6th	8. Incident report (windows appear suddenly)
7th	3. Sharing passwords (with managers)
8th	14. Deleting shared files without authorisation
9th	10. Disabling antivirus protection
10th	5. Physical security
11th	12. Not using email for commercial or personal purpose
12th	11.Downloading software from the internet
13th	1. Backing up confidential data

***Note:** scenarios number 9 and 4 are same ranking level (3rd)

5.3.2 Reasons for ranking

After participants ranked the policy behaviours they were asked for the main reason behind their ranking. Some participants reported behaviours to be important because those behaviours are frequently required in their organisations, as one participant said:

> *These are most important because these scenarios regularly happen in the workplace [P13]*.

Note, none of the participants were willing or able to divulge numbers of incidents that had occurred, either because they do not keep logs or because they felt such information was too sensitive to share. Another key issue was whether or not the behaviour would compromise the organisation's assets as two participants pointed out that:

> *More important is the confidential assets and we are responsible [P8]*.

> *My selections depend on whether the wrong behaviour leads to access to the confidential data directly [P15]*.

Another participant suggested that computer access and network policies should be secured first (such as privileges to download and install software, disable antivirus and policies around creating strong passwords):

> *For me one of the most important is the system security so system should come first then files then emails [P4]*.

5.3.3 Specifying the five most important scenarios

The scenario ranked most important was one concerned with receiving and sending emails between users and outsiders (see Table 5.3). 11 participants ranked scenario 7 (email communication) as the most important policy behaviour because most employees continued to repeat the same mistake and were putting the organisation's information at risk.

Table 5.3: The five most important scenarios

Security behaviour rank	Scenario description
1st	7. Said has received an email that appears to have come from an administrator asking him to go to a specific web link to confirm his personal details. He phones the administrator to report the email as it may be a phish.
2nd	13. Bakhit has discovered that some files are missing from his computer and some changes have happened to his computer. He informs IT staff immediately.
3rd	9. Badr receives an email with an attachment from an unknown source. The email says that the attachment should be opened which will get rid of the virus. He deletes the email immediately without opening the attachment.
3rd	4. Ali is having a day off and refuses to give his co-worker his password in order to access an important email he has received.
4th	6. Khalfan received an email that appears to have come from administrator asking him for his username and password as the IT staff want to perform some troubleshooting. He deletes it.

Interview question: Why did you choose those behaviours as your five most important ones, and how did you choose which five behaviours were your least important?

11 participants believed that emails are an easy way to trick users. As emails are the most common communication in the workplace, employees can get a lot of spam and phishing emails and viruses. The 11 participants ranked policy behaviours related to sending confidential data through emails as most important. As one participant said:

> *I think most of it is concern on getting information from employees coming from other resources which are unknown. We [organisation] are getting attack from outside or spam emails coming because of those staff give this information [P2].*

In addition, another reason for ranking scenario 7 as the most important is that IT staff at any organisation are very important and should have knowledge of how to behave in a secure manner. One participant said:

> *Related to information security, first administrators should know what they are doing then client side [P7].*

The second highest ranked scenario concerned employees informing an administrator if files were missing from their computers. For example, one participant said:

> *The second scenario about missing files that if any users have missed his files from his computer they have to inform the technical support if someone access to his computer by different account [P16].*

The third highest ranked scenario was to do with sharing passwords and receiving emails with attachments from an unknown source. Regarding unknown email sources one participant said:

> *Because these [emails] are coming from outside and unknown email could bring viruses and asking for personal details and the password [P17].*

Regarding password sharing, one participant said:

> *User has given his username and password to one of his trusted office colleague and maybe they deleted some files by mistakes, security is very concerned that you should not share your password to anybody [P3].*

In addition, because of the consequences of sharing usernames and passwords, the participants ranked sharing password again as the fourth most important.

> *Because of 1 to 5 (important scenarios) always related to the username and password of users. If someone took it will get all your personal data [P8].*

5.3.4 Specifying the five least important employee behaviours

Table 5.4 presents the scenarios that were ranked as least important to the security of the organisation.

Table 5.4: The five least important scenarios

Security behaviour rank	Scenario description
10th	10. Ahmed is very busy and has a lot of work to do. He doesn't disable the antivirus software even though he thinks it slows down his computer.
11th	5. Sami works in his own office, and makes sure he locks the door, windows, and his computer's screen takes time even if he leaves the office for a few minutes.
12th	12. Noor never uses her work email for her own commercial purposes.
13th	11. Hasan urgently needs to install some free software that he has downloaded from the Internet for work purposes. He waits until the technician has time to check this for him.
14th	1. Adam wants to back up a confidential file. He does not email it to his Gmail account.

Participants had different views regarding the least important policy behaviours. As one of the participants said:

> *Based on the scenario on backing up confidential data there are a lot of ways to save data not only sending to the Gmail account especially if you are the owner of that data first save in your computer second in your own flash drive or CD and file server but it should be there passwords [P1].*

One reason for the lower ranking is that this behaviour was believed to happen less frequently in the organisation:

> *It happened less or it is not behaviour of our colleagues in our college [P6]*

Using an organisation's email servers for commercial purposes was not seen as directly impacting information security. For example, one participant said:

> *I have ranked these at the bottom because these behaviours are not connected to data directly like if someone uses his email for commercial purposes but might effect the work performance [P15].*

Some answers are ranked low because employees do not have privileges to disable the antivirus in the organisation network, and so it was perceived as not important. As one participant said:

> *Now in the university we do not give the users privileges to disable or remove the antivirus. [P15].*

5.3.5 Summary of ranking importance of employees' behaviour

The results show that the reasons for ranking scenarios differently were related to these being frequently occurring problems with a high perceived risk. Behaviours ranked low were those perceived as not being possible in an organisation or not directly relevant to security.

The findings identified that the most important security compliance behaviours, in the opinion of the IT staff and system managers, were that employees should inform IT staff if there are any information security incidents such as emails asking for their personal data or password even it purported to come from IT staff, missing files from their computers, receiving email from unknown sources, and not sharing passwords with IT staff and/or co-workers. In comparison, Kruger and Kearney (2008) report six information security awareness areas that senior decision-maker ordered by importance. In this study they were ordered as most important 1st was keep passwords and personal identification numbers (PINs) secret, 2nd adhere to company policies, 3rd use e-mail and the Internet with care, 4th report incidences like viruses, 5th be careful when using mobile equipment, and 6th be aware that all actions have consequences.

The rankings found in this study would be helpful for information security management in organisations to focus more on those behaviours at the highest level importance to reduce employees' mistakes.

5.4 What employees do and IT staff and system administrators find acceptable and unacceptable security behaviours?

IT staff were asked to provide acceptable answers for each of the scenarios thus highlighting whether they would accept non-policy-compliant behaviour (they were

also allowed to add other acceptable alternative behaviours with free-form text). The overall findings reveal that IT staff and system administrators had a mean ISP-compliance score of 81% as measured by what behaviours they deemed to be acceptable.

Figure 5.2 shows that all IT staff and system administrators have different scores depending on different aspects of information system security in the 14 scenarios. Comparing the answers, they judged to be acceptable with the ISP-correct answers, 100% of staff chose the policy compliant answer in scenarios 11, 12 and 13 which concerned incident reporting, downloading software from the internet and not using email for commercial or personal purposes respectively. On the other hand, only 53% of staff chose the compliant answer for creating new passwords and 59% for not sharing passwords with IT staff. Although more IT staff chose policy compliant answers than other employees, it is clear that even IT staff are willing to accept some non-policy-compliant behaviour.

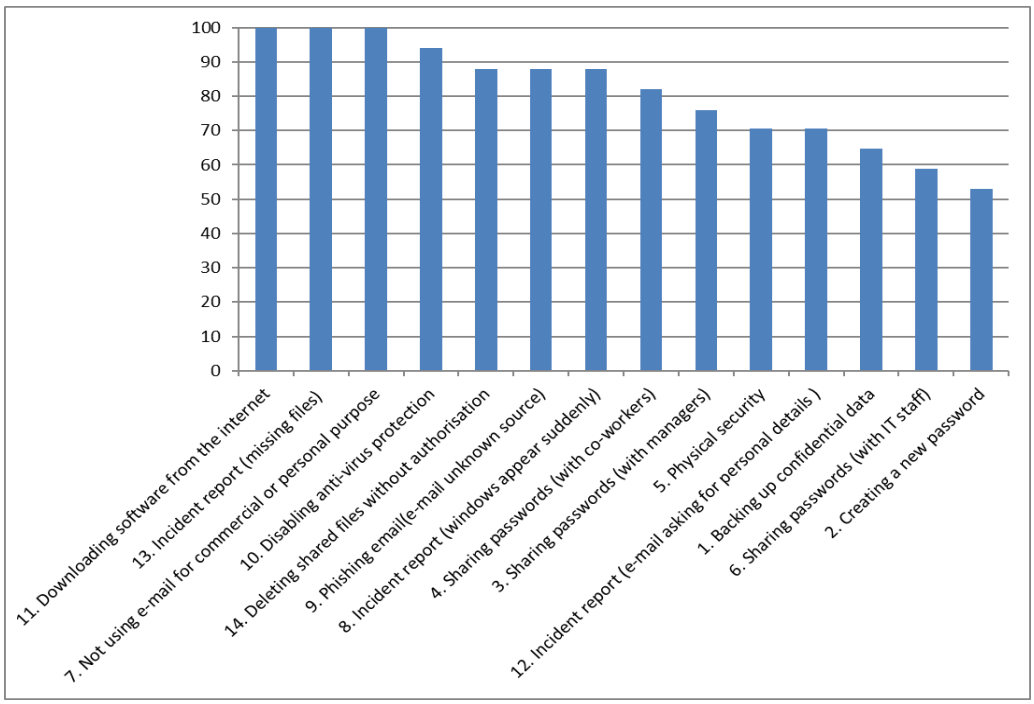


Figure 5.2: % IT staff and system administrators' choosing information-security-policy-compliant answers

IT staff and system administrators were asked to select as many options as they would find acceptable for each of the 14 behaviour scenarios. In addition, they were asked to list any other alternative acceptable employee behaviours in their organisation or behaviours they deemed to be unacceptable.

5.4.1.1 Passwords management

A number of scenarios dealt with the issue of password management. Table 5.5 highlights the percentage of IT staff compliance with the ISP on these sharing passwords.

Table 5.5: Compliance around sharing passwords

Scenario	Circumstances	Share password with	ISP-compliant behaviour	%
4	When employees are having a day off their co-workers need to access an important email they have received in their email accounts.	Co-worker	Not give co-workers their password	82
3	When manager is very busy and need to retrieve some files for employees' accounts.	Managers	Decline the order and remind their managers that is not allowed.	76
6	The IT staff want to perform some troubleshooting.	IT Staff	Delete the email without replying to it	59

For scenario 6, ten respondents indicated intention to follow the information security policy by expecting employees to delete the email without replying to it. However, IT staff were also willing to accept non-compliant behaviour; four accepted their employees checking the email's source and, if it appears to be valid, sending the information. In addition, three of them accepted employees asking who the sender was by sending an email and only one participant thought that employees should do what the IT staff had requested. A further two participants suggested that employees should inform IT staff about this email, and the same

number suggested that they should not give their email to any one and just one participant suggested that they should mark the email as junk and block the sender.

In scenario 3, four IT staff accepted employees could give their password to their managers when managers ask. On the other hand, 13 IT staff indicated they would decline the order and remind their managers that is not allowed.

In scenario 4, 14 IT staff were against sharing passwords between employees in the workplace when they were on holiday. However, two of them agreed that employees could give their passwords to their co-workers because their co-workers are trustworthy, with a further participant agreeing that employees could give their passwords to their co-workers to access to their email account if does not contain sensitive information. Three participants suggested in the free-form text that employees should send an email to their co-workers but not the password and one of them suggested that when employees ask for their password they should ask the manager first.

- Creating a new password

The lowest scores for policy compliance were in scenario 2 where only nine IT staff chose the policy-compliant answer (insisting that employees remember new passwords without writing them down, saving them in a mobile phone or telling anyone). Surprisingly, ten accepted that employees could use a password they have for another service but change one of the characters in it. In addition, four of them accepted that it could be saved in their mobile phone or computer and three of them accepted that employees could write it on paper and put it in their drawer until they remember it. One participant suggested that employees could write their passwords down then keep them in a safe place. In addition, two respondents gave further suggestions: One suggested that employees should remember their password because their organisation should have a system in which when employees forget their passwords they would be given a new one. The other participant added a suggestion of rules for employees to remember their password easily, such as combinations of initials and any digits from their mobile number or date of birth.

5.4.1.2 Phishing and virus threats:

The results show that all participants chose policy-compliant answers for scenarios 12 and 13 which concerned email usage and missing files from employees' computers respectively (see Table 5.6). Similarly, in scenarios 8 and 9 which concerned viruses and receiving email from unknown sources, fifteen of them gave policy-compliant answers. The worst response rate in this group was scenario 7 which showed that only twelve agreed that employees should follow the information security policy regarding personal details.

Table 5.6: Phishing and virus threats

Scenario	Circumstance	ISP-compliant behaviour	%
12	Employees want to use their work email for their own commercial purposes.	Not use their accounts for personal or commercial purposes.	100
13	Some files are missing from their computers and some changes have happened.	Inform the IT staff immediately.	100
8	Application windows start to move around on employees' computers and many new windows suddenly appear	Disconnect their computer from the network and inform the IT staff.	88
9	Opened attachment email which will get rid of the virus.	Delete the email immediately without opening the attachment.	88
7	Personal details by login to specific web link.	Phone the administrator to report the email.	70

In scenario 12, all IT staff believed that employees' organisation email accounts are not for personal or commercial purposes. However, four participants accepted that employees could reply to their customers if they have personal businesses, but they should not sell products through their university email account. In addition, one participant accepted that employees could use their organisation's email account just for people they trust and one participant accepted that employees could use the organisation's email account for business purposes if they did not attach any files. The results show that in scenario 13 all participants suggested that when

employees' files are missing from their computers and some changes have happened they should inform the IT staff immediately. However, two participants would accept employees not reporting missing files if the information they contained was not important.

For scenario 8, 15 IT staff first accepted the policy-compliant behaviour of disconnecting their computer from the network and informing the IT staff when their application windows start to move around. However, they also agreed that employees should make sure that the antivirus software is on even though they are already infected. Eight IT staff accepted employees should log out of their account. In addition, four suggested that employees should call their co-workers over so they can witness what is happening. Two participants added a suggestion that employees should inform the help desk.

15 participants in scenario 9 accepted the policy-compliant behaviour of deleting the email immediately without opening an attachment when it comes from an unknown source. However, one participant agreed that employees could reply to the sender and ask who they are and another participant believed that employees could forward the email to a co-worker and ask him what to do. In the suggestions and comments, three IT staff would advise their employees to inform IT staff about this case.

In scenario 7, 12 IT staff accepted employees telephoning the administrator to report receiving an email asking for username and password which appears to have come from an administrator. In addition, ten respondents accepted employees deleting the email. By contrast, three IT staff accepted employees checking the email's source and, if correct, clicking on the link, and two of them agreed that they should click on the link to check what is there which could release a virus.

5.4.1.3 Technical security with privileges

In this set of scenarios dealing with technical security for employees with elevated computer privileges a higher proportion of IT staff chose the security compliant behaviour (see Table 5.7).

Table 5.7: Technical security with privileges

Scenario	Circumstance	ISP-compliant behaviour	%
11	Employees urgently need to install some free software that they have downloaded from the Internet for work purposes.	Ask a technician to install the software	100
10	Employees want to disable the antivirus software in their computers when they are very busy and have a lot of work to do because they thinks it slows down their computers.	Not disable the antivirus software	94
14	When the project is finished employees want to delete the files because they no longer need them.	Ask permission from all the colleagues they work with.	88

For scenario 11, all 17 participants suggested that employees should ask IT administration to install the software to be on the safe side. In addition to policy compliant behaviour, four IT staff accepted that employees could install software from the internet by themselves, but they would have to make sure it had no virus. Furthermore, four agreed that employees could ask for a technician's username and password to install the software by themselves and two of them agreed that employees should install the software immediately if they can.

For scenario 10, 16 participants did not agree with employees disabling the antivirus software on their computers when they are very busy. However, two participants suggested that employees could ask the IT staff to disable the antivirus software for a short time and another one thought that employees should ask the IT staff to give them administrator privileges to save time.

In scenario 14, 15 participants gave ISP-compliant responses, insisting that employees should ask permission from all the colleagues they work with on a project before deleting files upon project completion. 12 participants accepted that employees could delete the files but make sure they save copies onto their USB memory stick first even though they could lose the USBs or unwanted people could get them which creates a security risk. In addition, five IT staff would accept their employees deleting unimportant files and two of them agreed that employees can

go ahead and delete the files they have access to. Only one participant noted that the shared files do not belong to just one person to do whatever he/she wants because the files are owned by many people at the workplace.

5.4.1.4 Backup confidential data

In scenario 1, 11 (65%) of the participants, which was the third lowest score, agreed that employees should not send their confidential work files to third-party sites (e.g., Gmail), yet 9 of them were willing accept that their employees send confidential data to a Gmail account when they got permission from their managers. Five of them thought sending confidential files to a personal Gmail account in order to have more copies was acceptable and three thought it was acceptable to do this in order to send files to trusted colleagues.

Six participants in the free-form text section added that it would also be acceptable for employees to send the email but should have password protection (two participants), save it in their organisation's internal backup services (two participants), or save it on a flash drive and/or DVD (two participants).

5.4.1.5 Physical security

In scenario 5, a number of participants would accept non-compliant behaviour. Eight participants found it acceptable to lock their computer's screen but not the office or work area (doors, windows). In addition, six participants accepted employees leaving their offices for a few minutes and not locking the door just their computer's screen. Moreover, four IT staff accepted employees not locking their computer screen if their colleagues are in the office.

5.4.2 Summary of acceptable and unacceptable employees' behaviour

IT staff were asked to select acceptable and unacceptable behaviours for each scenario not only to identify the level of policy compliance with the information security policy, but also to highlight other acceptable employee behaviours. Acceptable means that IT staff allow employees to behave in a way that is not fully compliant with the organisation's ISP.

The findings show that IT staff and system administrators did not all know the compliant behaviour for the 14 scenarios. The highest percentage would look for policy compliance for incident reporting (missing files), and the least for creating new passwords and not sharing passwords with IT staff (10). This means that not all IT staff and system administrators have good knowledge when it comes to information security behaviour. Furthermore, they accept some alternative behaviours, a phenomenon Kirlappos et al. (2014) have called shadow security, or non-official policy.

For example, nine of them would accept employees sharing their password with their managers if the manager agreed to take responsibility and to send confidential data to commercial email servers when they get permission from their managers. Ten of them would accept employees changing one of their password's characters in order to create a new password for another service. These proportions are not small, and all organisations should make sure that all IT staff and system administrators understand and follow the information security policy properly and not just focus on their end users because the IT staff and system administrators make decisions related to information security management. In depth interviews with IT staff and system administrators were needed to explore the main threats to information security, their perspectives on organisational information security management and behavioural factors affecting employees' information security behaviour. Section 3.5 and 3.6 are also extended to highlight the need for a comparison between IT beliefs and actual intentions, to establish whether those responsible for policy (IT staff) understand the effectiveness of that policy.

5.5 Qualitative data analysis of IT staff and system administrators' views on organisational information security management and behavioural factors affecting employees' information security behaviour

This section highlights four separate aspects of employee behaviour: types of information security incident and employees' reporting, factors influencing employees to comply with an ISP, barriers to compliance with policies. Finally, recommendations are made regarding the development of an organisation's information security strategy and to successful change employees' behaviour to comply with information security policy.

5.5.1 IT staff and system administrators' views on employees' behaviours in information security

All IT staff and system administrators agreed that human behaviour is very important in making an organisation secure. As one participant said:

> *The system will become more secure if the behaviour of human will be applied meaning if that staff will follow strictly the security policies [P4].*

Participants were asked to identify the main vulnerabilities that caused security breaches in their organisations, they believed that most security breaches happened in their organisation because of their employees' behaviour not because of technologies and they were encouraged to train them to avoid such behaviours. One participant put it this way:

> *If there are any breaches it is by human not the machine itself so humans they should be trained for the security thing [P10].*

All participants agreed that lack of awareness and knowledge in information security leads to security breaches, as expressed by participant:

> *The employees are still not aware regarding to information security ... Many breaches happened because users do not have knowledge about information security [P12].*

This is in line with our earlier findings in Chapter 3 in which the majority of IT and administration staff stated that the main problems of information security are a result of their users' behaviours.

5.5.2 Types of information security incidents and employees reporting behaviour

The participants identified that incidents happened in their organisations because of their users and there are different ways to cause incidents. In addition, they were unclear whether employees know how, when and to whom they should report an incident.

5.5.2.1 Types of information security incidents

The participants declared that there are many information security incidents that occur as a result of employee behaviour, especially via emails when they click on links, open attached files or open spam emails that have viruses. Email incidents are the most prevalent:

> *Email is very common communication which is widely available and one person has more than one email address and they [employees] can get a lot of spam claiming that to get information [P3].*

Sending important information such as usernames and passwords to phishing emails was common according to the participants who acknowledged that employees' behaviour caused problems:

> *Some of the employees are writing their passwords. Sometimes they are using their colleague's mail to register in some phishing websites this is affecting mail server they receiving a lot of spams because of this [P6].*

Users created incidents through their personal devices, such as their laptops, when they are authorised to disable their computer antivirus software:

> *If some staff may feel that antivirus blocking something and they could disable that but in the domain level they cannot because it centralised but they are disabling it on their laptop which is not good [P11].*

> *The last incident we have faced last semester that one employee installed software from the internet and that software sends packets to breach our network ... but we found that he installed it through his laptop which is out of our domain network [P12].*

5.5.2.2 Employees' reporting security incidents

Participants indicated the types of security incidents reported by employees and reflected on the compliance intentions and awareness levels this reporting represented. Users have an important role to play in reporting a possible security incident before any major consequences of an incident occur. It is important for an organisation to make their employees feel responsible for security and be willing to

report information security incidents. This requires that the employees are not fearful of blame for mistakes.

Three participants agreed that employees do not report information security incidents and 12 of them indicated that they report the incident after it happened. As one participant said:

> *Both happened [incident reporting] sometimes [employees] report and not, but they report when the problem happened [P10].*

The IT staff hold different beliefs about why employees report incidents or not. Reasons that most employees do not report incidents include lack of knowledge about incident reporting and consequences of incidents (there are no sanctions associated with not reporting incident).

> *Most of the time they [employees] did not report about the incident because they do not know if there is a problem or not but we discover the problem of that [P12].*

Figure 5.3 shows the participants' views on employee behaviour around security incident reporting. Employees may report an information security threat either before or after an incident happened. Some employees did not report information security incidents and may have lacked appropriate knowledge or were not aware of the consequences of not reporting.

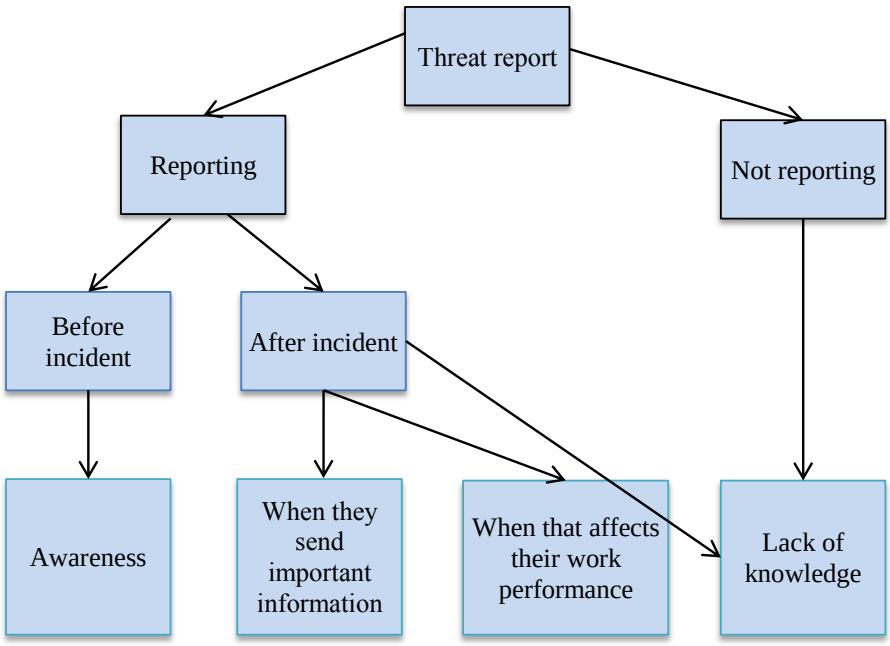


Figure 5.3: Employees' behaviour threat reports

> *Most of them [employees] reported after the incident happened because they do not know the effects [of the incident at the time] [12].*

Some employees never report an incident until the incident makes their work difficult.

> *If there is incident that makes them struggle with their work they will report it other than that they will never report. Usually they report after it happens [P6].*

Employees reported information security incidents after sending important information in response to phishing emails such as username and password or personal details.

> *Most of employees report to us after replying to phishing emails [P1].*

When employees are late to report an incident, the time required to fix the problem is increased.

Most employees reported the incidents after it happens and this cause us [IT staff] more time to solve the problem [P15].

5.5.2.3 Solutions and lessons learnt from incident reports

Rader et al. (2012) found that most people have learned lessons from their friends and families' stories of information security incidents and that this can increase security behaviour when making data decisions. In addition, employees sharing stories of negative experiences indicate that self-efficacy may well be a strong determinant (Conway et al., 2017). In this study the IT staff discussed some solutions for organisations and their employees when faced with information security threats. Most participants send an announcement to all employees through email and mobile devices to avoid a repeat of a problem once it has been discovered by employees reporting the incident to the helpdesk or IT staff finding the problem.

We [IT staff] are experiencing the email phishing they send to the help desk, in the past they reply but now through the awareness by sending messages through mobile and emails to the staff if you receive this kind of email do not reply [P1].

When users discover there is a security threat from inside or outside of the organisation they should inform responsible people in security before an incident happens. Participants believed that the best way to make employees aware that they need to inform their IT help desk and/or system administrators is by sending emails to them.

Before they [employees] informed us after the incident but because of our awareness through sending emails to make them aware about malicious emails they now delete and inform us before doing anything [P13].

IT staff also thought it was important to have consistent ways of dealing with new and/or existing staff, and they should be told immediately.

We need some procedures and policy to know who are joining and leaving the college to delete or add new accounts [P9].

Some participants took the opportunity of an information security incident caused by employees in the workplace to create a lesson for employees, so they could warn all employees about that incident, tell them how to avoid it in the future and remind them of the policy.

> *Incidents help them [employee] as lesson and we send them a message that or we convince them by saying to them that you put your organisation to this risk because of your behaviour [P15]*.

Another participant pointed out that employees would know the information security policy after the incident happened to them:

> *Most of organisation, the policy is there but nobody have the time to read that policy so they will came to know the policy when incidents happened [P10]*.

One participant pointed out that an incident, even though it happens to someone else, could be a lesson for anyone in the organisation:

> *From my experience other way around that a friend who has victimise by scam he experience scam and he lost a lot of money. I think that negative behaviour of colleague helps me to change my behaviour regarding information security policy [P2]*.

Making people aware of incidents provides good lessons for employees, reduces the likelihood of repetition, and avoids the consequences their co-workers have experienced, such as loss of money, time, or important information. Organisations need to have a strategy to increase information security management and awareness of their employees to reduce mistakes and avoid all these consequences.

5.5.2.4 Summary of employees' incident reporting in information security

The interviewees indicated that there are a number of incidents caused by human behaviour rather than technology. The most common problem was said to be responding to emails in the workplace. Participants noted that there was a lack of security incident reporting by employees. Most participants indicated that employees only reported a problem if they experienced a noticeable consequence

with their work. IT staff did not believe that very many employees would report a mistake without experiencing some consequences.

5.5.3 IT staff and System administrators' views on individual behavioural factors affecting information security

The purpose of this part is to understand the factors that IT staff believe influence employee ISP compliance. Understanding these factors could lead to improved compliance levels in the higher education institutions. All participants were asked, from their experience, what factors (knowledge and awareness, managers and co-workers, and sanctions and rewards) they believe influence employees compliance with the organisation's ISP. Participants were prompted with the same eight factors (except response efficacy and behaviour intention) across 14 scenarios from the questionnaires as explored in the previous chapter.

5.5.3.1 Knowledge and awareness roles in information security

Interview question: Do you think knowledge would change employees' behaviour positively or negatively? Do you have experience or examples of where you have seen knowledge change users' behaviour positively or negatively in specific security areas?

The importance of Knowledge: Participants were asked if they believed that improved knowledge would change employees' compliance with the ISP and all of them agreed that it would change positively. In addition, 13 of them brought examples from their own experience. One participant mentioned that an employee who has knowledge will avoid any phishing emails from hackers and one without knowledge would become a victim.

Understanding consequences: All participants linked employees' information security awareness to their knowledge of the consequences of their behaviour when they were asked if knowledge would change employees' behaviour. As one participant put it:

> *Yes definitely, if they [employees] know the hazards the knowledge will help protecting the environment [P6].*

Another participant said:

> *Positively, if the staff knew what will be the effect [of their behaviour] [P4].*

Others agreed that knowledge would allow employees to avoid security incidents, as one participant put it:

> *Giving knowledge to employees is very important to prevent these incidents [P2].*

Another participant said:

> *Yes, if the person is educated and aware and qualified that would help. The person should have the ability to develop himself and really the education and guidelines and what they should do and not do and what is wrong and correct action would help even by training [P16].*

While this is a rather naïve view of the participant, it reflects the belief of IT staff that knowledge by itself can prevent harm.

5.5.3.2 Managers and Co-workers

Employees' compliance behaviour may be influenced by their managers' and/or co-workers' reactions to the policy. The respondents were asked how managers and /or co-workers change employees' behaviour positively or negatively with examples they have experienced.

Managers are the decision makers in their department and they have more privileges and rights than other employees do. This study attempted to explore managers' roles in changing their employees' behaviour (positively or negatively).

15 participants agreed that managers who have knowledge about the ISP are a positive influence on their employees to comply with organisational information security policy, as one participant said:

> *Yes [positive effect], if the managers understand and practise the ISP for themselves first. And he added that: It depends on the knowledge and privileges of the managers in the network [P16].*

If instructions come from a manager/superior it was thought more likely that instructions would be followed:

> *Yes, it is happening the hierarchy of the administration it has to go from up to down and how important is data and how important is the security policies [P2].*

Another participant confirmed that:

> *Yes, actually for any organisation happened from the top to the bottom. From the top - if follow the policies down employees definitely do but if the top not follow, the staff also says if my boss is not following they say why I need it, this is the reason we sometime we face it like if we ask them sometime to do they say my boss not doing why I should do [P10].*

One participant pointed out that a manager could influence employees in the same department:

> *To comply with ISP especially if he is manager he could convince his employees in his department [P15].*

One participant suggested that information security threats would be reduced when managers work with their team to reduce the risk of information security:

> *We [IT staff and system administrators] have faced many spamming emails and flooding and many problems. Then the head of the university team work on the security then the problems reduce to 80% [P12].*

On the other hand, he added that an older manager has a negative effect on ISP compliance in their department:

> *It depends to the manager if that position taken by someone who is from the oldest I do not think so because they do not care about information security and he cannot implement awareness and ISP [P12].*

One participant suggested that managers could motivate their employees to follow the ISP when a member of IT staff has a good suggestion to a manager regarding security:

> *It depends on the head of department how he can to handle the staff. For example, for me if I have a good suggestion and the manager not agree with my suggestion and if he not agrees it will be negative. But if I have suggestion and the manager agrees and implements this suggestion it is positive [P8]*.

Only one participant thought that managers do not have that big an effect on their employees' compliance with the ISP:

> *Sometimes we [IT staff] ask managers in the colleges to do guidelines about information security but they [employees] did not practice it so that means that they do not have that big effect [P5]*.

Participants reflected not only on the departmental level, but also at institution level. For instance, one participant said:

> *We [IT staff] find it that one college are adhere to ISP and other not because of their managers [P14]*.

Another participant said:

> *Some colleges are following ISP and others not because of the relationship between the IT centre and the managers. If the manager or the dean are good in IT and attend the security awareness, because we are conducting awareness to the managers and top positions they will have good response and his employees try to follow the best practice of the protecting data [P15]*.

Participants believed that IT managers practised more compliance with the ISP than other departmental managers and insisted on more compliance from their staff. One participant said:

The managers in the IT department always are practising ISP more than other department such as administrative department because they don't have background about security [P16].

Another participant said:

For example, IT department has strict policy to not install any program which is not licenced [P1].

While differences in ISP compliance may be due to job roles, these quotes show that IT staff in these organisations believe that knowledge is the crucial factor.

- Authority and enforcement

Another reason why managers are very important in changing employees' behaviour is that they are authorised to implement the ISP in the department and are responsible for ensuring that employees follow policy, and can effectively block any suggested changes. As one participant said:

Sometimes if the authority did not give any support to worker, even when we [IT staff] have good ideas for security and we did not have approval from the managers we cannot do anything [P4].

Another participant said:

We [IT staff] cannot implement [ISP] until managers do that, if manager will not do staff will never do [P10].

Participants thought that managers should be a good example to their employees. When managers comply with policy, participants thought that employees would in turn be more likely to comply (and *vice versa*). As one participant said:

If the managers are following ISP and if they are enforcing it to their subordinates then it gives positive feedback from their employees too as well as managers do because if the manager is not care so why would the employees care [P2].

- Communication with managers

The line of communication for most education organisations to implement a policy is to go first from information security management to managers of departments then to employees. The majority of participants agreed that communication between them and managers of departments and employees is a vitally important factor to enforce compliance of organisational ISP. As one participant said:

> *If sometimes we [IT staff] want to make decision we have to follow the rules and procedures for some information we have to inform team leader the head of section then head of department this is the hierarchy level we are still maintaining [P9]*.

5.5.3.2.1 Co-workers' roles in information security

Participants were asked whether they believe employees' ISP compliance behaviour would change other employees' behaviour positively or negatively in the same organisation. Ten participants agreed that employees could be affected positively if their co-workers follow the ISP and have knowledge about security, as one participant said:

> *Yes, they have positive impact especially when there is some employees' neglecting at duty and working with other who is complying with ISP they will affect them positively [P13]*.

And another participant said:

> *Yeah, it affects co-worker also because human nature is learning from the experiences. It helps if one to two in every room strictly complies with the policies the other people start to do that behaviour also [P10]*.

Sharing knowledge between employees in the workplace is a very important factor for success in information security compliance. Some employees don't have knowledge of how to deal with information security problems and they can avoid mistakes when they ask their co-workers who have knowledge.

I believe so it will help others [employees] because once a person who has experience of those things [information security] they share it to their colleagues [P2].

Employees are willing to learn from each other, especially if someone has knowledge about security:

Yes, they [employees] will be affected positively because nowadays people are trying to learn and avoid problems and employees will learn from the person who has knowledge and we found that has advantage they are cooperating to teach each other in the college [P12].

On the other hand, a few participants thought that employees would affect each other negatively because they learn unacceptable behaviours from each other to avoid spending time in security structures or they do not have skills to practice securely.

Negatively yes will affect but positively rarely. I have seen they giving advice to write the password and you can save it in mobile and disabling the antivirus [P6].

Participants agreed that employees follow each other due to friendship without knowing if they comply with the ISP:

Yes they [employees] will follow each other's by not following ISP but they are copying their friends. For example, replying to the emails and they ask each other if those users will ask his friend if he replies to that message then he will reply without knowledge [P1].

Let say some employees do not know to do something then they [co-workers] will tell him click this and they will follow because this is about knowledge if you give them things and new information they will follow [P17].

However, another believed it would depend on the awareness level of the individual. For instance, when one participant was asked if seeing someone writing a password on paper would affect other employees' behaviour he said:

It depends to the person some people use to them [passwords] this is not security threat depends on the awareness and habit [P17].

The fact that employees are more likely to ask their colleagues for advice than IT staff can cause problems. IT staff are left to try and explain that the employee's friend gave the wrong advice:

Yes, it has positive effect as lessons. For example, about antivirus, if the first one is asked for exception to do the disable then they [employees] come to us [IT staff] and we convince him that antivirus not slow down his computer process and clean his system from viruses and we have done configuration in his system then he [employee] informed his friends [co-workers] about that then they come to us for help or any action regards to IT [P15].

5.5.3.2.2 Summary of managers' and co-workers' findings

The results demonstrate that managers and co-workers are judged to have an effect on employees' compliance with organisational ISPs. 15 participants agreed that managers have a very an important effect on their employees' compliance and ten of them agreed that employees follow their co-workers' behaviours rather than referring to policy.

Managers of departments and colleges have more authority than IT staff to enforce the policy. They also serve as role models and can be a good example to their employees and have information security knowledge and good communication with information security management and their employees. In addition, it was felt that colleagues influence each other positively and negatively depending on their knowledge and awareness. Any incident could serve as a lesson for other employees to learn from when it is communicated to all employees to avoid it happening again in the future (Tatu et al., 2018).

5.5.3.3 Sanctions and Rewards

Sanctions and rewards at any organisation could influence ISP compliance. To explore IT staff and system administrators' experience of sanctions and rewards and their influence on employees' security behaviour participants were asked two separate questions.

In terms of sanctions, 13 participants believed that when organisations use sanctions, employees' ISP compliance behaviour would improve. However, most of the organisations studied did not practice this. All organisations have punishment rules but the problem was seen to be that they do not apply them. When participants were asked if sanctions by their organisation would motivate employees to comply with their organisational ISP one participant said:

> *Yes, I believe it will effect positively if you punished one employees the others will follow the policy. We have the rules of punishment but not implemented [P12].*

And another said:

> *Yes, I believe it will effect positively. I do not have experience on enforcing sanctions but for my personal opinion having sanctions to the users would force them or changes their behaviour on security policy [P2].*

Participants from several organisations believed that sanctions should be used in an organisation and they suggested different options for an organisation to force employees to comply with the ISP.

> *Of course, they [employees] will follow security policies if there is a sanction for example for sharing password they should give them three warning [P1].*

> *As in the education sector I prefer to be sanction and it should be depending on the level of the behaviour of the employees [P16].*

IT staff were aware that staff would require education and awareness before implementing a sanction, as exemplified by two participants:

> *Yes, I believe it will effect positively. We [IT staff] have to do the awareness and educate them that there will be sanction for misusing of devices and data in the workplace [P5].*

> *Yes, positively, when employees know what is the consequence in doing anything [P8].*

IT staff believed that the ISP would be followed by employees if there was a punishment and, conversely that they would ignore it if there is no punishment. They will neglect to follow as one participant said:

> *Sometime if we [IT staff] apply strict policy sometimes they neglect, they will say this time if I do not do it there is no issue but if there is punishment then definitely they will follow [P10]*.

A few participants believed that sanctions would have no effect on employees' compliance behaviour:

> *Punishment will not change users' behaviour we have to educate and train them [P7]*.

> *No [effect on employees]. The punishment as since of denial of services yes, but extreme punishment, No I do not believe [in punishment] [P6]*.

Some participants provided examples of when punishment had been seen to work for an individual:

> *Sometimes there is abused of using computer by sending bulk of emails from one computer then we [IT staff] inform the person about that then we terminated his account then he responds positively and try to avoid same problem [P15]*.

An example was also provided of when the sanction was announced to other employees in same organisation to encourage them to follow the guidance:

> *I will give you an example, before the staff doing the exams so we have told them you have to save that files in this location but he did not save it and he lost all the files so that exam was gone and no one know where it is, student were saying we give him and we ask the staff where did you save the files and he said I put it in the desktop then we said we told you have to save it in that location so you are responsible then the management decided what action to do then we announced it and definitely it affect [P10]*.

5.5.3.3.1 Rewards in information security

Participants were asked if rewards would change employees' behaviour positively or negatively. Only eight of the participants said that rewards would help to encourage employees to follow ISP as one participant said:

> *Yes, it is 100% that should be [rewards] by the HR if you are not encouraging the employees after some time the employees will lose interest and they loss everything but if you encourage them then definitely they will do [P10].*

Suggestions were made as to how the rewards could be structured to motivate employees to comply with their organisational ISP.

> *Before we [IT staff and system administrators] apply for some rules and no one [employees] are following after that with co-operation with other organisation, people how follow this we will make a draw and will give them some gift first time some people came and second time when we announced 20% people come third time when we announced 50% people come. They go for that document and follow the rules [P10].*

Another participant suggested that rewards that recognise performance (such as a certificate for those who follow the ISP) would help to motivate employees to comply with the ISP. One participant suggested:

> *Yes, it will affect positive when the management reward or give credit to the person. ... They [management] give certificate for precautions when employees' performance is better and that will motivate employees [P8].*

However, the half of the participants felt that rewards would have no effect:

> *Reward system I think it is not affected [P3].*

> *No that [reward system] is their deity and this is protecting for them [employees] and they have to follow that policy [P4].*

A few participants indicated that sanctions and rewards do not exist in their organisations or are not a big issue. For example:

Since we [organisation] do not have punishment we do not have rewards in the system [P6].

I think it [reward] has positive affect sometimes. We do not follow this as big issue [P15].

Only one participant believed that rewards for employees who follow the ISP would have a negative effect on others:

The security is very important especially in admission and registration department. To motivate the employees to comply with ISP from my opinion I am afraid that reward will be competition between users on the rewards and it could be it is a negative effect [P16].

Another participant suggested that rewards have a positive effect just on the IT staff and system administrators who create the ISP and working in IT staff as he said:

Yes, it will effect for the developers who are updated and brings ideas for ISP. But if one person updated and producing a new ISP ideas and then his suggestions is not accepted or been ignored that will stop him to bring suggestions and this will effect negatively [P13].

The same participant continued, suggesting that the reward would be if the organisation accepted his idea in security environment:

When organisation is accepted staff suggestions regarding secure environment that is the reward instead of gift or certificates [P13].

5.5.3.3.2 Summary of sanction and reward factors

All participants were asked about the impact of rewards and sanctions on employees' compliance behaviour. The results show that most participants believed that sanctions would be effective. In addition, almost half of them agreed that rewards could also be effective. A few of the participants agreed that sanctions and rewards may have a negative impact on employees' compliance behaviour. Despite

these beliefs it does not appear to be the case that rewards or sanctions are implemented within the majority of the organisations studied.

5.5.4 The main barriers to compliance with the information security policy

Several barriers that hinder employees' compliance with their organisation's information security policy were identified under two main themes: organisational culture and employee culture barriers. Each theme includes several discrete aspects that can impede employees' compliance.

5.5.4.1 Organisational culture barriers

The participants indicated several aspects that can substantially inhibit employees' compliance with the ISP.

a. Lack of awareness of threats and consequences of non-compliance

11 participants indicated that employees are not aware of the ISP because their organisation does not provide training or awareness programmes for them and that this can lead to increased security breaches:

> *We do not have that much awareness in the college especially in the security or in the way of dealing with security problems [P6].*

> *Users do not know about security just he open what he want to open. Knowledge and awareness in our organisation is very weak [P12].*

Participants suggested that employees should be aware of the threats the ISP is designed to protect against and the consequences of not complying with it:

> *As long as it is clear to the staff the advantage and disadvantage of the security will help to comply with ISP [P8].*

> *If they [employees] know the hazard or the effect of their action definitely they are not going to do it [P6].*

> *Number one is the knowledge by employees has a knowledge it would give them adequate information regarding of the dangerous or the threats of not following information security policy [P2].*

- Infrequent information security awareness campaigns

Three participants mentioned that their organisation has an information security awareness campaign and training for their users, but that it is not effective when it happens just once. Training, which helps them to stop making mistakes, needs to be regular and evaluated for its effectiveness.

> *It [information security awareness] should be ongoing process and should not stop whenever it stop people will not do it and will forget it [P10].*

> *Also, the training should be continually repeated as security awareness is an ongoing activity [P2].*

> *Awareness seminars should be regular which has done one year before but that is mean not enough which is not possible for organisation to conduct awareness programme for three months it should be small teams in departments at least once in the month or twist and it has to be streamlined [P3].*

b. Managers' behaviour, attitudes and communication

The second main barrier to compliance with the ISP was the managers' behaviour and attitude. When managers do not understand the advantages and disadvantages of the ISPs, are not persuading employees to follow them, are failing to communicate and do not follow the ISP themselves, the employees are less likely to comply:

> *Knowledge and manager have positive effect on employees' behaviour to comply with ISP. The manger should have knowledgeable about security policy, because the manager forcing employees without knowledge what is advantage and disadvantage will be useless [P8].*

> *[Managers] should force the staff to follow the policy and the managers should follow the policy then the staff will follow also. We have the policy but there is no strict implementation of the policy from the higher-ups (managers) there is no supporting that is why security is not strong [P4]*

Lack of seriousness of compliance with information security policy from the small management to top [P13].

Lack of awareness and there is communication gap between one department to another department and from higher position [manager] to lower position [staff] [P4].

c. Information security policy

Participants pointed out that when the ISP is difficult to understand, does not cover all required behaviours, gets in the way of productivity or prevents employees doing things the way they want to, then employees would be less likely to comply:

If the policy is not clear for them and if the policy blocking their process [at work time] and they did not know what the effect of that policy is [P1].

Work pressure makes employees to not follow the ISP [P12].

They [employees] want everywhere shortcut if they follow the policy they will go for long run [P7].

We have ISP but it is not related to the behaviour for example if the staff want to access to the internet what they have to do [P8].

The organisation should cover everything in the security and continues to aware their employees [P14].

If we [IT staff] do not give the proper explanation [about ISP] they [employees] will be angry and they will not meet their understanding [P11].

The culture her that they [employees] are feeling information security something like limitations stopping them do what they want to do [P5].

Another participant pointed out that if employees had to take responsibility for their actions, then they may be more likely to comply with the policy:

The hackers say that we are supporting email and send me your [employees] username and password to do the rest and because users not sign for password responsibility they do not care about it [P14].

d. Lack of security organisation

An organisation needs to have information security staff to follow up the work and observe employees' behaviour relating to security. One participant thought that this is a problem with most organisations as they do not have sufficient staff for information security.

Actually we have a plan for the awareness but you have to get staff for information security [P15].

e. Technology and hardware

Old technology may be slower than employees like and employees may disable security software to speed up their system. Participants identified not keeping technology up to date as a potential barrier to security compliance.

We [organisation] have to upgrade our software and hardware because for person disable his antivirus because of slowing the computer because if the computer upgraded the employees will not disable their antivirus when they are busy [P3].

f. Lack of sanctions and rewards

Some participants mentioned that when there are no sanctions or rewards in an organisation that employees would be less motivated to comply with the ISP. For example:

There is no punishment and motivation [P12].

5.5.4.1.1 Summary of organisational culture barriers

In this section, several organisational culture barriers to employees' compliance with information security policy are identified. IT staff and system administrators indicated that they believed the main barriers were:

- Organisations not providing regular awareness and training programmes that clearly illustrate the advantages and disadvantages of following the ISP and not evaluating the effectiveness of these programmes.
- Top management and middle managers not understanding information security policies and not complying with them. In addition, lack of communication between them with information security management and their staff and not enforcing policy on their employees.
- Information security policies and behaviour guidelines which are not available, difficult to understand or do not cover important behaviours.
- Lack of security staff.
- Old and slow software and hardware.
- Lack of sanctions and rewards for security behaviours.

5.5.4.2 Human behaviour and culture influencers

There are several human factors that could influence employees' non-compliance with their organisational ISP. These include trust, bad habits, misunderstanding the security policy, lack of interest, lack of security skills and work pressure.

a. Trust

Most participants suggested that trust between all staff in the work environment is the main problem for security. There is a culture of trust which means that staff may leave a door open when they leave their offices, would not lock their screen if they leave the computer (if other staff are in the room) and may share usernames and passwords:

> *The main reason of not following ISP is our culture because we [all staff at organisation] feel that we have trust each other. It is difficult to say no to our co-workers if they ask to access to your computer or use your password [P15].*

> *We [IT staff] do find that incidents where users attempt to share information with friends which is good for them but not good for organisation. We inform*

the employees not share their username and password even with their boss and security policy is this and that [P3].

They [employees] share username and passwords with their co-workers because of trust [P12].

Because it depends on the culture here like locking the door window especially there are more than one employees in on office and the society is trusted in the university culture [P17].

b. Bad habits

A few participants mentioned that employees are not complying with the ISP because of bad habits. One asserted that employees should change their habit to comply with ISP:

Time is not the factors of following the procedures it is meter of habit and change your habit [P6].

Another participant, when asked about the main barriers to employees complying with information security policy, said:

They think it is the habit and culture [P17].

Employees do not close their doors when leaving their office and one participant admitted that even he does not close his office when he leaves for a short time such as for coffee.

Further one is physical security, usually happened by not closing the doors even myself not locking the door when I go for coffee or for breakfast. Most employees leave the doors open and there is no screen saver in their computer [P13].

c. Lack of interest

Some participants indicated that one of the barriers to compliance was lack of interest as one participant said:

Because of personal interest for example you want to open YouTube [P8].

Another participant said:

You know that each user has his own computer and connected to the internet and he has free to do what he wants to do [P5].

One participant thought that employees are not taking ISPs seriously because they will not lose any money:

Some employees take ISP as not serious issue in the college because they are not going to lose money or something that important as they think [P14].

d. Lack of security skills

One participant pointed out that when employees created a strong password and they came back from a long holiday then they forgot their password.

We [IT staff] are facing problems [from employees] about strong password especially after long holidays also the password if it is strong it should be changed every six months [P13].

Another participant indicated that some employees do not have basic IT skills such as searching for deleted files in their own computers.

Employees do not have skills to search for deleted files and when they told us that they lost their files we find that he deleted it mistakes or he did not know where he moved it [P14].

5.5.4.2.1 Summary of behaviour barriers

To summarise the findings regarding behaviour barriers to compliance with information security policies, several reasons were highlighted:

- High trust between users can lead to failure to comply with organisational information security such as sharing password and leaving their office's door open when they leave for short time.
- Bad habits.
- Lack of understanding of the benefit of complying with the ISP.
- Lack of interest in security issues.

- Lack of information or security skills.

5.5.5 Information security management and recommendations

After the obstacles and factors that influence employees' compliance behaviour were identified, participants were asked to give their opinions and recommendations to information security management to raise the employees' behaviours and awareness and organisational security environments.

5.5.5.1 Ranking important factors to help employees to comply with ISP

Participants were asked to rank the influencing factors in order of importance to motivate behaviour to comply with organisational ISP such as knowledge and awareness, managers, information security policy, culture, sanctions and rewards. Figure 5.4 shows the order in which the factors were ranked. The results indicate that the participants consider the most important factor to be knowledge and awareness and the least influential to be a rewards system.

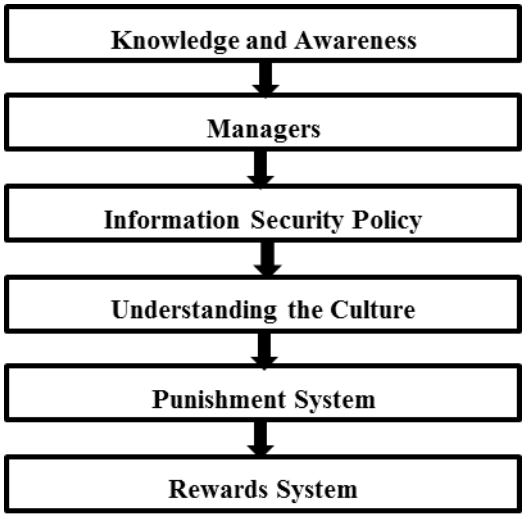


Figure 5.4: IT Staff ranking of important factors for employees' behaviour

All participants agreed that the most important factor is knowledge and awareness and therefore the organisation should educate and explain to employees why the ISP is important to follow. Security management should inform all employees where and what is their ISP and how important it is by conducting seminars.

> *Any employees should be informed about what are their policies available in the organisation especially regards to the security and how important data to*

this organisation and how important they reliable to securer their information that should be some seminar kind of workshop for administrators and employees [P2].

One participant mentioned that all the above factors collectively influence employees' behaviour:

All of these factors [knowledge, managers, sanctions and rewards] are related to each other and work together [P15].

5.5.5.2 Recommendations to improve information security policy compliance

Two recommendation themes were identified: information security management requirements and employee security behaviour.

5.5.5.2.1 Information security management requirements

The participants provided various recommendations about how to improve compliance behaviour to reduce security incidents by improving information security management in the following areas.

a. Awareness requirements

All participants believed that employees' security compliance would improve with more information security awareness and they specified that knowledge, training, education and manpower resources to deliver the training are the most important factors for successful compliance with the ISP.

- Knowledge, training and education

Participants identified several solutions to raise security awareness and educate employees to comply with organisational ISP including that organisations should train their employees through workshops and explain to them what the effects would be if they do not follow the ISP. For example:

Firstly is again I would provide knowledge awareness to the employees by providing trainings workshops and giving them examples or ideas that information security policy is very important that it should be followed [P2].

First they [employees] should be aware of that policy and what is the affect if they did not follow [P11].

Yes, educate means we have to give some security training, seminars. We have to explain and train them it is education purpose we have to educate and give the solid training needed [P7]

The organisation should have a strategy for differentiating between employees who read the ISP and have knowledge about security and those who don't. One participant expressed it this way:

For a new staff when they join the university they should read the policies and the regulations of the university but if someone has a knowledge and reading them what he has to do and what we have to do [P14].

- Information security team

Participants recommended that each organisation should have an information security team with representatives from different departments.

There should be small committee [information security team] in different department of the organisation because it is very difficult for the organisation to understand all employees accessing the computers and doing all the works in the computer [P3].

It would be the role of this information security team to communicate the importance of security to the departments. As one participant said:

As we are information security [staff] in the organisation the one who are responsible about availability, confidentiality and integrity of data in the organisation and anything could affect the data which is our priority [P15].

- Continuous awareness

Participants believed that awareness and training should be carried out regularly to maintain the employees' knowledge of best practice.

After period of time for example semester circulated like emails also should be there panels and some activity should be done so they [employees] will be aware and recall what the policy says about it. So the awareness should be continuous. … Awareness in the beginning and continues of awareness and sanctions [P14].

For example, there is email every six months spread to all employees about awareness for example password sharing or do not give it even to the administrators or their managers [P10].

- Methods to increase awareness

IT staff suggested different methods they have tried in order to maintain their employees' awareness about sending emails, putting information online and having face-to-face discussions about specific issues. Some suggestions for how to improve awareness provision were given. Examples are provided in the quotes below.

We have to encourage employees through occasion meeting and emails [P9].

In the past they reply to spam emails but when we aware them through emails they are becoming better [P13].

When we are getting many problems from one department because of particular issues but we explain to them [employees] this is the scenario and this is the affect then the number of incidents is decreased [P4].

We [IT staff] explain it to them [employees] that make sure you do not do it again when you receive these emails their behaviour changes by next incident they receive the same request from the sources and unknown sources they informing us do we answer this or do we need to follow this link so it helps a lot if they proper information [P2].

Some staff from science department they are not familiar with IT skills and we are providing training online at E-learning after that they are good and they do not repeat the mistakes [P9].

We have to have something more about security awareness programme or something centralised, awareness video or awareness instructions in our college website E-learning even though it is available in the internet we have to customize and keep it in to understand according to which one we are implementing of policy in the organisation [P11].

IT staff should consider employees' reaction when they establish a new security system. Therefore, any awareness training must provide clear explanations of why employees must follow policy:

We [IT staff] have the device to implement the policy hopefully not access this and that in case the security aware about that things to implement the policy up-to-date and then to avoid our staff feeling bad we have to give proper explanation in our website then they can understand so they will be happy to implement the security nicely [P11].

- Skills

Participants agreed that all employees should have appropriate knowledge and IT skills. They mentioned some examples of information security skills such as creating a strong password for their folders and files. One participant highlighted that they had insisted on the use of long passwords but that this had caused some problems for staff.

Other participants offered some examples of how employees could create long passwords and remember them easily.

Before we [IT staff] are using only very minimal numbers of password accepting short password for employees now we [IT staff] implemented the ten characters password and some employees are having difficulties because sometimes they forget the password then we let them to change the password based on our requirements from that time the behaviour of that employees change by securing their computers [P1].

For example everybody should have ten characters for their password for security purpose maybe they do not like it but I do not know here but in basic

if you introduce the knowledge they will accept it but this one takes time [P17].

Another participant discussed how they had to change employees' behaviour to prevent passwords being saved in a file.

It does happened when some incident happen then we [IT staff] came to know after we arrange training for them then they beneficial that they are keeping how they are storing their data, how they are putting the password in the folder [P10].

b. Effect of managers

The majority of participants suggested that managers have a strong effect on employee ISP compliance. The manager is an important communication link between IT security and staff behaviour, influential in determining that staff attend training and which rewards could be available to employees.

I will mention the ongoing training or ongoing rewards which is more attractive for the staff which are coming from the managers [P10].

They also felt it was the managers' responsibility to monitor compliance and correct any non-compliance, making sure the employee is aware of the consequences of non-compliance.

If the manager is seeing he has to call that guy and tell this password is important and if someone has your password from outside they can access to our server [P7].

The managers should observe their employees behaviour [P16].

The manager is the key communication between the technicians and his employees [P12].

c. Information security policy

According to the participants, the information security policy and guidelines should be documented, understandable and available to everyone in the organisation but believed they were not accessible to the users in the organisation.

> *The policy should be available and enforced to follow and even the physical security so they [users] have to feel serious about policy [P15].*

> *For security we have to educate [employees] then it will come to the knowledge then we have to think about policies one by one and place it [P7].*

d. Sanctions

Some participants thought that if the organisation has ISP education in place and staff do not follow the policy, then it would be acceptable to enforce sanctions against employees.

> *When you punish a person without knowledge and awareness is difficult but you could educate him and when you see that he is still repeating the mistake you might use the sanction with him and that could solve the problems [P5].*

One of the sanctions suggested is disabling users' accounts:

> *The administrator should not ask for the username and the passwords of the users under any circumstances accept if he [employee] has done some mistakes and I can disable his username and password to access to the organisation [P16].*

They also point out that telling others about the behaviour and the sanction could prevent others from repeating the same mistake:

> *The sanction is when we announced that for one user he has done this and that would be a lesson to others that we are observing them that would help to stop this type of behaviour [P16].*

However, another participant pointed out that sanctions, without an understanding of the risk they are creating, are not likely to be effective:

If you are forcing them [employees] to do or giving them sanctions but they do not understand why you are providing this sanctions or why you need them to follow this policy the first thing is educating them to understand the risk involve following ISP that's why knowledge then you can implement policy and then you can have your sanction [P2].

5.5.5.2.2 Social issues effect on human behaviour

The majority of participants suggested that organisations should recognise social issues such as habits, trust, satisfaction and responsibility as important factors to motivate employees to comply with the ISP.

- Trust

Participants brought up the issue that employees place trust in other people over following the ISP and believed that overriding this behaviour would be difficult.

One of the solutions of changing the culture by awareness and make them trust the policies but employee would say this is my friend and I know him but about using the system no, I should not use his system [P15].

They [employees] should not trust anyone about username and password. Of course, most employees in IT department when we ask them that not allow to do they follow but after one or two semester they go back and do the same mistake [P12].

- Taking Responsibility

One participant agreed that awareness of and understanding the culture is very important in changing employees' behaviour security for the better. They indicated that an organisation is responsible for making their employees aware of what is required of them, but that each employee must take responsibility for their own compliance.

Awareness by educating people and second they should know that they are in work and they have to do it by computer then they have to use it with aware not for personal use and in proper way to finish the job…..ISP should be

known for everyone, and then they will know that they are responsible for their actions and comply with ISP [P13].

5.5.6 Summary of managers' ranking of effects and recommendations

The participants provided the following order of importance for factors that could improve employees' compliance with the ISP: accurate knowledge, training, education, managers, information security policies and guidelines, understanding employees' social issues, punishment and then rewards.

All participants recommended that organisations should educate and train their users in information security covering areas such as how to create strong passwords, report security incidents, check email sources, backup confidential data, use antivirus software and to be aware of transferring information and so on. After that, they should make sure that their users understand what the consequences of poor behaviour are for themselves and their organisations and introduce appropriate disciplinary procedures covering non-policy-compliant behaviour.

Moreover, participants suggested that managers' enforcement and communications with information security management and employees are very important factors in ensuring policy-compliant behaviour. Organisational information security policies should be documented, reachable and understandable for all users. Finally, the results indicate that human social influence is very important in influencing compliance.

5.6 Comparison of employee survey with IT staff and system administrators

The first aim of this section is to compare IT staff and system administrators' ISP compliance with the results found in the employee survey (Chapter 4) and to order the behaviours by importance (as ranked by the IT staff). This comparison will help to understand the order of importance of behaviours and the relationship between what IT staff will accept (out of policy) and staff behaviour. The second aim is to explore if non-compliant answers IT staff and system administrators' find acceptable are behaviours chosen by staff.

Both groups were provided with the same set of scenarios in a questionnaire for evaluating their security awareness, but employees had to select only the answer they believed to be correct while IT staff and system administrators were asked to provide more than one option if they found other non-policy-based options to be acceptable.

Table 5.8 shows the scores from of the employees and IT staff and system administrators sorted by the rank order given by the IT staff and system administrators (1^{st} to 14^{th}).

5.6.1 Comparison of employee scores with IT staff and system administrator scores

Analysis of the results shows that the IT staff and system administrators had a mean ISP-compliance score of 81% while employees had a mean of 57%. This means that IT staff and system administrators are more aware of how to comply with the ISP than employees by a large margin. In general, the results in Table 5.8 show that the IT staff and system administrators in all scenarios are scored higher than employees' compliance scores accept in scenario 3^{rd}, they are equal. Surprisingly, that the both group employees and IT staff are scored very low in scenario 1^{st} as it is the highest important employees' behaviour.

Table 5.8: Comparison between employees' answers and IT staff and systems administrators ranked in order of importance

Importance Ranking	Scenario	Employee scores %	IT staff and System administrators' scores %
1^{st}	7. Incident report (email asking for personal details)	33	71
2^{nd}	13. Incident report (missing files)	94	100
3^{rd}	9. Phishing email(email unknown source)	88	88
4^{th}	4. Sharing passwords (with co-workers)	65	82
5^{th}	6. Sharing passwords (with IT staff)	31	59
6^{th}	2. Creating a new password	51	53
7^{th}	8. Incident report (windows	57	88

	appear suddenly)		
8th	3. Sharing passwords (with managers)	29	79
9th	14. Deleting shared files without authorisation	62	88
10th	10. Disabling antivirus protection	67	94
11th	5. Physical security	41	71
12th	12. Not using email for commercial or personal purpose	80	100
13th	11.Downloading software from the internet	63	100
14th	1. Backing up confidential data	35	65

The results in Table 5.8 illustrate that less than 80% of IT staff and system administrators provided compliant answers for four scenarios (1st, 5th, 8th and 14th); while 36% of employees chose the compliant answer in these same scenarios. On the other hand, 80% of IT staff and system administrators chose compliant answers in seven scenarios (2nd, 3rd, 4th, 9th, 10th, 12th and 13th) compared with an average of 60% of employees. That means the level of employees' behaviour (in eleven scenarios) may be influenced by level of IT staff and system administrators.

The number of IT staff and system administrators who would accept non-compliant answers ranges from 6% on scenario 3rd to 88% in scenario 7th, indicating that for some behaviours very few alternatives are acceptable, but for other behaviours, non-compliance is acceptable to IT staff. Unfortunately, this does not appear to be related to the importance of the behaviour.

Figure 5.5 shows the relationship between the IT staff and system administrators' scores and employees' scores by scenario using the same rank order).

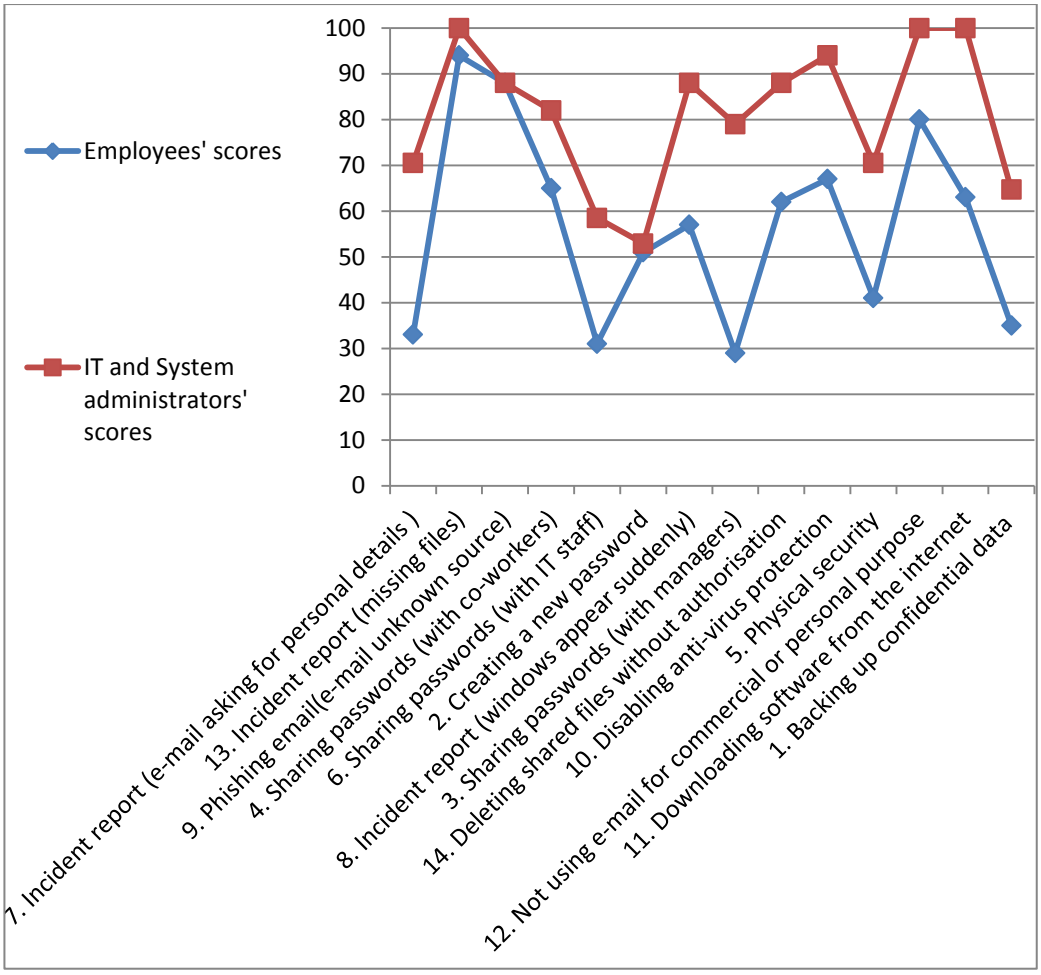


Figure 5.5: Comparison between employees' compliance with ISP and IT staff and systems administrators ranked in order of importance

Incident reporting (email asking for personal details) is the most important information security behaviour and backing up confidential data is the least important to IT staff. The results show that for the most important behaviour only 33% of employees show policy-compliant intentions.

Scenarios ranked 1st, 4th, 5th, and 7th in both groups have big differences in compliance scores. Despite 1st being the most important behaviour for IT staff and system administrators only 71% of them agreed that employees should phone the administrator to report a phishing email (with only 33% of employees indicating they would likely do so).

Regarding sharing passwords between employees (fourth most important) and sharing with IT staff (fifth most important) both groups have scored differently. 82% of IT staff and 65% of other employees would not share passwords with colleagues

but only 59% of IT staff and 31% of employees would not share with IT staff. These scenarios highlight a big issue with sharing passwords with IT staff. Trust between employees and IT staff to share password is a major barrier to compliance with the ISP.

In contrast, there are a number of similarities in scores in the scenarios ranked 2nd, 3rd and 6th. The incident report (missing files) scenario is the second most important behaviour to IT staff and system administrators and they scored 100% compliance and employees scored 94% which is the highest employee score. This may be a result of this outcome (lost files) directly affecting productivity in the past.

Compliance intention was also high for the 3rd most important scenario, with both groups having 88% compliance in the phishing scenario (email unknown source).

While creating a new password was the 6th most important behaviour only 51% of employees and 53% (9/17) of IT staff and system administrators would comply with the rules around creation of new strong passwords.

In scenarios ranked 1st and 8th both groups scored low for ISP compliance compared to other scenarios; employees scored less than 42% and IT staff and system administrators scored less than 80%. For instance, only 29% of employees and 79% of IT staff agreed that employees should not share their password with their managers with the remainders indicating they would share their password. In this case, the managers' authority seems more important than compliance. In addition, because of trust and lack of responsibility in physical security, IT staff scored 70% (which is low compared to other scenarios) with employees scoring 41%. Furthermore, the backup of confidential data is given a low importance and both groups scored less when compared to other scenarios; IT staff scored 65% and employees 35%, which may indicate that employees and some IT staff do not see back up confidential data as a security task.

On the other hand, IT staff and system administrators scored high in the 13th, 12th and 10th ranked scenarios because bad behaviour of employees in these scenarios can lead to employees' computers becoming infected with viruses and it will then take time to remove them from the organisation networks. For example, IT staff

scored 100% in the downloading software from the internet scenario compared with only 63% of employees. Also, both groups scored high in not using email for commercial or personal purposes (IT staff 100% and employees 80%) and the antivirus scenario (IT staff scored 94% and employees 67%).

5.6.2 Comparison of employees scores with IT staff and system administrators' scores non-ISP-compliant acceptable behaviours

As mentioned above, the IT staff were able to select more than one acceptable behaviour option. This section looks at the most popular non-policy-compliant answers given by IT staff and the percentage of employees selecting the same answer. This gives an indication of "shadow security" (behaviours which are accepted even though they are not the behaviour documented within the ISP). Figure 5.6 shows that more than 50% of IT staff accepted alternative behaviours for six scenarios (1^{st}, 6^{th}, 7^{th}, 8^{th}, 9^{th} and 14^{th}) while all employees scored less than 50% in these behaviours.

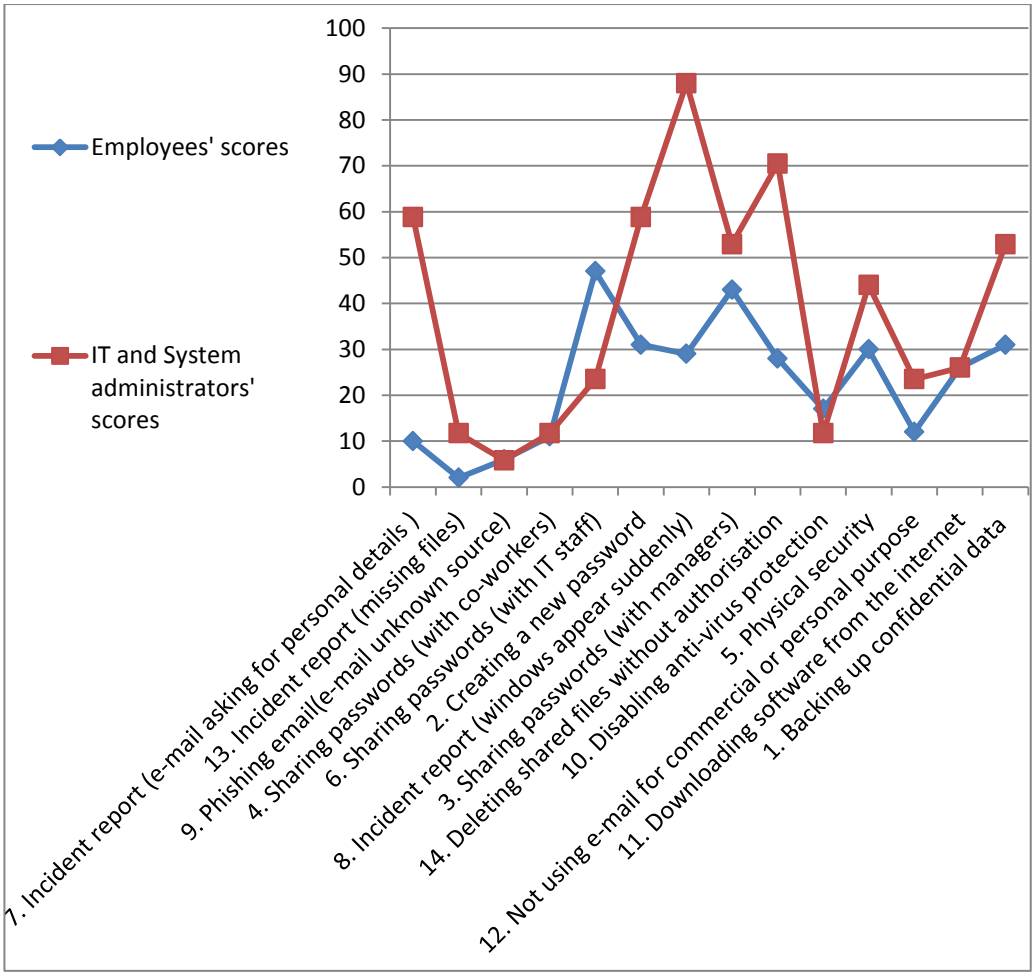


Figure 5.6: Comparison between employees and IT staff and system administrators in acceptable non-ISP-compliant employee behaviours

The results show that 15 IT staff and system administrators was the highest number to accept a specific employee behaviour which is non-compliant with the ISP. This occurred in the virus scenario in which many new windows appear on an employee's computer screen. IT staff found it acceptable to check the antivirus software is switched on and 29% of employees selected this option rather than the compliant answer. This indicates an assumption that the antivirus software will work even when the computer is compromised.

Ten IT staff accepted employees using the same password they use for other services as long as they change one of the characters in it; 31% of employees selected this as the correct answer. This action does not comply with the ISP but it is an easy way for employees to remember passwords. Furthermore, the same number of IT staff accepted employees' behaviour when they delete an email that

appears to have come from an administrator asking them to go to a specific web link to confirm their personal details while only 10% of employees think that is the right behaviour. This is a secure action to delete the email but employees should inform their IT security management about it to avoid the incident happening to other employees on same network.

Regarding the physical security scenario, five IT staff and 30% of employees believed that employees do not have a responsibility to lock the doors and windows of their offices when they leave, and that they should just lock their computer's screen.

Five IT staff accepted that employees could send their username and password to IT staff for troubleshooting purposes after checking the source of the email requesting them to do so while 47% employees believed this to be an appropriate action.

12 of the IT staff accepted that employees could delete the files of a project without asking permission from their co-workers working on those files when project is finished as long as they save copies onto their USB memory stick while only 28% of employees selected this answer. This may be because it is not seen as a security task, and that the action is reversible, as there is a copy on a USB. Of course, USB security is another issue.

In the 8th and 14th ranked scenarios nine IT staff accepted that employees should share their password with their managers when their manager agrees to take responsibility and that employees can send a confidential file to their commercial email account when they have permission from their managers. Both of these scenarios are associated with managers and more than half of IT staff trusted managers, this causes employees not to comply with ISP. In addition, 43% and 35% of employees respectively chose these behaviours.

26% of both groups agreed that employees can install software programs downloaded from the internet by themselves for work purposes as long as they ensure it is virus-free. However, it is not always straightforward to ensure software is virus-free and so this should be the responsibility of the IT staff. Four IT staff

agreed that employees could use university email to reply to their customers for commercial purposes while 12% of employees agreed.

5.6.3 Summary of comparison of employees and IT staff and system administrators

This section analysed the results by comparing the employee and IT staff survey results. In all scenarios, all the IT staff scored more than or equally to employees' scores which indicates that IT staff were more aware than their employees of the compliant answer, but that even among the IT staff there was not 100% awareness, and IT staff found some non-compliant behaviours acceptable.

The findings show that the importance of behaviours (as ranked by IT staff) did not correlate with ISP compliance as both neither groups' performance matched the importance of the behaviours. In addition, IT staff and system administrators accepted some non-ISP-compliant behaviour by employees, such as sharing passwords between employees and managers, creating passwords similar to previous ones, saving confidential data on commercial email servers, not reporting incidents, and not asking for permission to delete project files.

Trust appears to have the most influence on employees' non-compliance with the ISP in most of scenarios. The results indicated that the authority of managers is believed to have a strong influence on both employees and IT staff in failing to comply with security policy.

5.7 Summary of chapter

This chapter has summarised the results of the study of 17 IT staff and system administrators from different organisations. Employee behaviour is influenced by several factors each with a different level of importance. This would help the organisation to prioritise poor behaviours in order to avoid information security incidents and increase ISP-compliant behaviour.

The results identified organisational and cultural barriers that could prevent policy-compliant behaviour. However, to reduce the threats of information security breaches in an organisation, information security awareness is very important factor (Akhunzada et al., 2015; Caputo et al., 2014).

In the current study, the qualitative results suggest recommendations for information security management: enhance the information security awareness and change employees' behaviour to comply with information security policy. Finally, the two survey results (IT staff and system administrators' data analysis and the employees' data analysis in Chapter 4) were compared and found that the level of employees' security awareness is influenced by IT staff and system administrators' security awareness. The next chapter presents a qualitative study with employees in focus groups discussions to explore their views on the scenarios used in this research.

Chapter 6: EMPLOYEE FOCUS GROUPS INTERVIEWS

6.1 Introduction

In Chapter 4 (employee questionnaires), employees in several colleges and universities in Oman completed a questionnaire to assess how they would advise third parties to behave in various cyber security scenarios and explore the importance of the factors that could affect employees' behavioural intentions regarding ISPs. The results revealed that some parts of an ISP were more likely to be followed than other parts and that authority and social influence were believed to be particularly influential on likely behaviour. The aim of this follow up study is to explore in more detail the reasons behind these decisions and why other non-compliant behaviours may be considered, and to identify why different factors may influence their behavioural decisions in context.

A series of focus groups was conducted with employees in one institution in Oman. The following questions were addressed:

a) What are the reasons behind the results in Chapters 3 and 4?
b) What is the employees' understanding of the ISP and their level of information security awareness?
c) What role does the information security policy play in these decisions now and in the future?
d) Given specific situations, how do staff believe they should behave and why?
e) What factors do staff believe influence their behaviour to comply or not with the ISP and why?
f) What advice do employees recommend for the ISP and an enhanced information security environment?

6.2 Methodology

The focus group method was used to understand participants' ideas, with the aim of understanding the motivation behind their behaviours and thoughts, and moreover,

to explore the justification behind their behaviours and thoughts. The focus groups were conducted in an informal and relaxed setting (Heary & Hennessy, 2002).

Krueger (1994), defines focus groups as "a carefully planned discussion designed to obtain perceptions on a defined area of interest in a permissive, nonthreatening environment" (p. 6).

6.2.1 Focus groups interviews

In this study, data was collected through focus groups discussions. The questions were grouped in two parts. The first group of questions was based on six different scenario questions to encourage discussions to explore employees' information security awareness and justification for compliance or non-compliance with their organisation's information security policy. In this section, six new indirect scenarios were formulated to explore with employees issues around sharing passwords, social engineering, physical security, backing up data, incident reports and disabling antivirus protection.

The second group of questions considered the availability of information security policies, employee understanding of security policy and compliance with their policy, the factors that influence compliance intentions and employees' recommendations for writing security policies and improving compliance.

6.2.2 Participants and the college:

After receiving ethical approval from Northumbria University (See appendix A fourth study), 21 participants (6 females, 15 males) with an average age of 40 were recruited via email. Empirical data were collected through four focus groups discussions within a single college in Oman but in two different departments (two groups from the Information Technology department [ITG1 and ITG2] and two groups from the Engineering department [ENG1 and ENG2]). The four groups comprised lecturers, coordinators and secretaries. This college was involved in all the three studies in this research and provided 181 participants in the second study (see Table 4.2).

The participants were randomly assigned to one of four groups, resulting in three groups of five participants and one of six, seeing as Hoppe et al. (1995) recommended that a focus group should comprise four or five members to guarantee at least three "talkers". Each participant had more than three years' experience working at the college and was in possession of at least a bachelor's degree. The only inclusion criterion required was to be an employee at the college. There were no exclusion criteria.

6.2.3 Procedure

Upon arrival at the focus groups venue participants were briefed and asked to complete an informed consent sheet. Participants were organised in a circle around a voice recorder to encourage discussion. The investigator then introduced the structure of the focus groups to participants, outlining two distinct types of questions that would be covered: understanding the information security policy in general and answering questions concerning information security compliance scenarios (see 6.2.1 focus groups interviews). The investigator then proceeded to ask the discussion questions. Each session lasted approximately 60 minutes. The English language was used in the interviews at the request of the participants as they were from different countries (India, Oman and Philippines).

6.3 Results

The results are discussed in two sections. First, the results of the discussions of the six different scenario questions: sharing passwords, social engineering, physical security, backing up data, incident report and disabling antivirus protection are explored and analysed. Second, the results of the discussion questions around general security policy information, factors that influence employees' compliance with policy and recommendations for success of the information security environment are presented.

6.3.1 Scenario questions results

The six scenarios dealt with information security issues such as sharing passwords, social engineering, physical security, backing up data, incident reports and disabling antivirus protection. To measure their application of knowledge in

relation to information security, participants were asked what a third party (employee behaviour) should do in each scenario. Participants were then asked what they should do if they were in the same situation in order to directly measure their behavioural intentions. Each focus group discussed each scenario following the same steps.

Scenario 1: Fahad's manager has forgotten his password and needs some important files. He asks Fahad for his user name and password so he can continue to work. What should Fahad do?

In response to this scenario some participants from the engineering groups said that the employee should give his user name and password to their manager. Engineering group 1 (ENG1) and engineering group 2 (ENG2) both pointed out that this relies on trust in the manager, while one participant pointed out that they would limit the time that the manager had access to the account by changing the password after the manager had the required files.

In ENG2, fewer participants agreed that Fahad should share his password, instead they suggested that they could log in on the manager's behalf and allow him to use the system. For example:

> *He cannot share any password with anyone but still if manager is working with him he can open the machine and the manager can work no need to share the password [P1, ENG2]*.

The ITG1 group was categorical that a password should not be shared, not even with a friend:

> *If there is security policy in the organisation it will strictly say that your username and password should not be shared with other people and you are the only one responsible for your identity in the network so they should not share even with the management [P2, ITG1]*

And that the manager should go to IT to get access in the proper manner. However, in ITG2 opinions were split; one participant recognised that their files were needed

when they were not present and so could give personal access credentials to the replacement.

When asked what they themselves would do in a similar situation, responses varied from passing the responsibility to provide access on to an IT technician while one participant did say that this would be a breach of protocol:

> *For me I will not give him my password even if he is my manager because we follow protocols and those protocols say you are responsible for your passwords. [P5, ENG1]*.

When asked if the situation would be any different if it was a co-worker asking rather than a manager, participants in ENG1 and ENG2 said it would depend on the situation and the trust they have in the person asking.

When asked how they would respond to an administrator asking for a user name and password, they said they would not provide it, and would suspect that they were being tested to see if they were adhering to the stated protocols:

> *I will not give him and I will ask him to type what he wants to get and IT technician normally do not ask for username and password if they do that maybe for the test employees awareness [P4, ENG1]*.

ITG2 point out that if data is compromised it would be a problem and that if an administrator used another staff member's password it could even be considered as a crime.

In summary, the engineering department groups seemed to be aware that sharing a password with a manager would be inappropriate, but that having trust in a person making the request might encourage them to breach policy. However, the IT department groups indicated they were less likely to share stating that a password should never be shared with anyone and that anyone who has forgotten their credentials should regain access by contacting IT administration. This was also the case for sharing with co-workers or administrators.

Scenario 2: Ali has received an email that appears to have come from an IT technician asking him to go to a specific web link to confirm his personal details. What should he do?

In response to scenario 2, all participants in ENG1 agreed that Ali should not follow a link to provide personal details. The reasons for this included that it may be spam and memories that following a link had resulted in a virus in the past for staff. However, participants in ENG1 and ENG2 did consider that if they could verify the legitimacy of the request by phoning IT then they would follow the instruction.

However, participants in ENG2 were less hesitant and felt that it could be a legitimate request:

> *If he is a technician person working so we can go to that website if it is required by the college like if we need to update our data [P5, ENG2].*

ITG1 staff agreed that if staff verify the technician's request by phone then they can send the details stating that it is IT's responsibility to check the source email and whether it comes from technician or not. However, ITG2 suggested the email should be deleted and no personal information should be given. P5 (ITG2) pointed out that they have received an email from administrators telling them not to answer this type of email.

In summary, it became apparent that participants were not in agreement about whether this would be a legitimate request or not. Although some clearly knew the policy and had experienced problems. This finding is in line with the survey result that 40% would be suspicious and phone IT. This suggests that organisations not only require a security policy, but they must also ensure that staff are aware of normal forms of communication within the organisation, and that such processes are implemented consistently.

Scenario 3: Noor works in her own office, and she is going to the staff room for a short tea break time. What she should do?

Three participants in ENG1 agreed that Noor should turn off her computer screen but that it would not be necessary to shut the door. One participant in ENG2 suggested it was not necessary to lock the computer or the door, as you should have nothing personal on your computer. However, other participants in ENG2 had experienced an office breach where a student had stolen an exam paper from an office and so were more cognizant of the need to lock the office door. Participants agreed that the office door does not need to be locked if staff are mindful of locking important papers in filing cabinets.

When asked about what they would do if they were in Noor's position, they said that if they were alone or the last one out they would lock the door.

The IT department groups were adamant that the computer should be locked when leaving the desk and the office door should be locked any time the office is empty.

In summary, this scenario again pointed to trust in other people influencing people to behave in a less secure manner, unless they had personally experienced a breach of that trust. As was similarly shown with this scenario in Chapter 4, not everyone felt physical security was necessary.

Scenario 4: Ahmed wants to backup important files for the institution. When he works at home he does not have access to the institution's network – what should he do?

Participants in all groups agreed that Ahmed should back up important files, but that this should be on the hard drive or the college network and not on a commercial server such as Gmail if it is important/sensitive/confidential. However, it is permissible if the file is not important (or personal) – this raises the question of the reliability of staff assessments of a file's sensitivity.

In summary, participants were aware that they should not use personal email via commercial servers to back up sensitive data. However, there is a security weakness as they were willing to use such a process for documents they deemed non-sensitive. The process by which a document is classified as not being sensitive should therefore be made explicit within the organisation and not left to individual

opinion. In the questionnaire findings in Chapter 4, 30% of staff selected the option of sending files to their personal accounts with a further 31% asking their managers permission to do so. This raises an issue for the clarification of the sensitivity of documents.

Scenario 5: Soliman's computer is behaving strangely. He is worried that his computer has a virus. What should he do?

Participants in ENG1 and ENG2 suggested that Soliman should immediately take the computer to a technician. ENG1 suggest this will mean getting it reformatted and the software updated, while ENG2 suggest they would leave it to the technician to decide what to do. The groups said that in the same situation they would do the same thing they advised Soliman to do.

IT groups emphasised the importance of immediately cutting connection with the network with the ITG1 group suggesting this should be followed by logging off, then calling the technicians. The ITG2 suggested that the next step was to back up data and then scan the disk. This first act of cutting the connection was not recognised by the engineering groups.

In summary, most participants were aware that they should get their computers checked if they are worried they have a virus, but they were not in agreement about the exact order of steps to take and the necessity to disconnect from all networks immediately to prevent further spread. These steps should be made explicit to all employees and regularly communicated. The questionnaire findings in Chapter 4 suggest that 57% of staff would carry this out in the correct order.

Scenario 6: Mona's computer is slow and she feels that the antivirus software is slowing it. What should she do? Should she disable the antivirus?

Participants in three groups (ENG1, ENG2 and ITG1) said that Mona should not disable the antivirus. Instead they suggested that she should call the technician to have the software updated, or choose different antivirus software, or simply be more patient. However, the ITG2 group discussed disabling the antivirus temporarily if Mona needed to get on with work fast.

IT department staff stated that staff should update all software immediately and run a scan. There was a difference of opinion between engineering staff and IT staff in this situation. The engineering groups wished administrators to take responsibility, while IT staff took responsibility themselves.

In summary, participants were aware that they should not disable antivirus software but should take some exploratory measures such as updating software to see if this would improve the situation. This is in line with the questionnaire findings where 70% of staff intended not to disable the antivirus.

6.3.2 Policy and behaviour results

This section presents analysis of the second group of questions and is divided into three parts: information security awareness, ways of influencing information behaviour and advice to inform an updated information security policy.

6.3.2.1 Information security policy awareness

Table 6.1 highlights a lack of awareness of the existence and/or contents of an information security policy within the organisation. Only one group (ITG1) stated that an information security policy exists within their organisation. They acknowledge that they have not read it in its entirety, but that parts of it are communicated to them via email. It may be that other groups do not recognise that the information about security which they receive via email forms part of an overarching policy. Participants were also unable to say where they had acquired any security behaviours via a policy.

Table 6.1: Information security awareness result

	Group			
Question	**ENG1**	**ENG2**	**ITG1**	**ITG2**
Are you aware that a policy exists?	No	No	Yes	No (but will in future)
Have you read the policy?	No	No	Yes	No
Point out that they receive emails telling them what they should do in different situations, when different threats are	No	No	Yes	No

observed by the organisation.

Have you read other institutions' information security policies?	No	No	Yes	No, point out that at Google, just tick the box to say you have read it.
Provide explanation for where they find information security knowledge	No	No	Yes	No

Those in ITG1, who had read the ISP, stated that it gives good guidance on what they are expected to do. However, they pointed out things they did not like about it:

- Prohibits some services they would like to use
- Does not allow all IT needs to be fulfilled
- Prohibits some staff from installing software
- Forces staff to do things they don't want to, for example, disconnecting from the internet for an extended period of time

6.3.2.2 Ways of influencing behaviour

Regarding ways in which employee behaviour was influenced, a number of suggestions were made. First, some pointed out that their behaviour is often influenced by the interpersonal trust they have with the person requesting the behaviour. This can be positive (if the requester is promoting secure behaviour) but it can also be negative (e.g., a manager asking for something which is against policy). Participants also pointed out that work overload could lead to non-compliance, particularly if the policy got in the way of efficiency (ENG1). Participants suggested that to improve behaviour, the policy should be:

- more readily available (ENG1) (e.g., on the notice board for everyone to see);
- employees should be regularly reminded (ITG1) via email about specific behaviours (e.g., update passwords, and at the beginning of each academic year to ensure everyone is aware and up to date);

- compliance should be monitored and enforced (ITG1, ITG2).

When asked if they follow advice they have been given at work, participants (ENG2) remembered that they had been asked not to open spam email, but admitted that they may forget advice when under pressure at work.

6.3.2.3 Advice to inform an updated information security policy

Participants were asked what advice they would offer when writing a new security policy. The results are provided in Table 6.2. The focus of their advice was not to respond to suspicious emails and ensuring that the policy is kept short.

Table 6.2: Advice to offer in writing an information policy

Advice	Group
Think before you click because people click on a link which came from email without thinking and that will affect the computer.	ENG1
Employees should know the importance of the information security policy otherwise they will not follow the policy	ENG1
Employees should not respond to any unknown mail or unknown link which is delivered in your mail or whatever.	ENG2
Do not use any link which does not have any https	ENG2
Keep it short, people do not read long policies	ITG2

Participants were also asked for suggestions on how to improve security behaviour in the organisation. Suggestions ranged from improving the way the policy is developed, communicated and enforced to suggesting that the organisation should look at the way it treats its employees in general to foster loyalty and to provide sufficient support to ensure that workload is not negatively influencing behaviour, and how support can be provided in a timely fashion. The following suggestions were made:

a) Involve staff in writing the policy (ITG1)

b) Implement a good awareness campaign, kept up to date and regularly communicated – why behaviours must be adopted, results of not adopting (ENG2, ITG1, ITG2)
c) The organisation must show that they are serious about compliance (ENG1)
d) Monitor that the security policy is being followed (ITG2) and ensure that staff are aware of the consequences of not following policy (ITG1), although it is unclear if this means potential security consequences or actual personal sanctions for non-compliance.
e) Top management must be seen to follow the policy (ITG2)
f) Facilitate loyalty to the organisation (ENG1) as one participant said:

    - *Also the employees should be very much loyal to the institution they are working with so in terms of awareness, any information can be leaked when there is no loyalty and when the management does not treat employees well, there is a chance their employees will leak the information [P1, ENG1].*

g) *Provide sufficient IT resource so that this does not become a bottleneck which staff then try to find ways round (ENG1)*

6.4 Discussion

The focus group interviews with employees presents several opportunities to explore employees' information security awareness by means of understanding their organisation's ISP and the influencing factors that enhance and/or are barriers to complying with the ISP. This discussion is divided into two sections to explore factors that influence compliance with the ISP by comparing the employee survey and findings from the focus groups interviews and recommendations for successful information security behaviour.

6.4.1 Employees' understanding of their ISP and their views on compliance

This section focuses on the questions that investigated employees' information security awareness and their application of knowledge in the organisation. In addition, it explores factors which influence employees' behaviour and the

recommendations they made to enhance employees' security behaviour and make an appropriate ISP which could then lead to a successful information security environment.

The findings from the focus groups interviews show that employees believed that it is very important for the ISP to be available and updated in their organisation. In addition, all the interviewees showed their understanding of the policy which came from their organisation through emails and given that complying with policy is exceedingly important.

6.4.1.1 Comparison between employees' survey and focus groups interview findings

In this section comparisons are made between the focus groups findings and those of the studies in Chapters 3 and 4. Table 6.3 compares the focus group results with the findings from the scenario questions in Chapter 4. The results show that the participants in the focus groups presented the security awareness information effectively in most of the scenario questions.

Table 6.3: Comparison between employees' survey and focus group interviews findings

No	Scenario area	Survey findings in chapter 4 (%)	Findings from the four focus groups interviews in chapter 6 (groups)
1	Not sharing password	29	2
2	Social Engineering	33	4
3	Physical security - lock office door	41	3
4	Not backing up data in commercial email servers	35	4
5	Report the incident and react against viruses	57	4
6	Not disabling antivirus	68	3

The findings in the interviews reveal that the four groups of employees indicated they would report security threats to the IT administrators (e.g., phishing emails and incidents that occur, such as viruses in their computers). Additionally, the four

groups indicated they would not back up sensitive data to commercial email servers, such as Gmail. However, these results do not match the findings from the employee survey, where more than half advised the person in the scenario not to report security threats or incidents.

Conversely, the findings from the focus groups show that employees were willing to breach their organisation's ISP because they trust their co-workers, IT staff and system administrators and the person who has more authority in the organisation, such as managers. Typically, half of the employees would share their password with their manager, whilst a few would share their password with co-workers and administrators for several reasons, such as to do work. The findings from the focus groups support the results obtained from the employee survey which revealed that approximately half the employees thought it was acceptable to share their password with their managers, co-workers and IT staff and system administrators. The reason behind this is the trust between employees (co-worker and IT staff and system administrators) and managers. This confirms that these factors have a strong effect on employees contravening the ISP.

In addition, the focus groups showed that only one group of employees felt it is acceptable for colleagues to leave their office doors unlocked for a brief time because of a trusting environment and disabling the antivirus for a brief time because of workload. This supports the results from the employee survey, although with a lower percentage. This illustrates that some employees still fail to lock their office doors and ignore policy related to finishing work, such as disabling the antivirus.

6.4.2 Information security awareness

In general, all groups agreed that an ISP is incredibly important, which shows they are aware of information security policy. Additionally, they recommended that the ISP should be available to everybody in the organisation, kept up to date and distributed to staff. However, the results of the four focus groups interviews revealed that employees have a low level of information security awareness regarding the existence of the ISP within the organisation. This is despite IT staff and system administrators in the first study in same institution (see Chapter 3)

indicating that they send security policies to every single employee. Unfortunately, only one of the four groups mentioned the availability of their college's ISP. Furthermore, the same group revealed dissatisfaction with their organisation's policies and moreover, that they are actively against policies that ban them from downloading software from the internet.

Therefore, employee behaviour presents a challenge in ensuring ISP compliance. Trust between employees and co-workers, managers or technicians has a negative impact on employee compliance and overloads them with work. The study suggests that organisations need to explain the importance of information security more to their staff and all employees should have zero trust in relation to security. In addition, the organisation should educate employees that following policy will not reduce their productivity.

Finally, to build employees' responsibility regarding information security, the study suggests that organisations should give their employees awareness programmes and feedback with regards to ISP. Furthermore, management should be committed to the ISP, monitoring employees' security behaviour, be more serious vis-à-vis ISP compliance and treat the employees well, so as to gain loyalty at work, effective communication and sanction non-compliance.

6.5 Conclusion

In this chapter, a set of focus groups illustrated that employees are aware of the ISP and they all recommended the importance of compliance with them. However, the mere existence of a policy is insufficient to ensure compliance. Staff believe that when organisations want success in information security they should monitor employees' compliance, distribute written policies, provided employees with appropriate IT resources and effective security awareness, treat employees well to gain their loyalty at work and senior management must be committed to the policies.

Conversely, this chapter shows that, in general, the participants demonstrated that they have an appropriate level of practising information security cases via the

scenario questions. However, the result of this study revealed that managers' authority, and trust between staff could compromise compliance.

Chapter 7: DISCUSSION

This chapter provides a comprehensive discussion of the results of the research work undertaken. First, the results of the four different studies are compared, and secondly, the results are compared with the findings reported in the literature.

The purpose of this research was to identify whether or not staff exhibited intentions towards compliance with behaviours identified in ISPs, the current threats to information policy-compliant behaviours of employees within higher education institutions in Oman and to explore the factors that could motivate and barriers that could demotivate employees to comply with the information security policy. The final aim of the research is to develop recommendations to enhance an organisation's information security environment and improve their employees' ISP compliance. This chapter is divided into three parts: first, information security threats and risk assessment, in particular problems caused by employee behaviour; secondly, organisational information security culture and human factors influences on employee behaviour and thirdly, the challenges of measuring awareness and compliance intentions. Finally, a number of recommendations are made, drawing from the findings and previous studies to improve organisation information system security awareness and guide employees towards better information security decisions.

The results of the four studies suggest that a number of organisational and human factors were perceived as reasons why employees do not comply with ISPs. These factors were highlighted by participants across the four studies. The results show that the main organisational factors that employees believe influence their compliance with security policies are top management support, immediate managers, IT staff, an effective ISP, communications and information security awareness through knowledge, skills and ongoing training and awareness campaigns. In addition, an organisation should consider that measuring actual employee behaviour is very important in order to discover the actual rather than intended ISP compliance.

A number of demographic characteristics were explored. The results suggest that an employee's organisation, country of origin, length of employment, qualifications,

and the availability and understanding of an ISP have no significant effect on their scenario ISP scores. This suggests that security behaviours are being learnt and adopted, regardless of the ISP.

In contrast, employment category, gender and admin privileges show a significant but small effect. This indicates reliable differences that are worth considering in future studies. Worryingly, those with admin privileges were less likely to provide policy compliant answers to the scenario questions. In the interviews reported in Chapter 6, IT staff discussed academic staff demanding to have admin privileges even though this was against policy. Given the culture in Oman, this was a demand they felt they could not refuse. This may have resulted in people without sufficient IT security knowledge having admin rights.

Lastly, the employee survey results show different levels of compliance intentions depending on the security scenario. Therefore, we need to consider each behaviour individually and cannot treat ISP compliance as if it were a single behaviour.

7.1 Information security threats and risk assessment

Based on the previous studies in the literature and the findings from this study, employees' behaviour is a major concern for the security of organisations. Organisations are concerned by the lack of universal compliance with their information security policy. Consequently, to deal with this problem an organisation should identify internal and external information security threats by risk assessment and remove or reduce the risk (Gupta et al., 2010).

7.1.1 Security threats

Once an organisation has identified and understood the internal and external information security threats, solutions can be implemented in the workplace to deal with and mitigate the associated risk. All IT staff and system administrators in the first and third studies thought that the greatest threat to their organisations' information security was employee behaviour, a view which agrees with previous research (Jaeger, 2013), while in the questionnaire it became clear that more employees would intend to follow some security behaviours than others.

While technology helps an organisation to control access to information, monitor and detect malicious activities, human factors and the work environment remain the real foundation for information security (Colwill, 2009). To build effective and high quality information security, organisations should understand employee behaviour and how employees may be targeted (Whitman, 2004) . An organisation should focus on both technology (antivirus, firewalls, proxy servers, intrusion detection software, etc.) and identify how employees are motivated through influencing factors (knowledge and awareness, managers, co-workers, sanctions and rewards, etc.) to use that technology reliably. Users behaviour is difficult to predict but can effectively cancel out the security afforded by technology (Dodge et al., 2007).

In this work, IT staff and system administrators perceive that their organisations have up-to-date software and hardware protection from outsider threats such as firewalls, antiviruses and patches. However, most interviewees commented that, employees behave in ways that reduce the effectiveness of these technologies, just employing a range of technological solutions is insufficient to ensure information confidentiality, integrity and availability. This result is similar to Safa et al. (2015).

7.1.2 Risk assessment

IT staff and system administrators suggested that organisations should identify the sources of threats and vulnerabilities and focus more on improving employee behaviour to make their workplace more secure. As Peltier (2005a) reported previously, companies must examine their services, for example, vulnerability, risk analysis, assessments, policies, standards, procedures and business continuity planning, and subsequently, identify how each of these services supports the business objectives.

To successfully improve information system security, an organisation should clearly recognise its assets then identify the employee vulnerabilities and outsider threats. In this research the actual number of breaches could not be reliably determined from the IT staff and system administrator interviews. This is because information security management did not divulge all the incidents that may have happened at the organisation in order to protect the organisation’s reputation,

customer confidence and financial loss. As Al-Awadi (2009) reported, employees will not tell what they have done wrong. However, in this study IT staff and system administrators identified some employee behaviours that they believe cause problems for the organisation. It should be noted they were talking about other staff behaviours, rather than their own. In addition, the survey of employee behaviour intentions resulted in employees choosing options that were non-compliant, while in the focus groups employees discussed some problematic behaviour.

In this research, the IT staff and system administrators' ranked employee insecure behaviours as more important if they believed they happened regularly (e.g., inappropriately responding to phishing emails) in the workplace or because the level of risk to the organisation's information would be high if the bad behaviour persisted (e.g. sharing password). Furthermore, IT staff were willing to accept many employee behaviours which contravene the organisation's policy. This revealed the underlying organisational culture. If the IT staff accepted these behaviours, then we must question either the appropriateness of the policy (is it over strict?) or the knowledge of the IT staff (are they unaware of the risks of these behaviours they allow?).

7.1.2.1 Level of employee information security awareness

One of the steps towards understanding an organisation's information security is to explore users' information security knowledge, attitude and/or behaviours. It is impossible to evaluate employees' behaviour from their knowledge and/or attitude because the findings suggest that employees know information security policies but would not always comply with them. In addition, they believe that policy compliance is very important despite not complying themselves.

The findings of the employee survey show that almost half of employees have a lack of information security awareness (or intention to apply those skills) and they potentially do not work securely. The employee survey (across the 14 scenarios) showed overall that only 57% of employees' behaviours were ISP-compliant. This ranged from 29% of employees complying with one behaviour to 94% complying with another, depending on the individual behaviour. For example, over 80% of employees stated that they would intend to behave according to policy with regards

to reporting an incident if they had lost files, receiving phishing emails from unknown sources and not using email for commercial or personal purposes. This high level of compliance is not surprising, as losing files or personal use of email affects productivity, and there are many awareness campaigns around phishing attacks. However, not all behaviours were policy-compliant. For instance, 71% of employees would share their passwords with managers. In addition, more than 50% of the employees would send confidential files to commercial email servers, not lock their office' doors and windows when they are leaving for short time, share their passwords with IT staff and click on a link to confirm personal details.

7.1.2.2 Security incident response

Incident reporting can be used as a way of measuring employees' information security awareness levels (Parsons et al., 2014). When employees accidentally or deliberately disregard the ISP or identify any information security threats in their organisation it is their responsibility to inform the information security team. This would help the organisation to react before an incident occurs otherwise these activities could cause damage to the organisation's reputation and have other serious consequences. Spilling (2009) determined that the reasons employees do not to report incidents is because of a lack of awareness of the incident or that employees fear that non-compliance with the strict security regulations could lead to personal consequences.

The interviews of IT staff and system administrators suggest that most employees would not report a security threat until that threat happened and affected their work negatively and/or they lost important data. These findings align with the findings from the survey of employees that employees do not intend to report incidents in all cases. Most employees would inform IT staff when they lose their files or some changes happen to their computers. Additionally, in another scenario, more than two-thirds of employees will inform IT staff when they discovered the threat but only when the threat is clearly identified such as when they receive an email from an unknown sender which asks them to click on an attachment file.

However, two-thirds of employees would not inform IT staff when they received an email asking them for personal details when it appears that the e-mail came from

an administrator. Since employees do not report the threats by phishing emails that could mean they are not aware of this being an attack, or are not aware of the need to report all incidents and how this would help IT staff to reduce the consequences. Furthermore, almost half of them (43%) would not report when there are viruses in their computers.

7.2 Organisational information security culture

Organisational culture has been characterised in different ways and attributed to numbers of identifiable esteem sets, for example, administration styles, manners of decision making, communication styles, management style, rewards system, all of which help to characterize an organisation's character and norms (Tang & Zhang, 2016). Findings from the IT staff and system administrators' interviews suggest that organisational information security culture plays an important role in employees' compliance with the ISP. These factors include the availability of a proper information security policy, management support, good information security management team, good communications and the use of sanctions and rewards systems.

7.2.1 Information security policy

Whitman et al. (2001) suggest that the first step in preparing an organisation against internal and external threats is the development of an information security policy. While it has been shown here that this is not sufficient to ensure secure behaviour, it is necessary nonetheless. The IT staff and system administrators studied in this thesis stated that they are responsible for writing and implementing the information security policies for their organisations. Unfortunately, in some organisations the policies were not documented and where a policy did exist, it was not well established. An organisation's ISP should fit with its culture so as not to conflict with employee performance and organisational requirements. The IT staff and system administrator interviews suggested that employees often do not comply with the ISP because they believe doing so would reduce their work productivity and they do not have time for additional steps.

If the information security policy is not visible to employees, then it is more difficult for them to know what behaviour the policy requires. However, as the IT staff and system administrators pointed out, merely sending the policy to all staff by email is not sufficient. Moreover, the interview findings showed that ISPs were often incomplete (in terms of the types of threat they covered) and out of date. While many IT staff believe they have a suitable ISP, some employees in the focus group interviews suggested that the people responsible for creating security policy should make policies available to everyone, involve all employees in writing policies, ensure policies are up-to-date and as short as possible, and that policy compliance should be monitored. Clearly, there is still work required in developing and communicating ISPs effectively.

The above notwithstanding, the employee survey showed that the existence of an ISP had no significant effect on their compliance intentions. In addition, there was no significant difference between employees who agreed that they understood the policy and those who did not. Availability and understanding of information security policy is not sufficient to ensure compliant behaviour. This highlights the need for future research to identify where information security behaviours are being learnt from, if not the ISP.

7.2.2 Information security training and awareness

The findings from the three interview studies suggested that information security training and awareness have a significant effect on employees' intention to comply with an ISP and these findings are line with previous research (Al-Kalbani, 2017; D'Arcy & Greene, 2014; Haeussinger & Kranz, 2013; Parsons et al., 2014; Safa et al., 2015; Siponen et al., 2014; Tsohou et al., 2015).

In the current research the IT staff and system administrator interviews indicate that Omani higher education institutions often lack security awareness training. Those that did have awareness training (albeit infrequent) did see improvements in security behaviour (such as locking doors and computer screens on leaving the office). None of the organisations studied had enough trainers for the number of employees.

7.2.2.1 Knowledge and skills

When an information security policy is in place, an organisation should make sure that employees are aware of it and possess the basic skills needed to comply with it. The findings from the four studies revealed that information security knowledge and skills are perceived to be the foundation of information security and the factor that they reported having the most influence on whether employees comply with an ISP, especially when they understand the benefits of ISP compliance (see also Han et al. (2017). In addition, the interviews revealed that they believe ongoing information security awareness and training for all employees would increase the employees' information security knowledge and, it is hoped, their behaviour.

From the eight proposed influencers of actual employee behaviour, the findings suggest that knowledge was thought to be the largest influencing factor. As Mahfuth et al. (2017) suggested, the level of knowledge essentially influences information security conduct and ought to be considered as a basic factor in the viability of information security culture.

In addition, the IT staff and system administrator interviews highlighted a few incidents where awareness training about specific security issues (e.g., looking doors when leaving the office) helped to change employees' behaviour to comply with the ISP. However, this behaviour is not necessarily permanent and employees need to be regularly reminded.

IT management should make efforts to understand the organisational and employee information security culture to identify and practice motivation mechanisms to improve their employees' information security skills and practice. The survey findings show that half the employees in this study lack the confidence and skills necessary to comply with a basic information security policy. For instance, only around half of employees indicated they would create a new password and remember it without writing it down, saving it in a mobile phone or showing it to someone else, and more than 40% of them do not have the skills to deal with virus infections in their computers.

Research suggests that organisations should use different ways to communicate with employees and deliver the knowledge, for instance, through an e-learning website, video, visiting face to face, workshops, sessions, SMS messages and emails (Wood, 1995). Moreover, organisations should investigate employees' acceptance and willingness to put the training and awareness campaigning messages into practice. Similarly, Khan et al. (2011) applied different security awareness tools such as posters, newsletter articles, educational video games, group discussion and computer-based training to measure which tool best raises employees' information security awareness and changes their behaviour and found that group discussion was the most effective tool. Nowadays, employees can raise their information security awareness through participation in the organisation's social media platform (Dang-Pham et al., 2017).

The current study demonstrates how an organisation could use scenario-based questions as a continuous measure of employee security awareness (Appendix D) in the workplace and create scenario behaviour guidelines to improve security behaviour and raise awareness.

7.2.3 Management information security commitment and support

The level of information security awareness of top managers and department managers affects the information system management at the organisation (Sonnenschein et al., 2017). The data analysis from this study reveals that top management and line managers may have the second strongest effect on whether users intend to comply with an ISP. Therefore, it is recommended that organisations should make information security a priority to these people. The IT staff and system administrator interviews showed that they receive financial support and technology from top management and immediate managers but, unfortunately, those managers did not commit to enforce the ISP. When top management and immediate managers are committed to the ISP and cooperate with the information security management team this may have an effect on organisational information security culture and could influence employees to comply with the policy these findings are line with previous research which included some Omani Higher Education Institutions (Al-Kalbani, 2017).

Overall, the interviews with IT staff and system administrators reveal that most organisations have a lack of management information security support and commitment. Only a small number of participants declared that managers have good security awareness and support IT staff and system administrators to implement the security policy.

7.2.3.1 Top management support

The IT staff and system administrators believed that top management support for information security can improve the information security environment at an organisation which is consistent with other studies (Ezingeard & Bowen-Schrire, 2007; Knapp, Marshall, Rainer Jr, et al., 2006; Kwon et al., 2012). Unfortunately, some IT staff and system administrators mentioned that top management and immediate managers did not see information security as a vital issue and do not support them in enforcing the security policy on all users.

While a minority of IT staff and system administrators were authorised to apply more control over information security management, unfortunately, the majority of IT staff and system administrators were not so empowered and worked in an unacceptable organisational culture where users put them under pressure to provide more privileges than they need because they think that it is their right to have these privileges, especially managers and academic users, even though it is against information security policy. That makes it difficult for IT staff to control the devices and the network because their users are not in the organisation domain network and some of them have a direct connection to the internet. IT staff and system administrators advise that all users at an organisation should join the organisation domain network to allow them to easily control and monitor users' systems and the network. This would facilitate immediate deployment of patches and automatic updating of all software. It would also prevent users from downloading unlicensed software from the internet and disabling the antivirus software.

Top management should support IT staff and system administrators in enforcing the policy that all users join the domain and each user (managers, heads of departments and sections, deans of colleges) should have limited privileges to

access and use software and hardware in a responsible manner when they are working individually or in groups. Management can give this by supporting IT department with sufficient staff and ensuring that their voices are heard and heeded. IT staff and system administrators suggested that top management support would influence immediate managers and all end users to comply with the ISP and this finding agrees with previous research (Hu et al., 2012).

The employee survey indicated that there are significant differences in intentions to following the ISP. Those employees who have admin privileges on their systems showed lower compliance intentions than those who do not. In three scenarios, more than 30% of them would likely go against the ISP because they have the privileges to do what they want to do or they think it is correct behaviour (e.g., disabling the antiviruses on their computer, installing software from the internet and deleting shared files without permission).

The findings from this study suggest that top management should collaborate with information security management to comply with organisational information security policy and ensure that all immediate managers and end users in the organisation are complying. In addition, organisations should limit access for all end users and identify authorisation functions. For example, if a user needs elevated privileges for specific work, such as an academic staff request to download software from the internet, then they should ask a technician to do it who will check if there are any viruses, whether it is a trusted website and if the software is licensed to the person requesting the software, before it is downloaded. Finally, top management should have good communications with all managers, IT staff and end users, and communicate an up-to-date and complete picture of how information security should be managed in line with policy.

7.2.3.2 Immediate managers

Karjalainen et al. (2013) also suggested that employees of a company with operations in China and the UAE were influenced by authority (such as managers or directors). Similarly, the four studies in this thesis found that employees' information security behaviour intentions are thought to be influenced by authority such as direct managers.

The studies indicated that immediate managers, such as heads of departments and sections, are one of the most important factors in influencing employees to comply with an ISP. Moreover, they play an important role in employee behaviour because they have direct influence over enforcing organisational policies.

Furthermore, top management, immediate managers and information security management should not ask for any employees' username and passwords or put pressure on IT staff to give them admin privileges or to share their username and passwords. Unfortunately, the IT staff and system administrator interviews pointed out that this does happen in some of the organisations studied.

The IT staff and system administrators' interviews suggest that managers should be committed to the information security policy and use their authority in the right way to ensure employees comply. In addition, they ranked managers as the second most important influencing factor, after knowledge and awareness, when considering how to change employees' behaviour. Furthermore, participants thought that managers should attend awareness training sessions to make them aware of the importance of their behaviour in influencing staff behaviours and that they should lead by example.

7.2.4 Information security management team

Information security management teams must consider the human aspects of information security (Loster, 2005; Rhee et al., 2012). Furthermore, IT management should make staff in their organisation aware that information security is important to the organisation and that changes in staff behaviour can improve the organisation's information security (Herath & Rao, 2009). This was also found in this research but the IT staff and system administrators suggested that they need support from top management to get more IT staff to deliver training and awareness sessions.

Some of the IT staff and system administrators suggested that organisations should have individual information security management or a small team of security staff with the responsibility for identifying and controlling organisation security risk,

and assisting and guiding employees in avoiding information security breaches and complying with the information security policy.

The information security management team should be available and easy to communicate with to provide guidance and problem solving. Unfortunately, with one exception, the organisations studied do not have such teams to monitor security issues. The IT staff and system administrators in the one organisation that does have such a team were not satisfied with the number of staff, feeling the team's size to be insufficient for the size of the organisation and its requirements.

When comparing the overall survey results of IT staff and system administrators with the survey of employees, there is a suggestion that the employee information security behaviour is correlated with the IT staff and system administrator behaviour. Those questions where higher numbers of IT staff gave policy-compliant responses were the same questions that employees scored well on and vice versa. This suggests that some behaviours within the policy were better established than others and a first step in improving employee behaviour would be to improve the knowledge and behaviour of the IT staff.

Network administrators and security experts acknowledge that the significance of privacy, information security awareness, knowledge and behaviour among Internet users is crucial (Velki et al., 2017). Surprisingly, interviews with IT staff and system administrators found that they accepted some employees' behaviour even when that behaviour was not compliant with the ISP. For instance, the ISP does not allow anybody at an organisation to ask for usernames and passwords. However, in the survey result, IT staff and system administrators did accept sharing passwords with co-workers. Around half of IT staff and system administrators (53%) agreed that employees could give their password to their managers if managers agreed to take responsibility. They also would all accept that confidential data could be sent to a commercial email server if they were given permission from their managers and that employees could reuse a password if they changed one of the characters. In addition, 40% of IT staff and system administrators accepted that employees need not lock their doors and windows because that is not their responsibility. Similarly, some of the IT staff and system administrators admitted that they do not

close their own doors when they leave their offices for a short time because they perceive it as a trusted environment and it has become a habit for them.

This finding was unexpected and suggested that the higher education institutes should make sure that all IT staff and system administrators know all information security policy requirements and that their responsibilities for information security are clear. Clearly, there is further work required to change these levels of acceptance and habitual behaviours. First, this may require investment in awareness training about the different components of the ISP. In addition, it would be necessary to focus this training on the aspects of behaviour where employees are scoring badly, and/or behaviours are ranked as most important, rather than always going through all the behaviours. Lastly, the fact that so many staff do not comply with their policy means it might be worth looking at whether the policies should be rewritten and, if possible, simplified.

7.2.5 Communication

To improve policy compliance a continuous communication process is needed (Puhakainen & Siponen, 2010). In the current research, both interview studies suggested that poor internal communication between top management, immediate managers, the information security management team and employees was one of the possible reasons for lack of good security behaviour at most organisations. For example, IT staff and system administrators complained that employees did not report possible security incidents because they do not know how or to whom they should report the incident. Further work is required to investigate how an organisation might adopt a range of techniques to communicate more effectively with staff, such as mobile phones, social media and face-to-face meetings, rather than depending solely on email communication.

The interviews identified that email is the most frequently used communication method in the organisations between IT staff and system administrators and other users. Emails are sent from IT staff and system administrators to spread awareness of information security policies and regulations. Once a security threat is detected (such as a phishing email), either by them or reported by users, IT staff send emails to alert all users not to reply to or interact with these types of emails.

IT staff and system administrators suggest that email is not an effective tool to disseminate awareness and policies to employees, and that this should be supplemented with alternative communication methods such as visiting all departments and sections, meeting employees and talking to them face to face. All these could be scheduled by an IT security awareness team and may occur every semester, or at monthly meetings. In addition, some employees in the focus group interviews suggested that experts should share the writing of the security policy with them as that would help to increase awareness among employees and motivate them to comply with the ISP (Safa, Von Solms, & Furnell, 2016). The aim would be for these meetings to be repeated at regular intervals.

7.2.6 Sanctions and Rewards

Previous research presented in the literature review has shown mixed results regarding how effective sanctions and rewards systems are at influencing employees to behave in an ISP-compliant manner. In the current study most IT staff and system administrators recommended that sanctions should be practised to encourage employees to comply with the ISP, and half of them recommended that reward systems should also be in place to motivate compliant behaviour. In the organisations studied, no sanction or reward systems are currently implemented. However, from the eight measurements which explore employees' perceptions of what influences their behaviour, employees reported that sanctions were least likely to influence how they behave. However, Pahnila et al. (2007)found that sanctions do not affect employees' intentions to comply with security policies and rewards do not affect actual compliance behaviour. Here we see a contradiction, where IT staff feel that rewards and/or sanctions would improve employees' security behaviour, but employees do not believe they would make a difference. Further research should be undertaken to understand how sanctions and rewards systems could influence employees' ISP compliance.

7.2.7 Summary of discussion on organisational information security culture

The present study was designed to determine the level of information security awareness within higher education institutions in Oman and to identify what factors people perceived would influence their security behaviour intentions and thus

enhance the information security culture. The results suggest that employees in the organisations studied have some poor information system security behaviour intentions. Similar results were found in the Zayed University in the UAE (Rezgui & Marks, 2008).

To improve the situation, organisations should consider the following six main components of an organisation management culture. First, an organisation has to implement a strategic information security plan and consider information security as their priority. In addition, organisations should spend time and effort to identify security vulnerabilities and threats, as well as having a clear understanding of their environment and employee culture and what they are protecting.

An organisation's culture should create information security policies which are readily available, understandable, complete, up to date, and outline the organisational commitments. The organisations should create appropriate and continuous training and awareness campaigns for all users as this is necessary to improve their skill and to avoid any vulnerabilities being exploited. In addition, top management and immediate managers' commitment play a very important role in implementing information security policy. Furthermore, all the security management team should have comprehensive knowledge of the information security policy and appropriate security skills to enhance the information security environment as results show that employees' behaviour correlates positively with IT staff acceptance of behaviour. Flexibility and multiple opportunities for internal communication between all members of an organisation are required.

As the higher education institutions studied are in one country (Oman) the study suggested that IT security management from higher education institutions in Oman should meet annually or every semester to share:

a) Current information security threats;
b) Employee information security behaviour;
c) Challenges that they face in the organisations;
d) Methods and tools to evaluate and develop information security awareness levels and to improve employee ISP compliance.

Finally, a contradictory finding of this study is that IT staff and system administrators recommend sanctions and rewards systems should be brought in, while employees believe that sanctions are not likely to influence their security behaviours. This issue requires further research to resolve.

7.3 Human factors influence on users' behavioural intentions

Even if an organisation puts a robust ISP in place, ensures continuous awareness and training, has top managers and immediate managers with a strong commitment to information security, maintains good communications between all users, and has appropriate sanctions and rewards place, this still may not be sufficient to ensure ISP compliance by employees. The organisations need to understand other ways human behaviour is influenced.

Once an organisation ignores their employees' perceptions of security behaviour, it may be more difficult to change behaviour. For instance, trust and authority were found to be particularly important in this research.

Most of the IT staff and system administrators' interviews stated that employees are not aware about information security and compliance with the ISP. In addition, the results identified the reasons why employees do not comply with the ISP and that would help organisations to focus on particular factors to improve employee compliance. In addition, the IT staff and system administrator survey showed that they accepted some employee behaviours that went against the policy.

7.3.1 Trust

Most IT staff and system administrators indicated that the greatest threat to information system security in their organisations is their employees' behaviour and that means they do not trust their employees to participate effectively in security. Furthermore, employees are willing to break their organisation's information security policy because of trusting their managers or co-workers (Alotaibi & Furnell, 2016). In chapter 3 and chapter 5, IT staff and system administrators reported that they were particularly worried that employees trust their co-workers and IT staff and share their passwords with them. In addition, the results in chapter 4 and 6 confirmed that some employees would share their

passwords with their co-workers and IT staff because of trust and thus IT staff were right to be worried. This trust in IT staff and co-workers leads to poor information security protection for an organisation and sharing passwords with someone they believe to be a member of IT staff could lead to information loss through phishing attacks. Initial access (physical access and software) to an organisation is very easy to get as people trust others in their environment and so share usernames and passwords and do not lock computers screens or doors and windows when they leave their offices. Similarly, some IT staff admitted that they do not close office doors when they leave for short time because they consider education institutions to be a trusted environment.

Employees refusing to share their password with IT staff or/and co-workers or locking their computer's screen when they leave them for short time is suggesting to other staff that they do not trust them. To remove these barriers, it may be necessary to ensure that IT staff stick to policy and do not request passwords or send links in emails. However, it may also be necessary to introduce new training which helps people learn how to be confident to say no to requests which they know are a breach of the ISP.

7.3.2 Authority

In this study both employees and IT staff and system administrators suggest they find it hard to refuse requests from managers. That is, their behaviour is influenced by those in positions of authority. IT staff and system administrators suggest that managers play a very important role in establishing security compliance. For example, half of the IT staff and system administrators agreed that employees could break the policy when they got permission from their managers. However, most IT staff and system administrators agreed that employees should not share their passwords with anyone (including their managers) under any circumstances.

71% of employees surveyed selected the option to share usernames and passwords with managers because they think managers have the authority to break the organisation's ISP. This behaviour was also reported in the employee focus groups. This behaviour has the highest percentage of employees reporting non-compliance intentions in the survey. In addition, 31% of employees would send confidential

files for back-up to commercial email servers when they got permission from their managers. These cases reveal that managers influence employees to break the policy.

7.3.3 Responsibility

The results suggest that more than half the employees think that locking their office door is not their responsibility. The IT staff and system administrator interviews highlight that employees do not take responsibility for information security because most of them do not report to them when they identify any threats and others only report after the incident has occurred because it interrupted their work or caused them to lose important information.

Clearly, employees should take personal responsibility for information security and one system administrator suggested that one way may be to get employees to commit to this is by signing an agreement that they are responsible for their security behaviour and that getting permission from their managers does not negate this responsibility.

7.3.4 Productivity

The IT staff and system administrator interviews highlight that one of the reasons for some of the users failing to comply with the ISP is that they think complying will slow their performance (Hwang & Cha, 2018).From the employee survey, it was clear that some employees would break the policy to quickly get what they needed to do their job such as downloading software from the Internet and disabling antivirus software. Since some employees perceive security to be counterproductive, IT management should make sure that the ISP is fit for purpose and does not cause unnecessary delays.

7.3.5 Summary of discussion on human factors influence on employee behaviour

An organisation's security culture and human factors together influence employee compliance with the ISP. The findings of this study show that the level of trust, authority, responsibility and productivity are the main barriers to compliance. Some of these results are in agreement with Al-Awadi (2009) interview findings with

employees in Glasgow University which showed that people believed that security was someone else's problem and that individual values and beliefs, work pressure, lack of awareness, an invisible security policy, and organisational security culture are barriers to compliance.

In the current study, more than one third of employees believed that they can break the ISP:

- When they feel they can trust people at the workplace, such as IT staff and/or co-workers;
- When someone at the workplace gives authorisation, such as immediate managers;
- Because information security is not their responsibility;
- When productivity will be negatively affected.

Trust and authority were the most influential factors on employee non-compliance and this is in agreement with Al-Awadi's findings (interviews with 25 employees of the University of Glasgow in the UK) that some employees would give their password someone else when asked to do so by a manager or when they were giving it to a trusted colleague. In the current study, the levels of trust employees have in their IT staff and colleagues at work strongly influenced them to break the security policy (e.g., sharing passwords). Therefore, managers' commitment to the ISP is crucial to prevent employees being influenced by authority to break the policy.

Another important finding was that productivity at work and security responsibility influenced non-compliance. Therefore, organisations should build on the beliefs of their employees that security is not a barrier to productive work. Organisations should ensure that staff take personal responsibility for security by explaining to them the information security consequences and benefits when they adhere to or break the policy. Therefore, it is important that organisations should take into consideration all those factors and an understanding of human factors to engage employees in security policy compliance.

7.4 Chapter summary

This chapter gathered findings from the four studies and suggested that employees cannot be entirely blamed for non-ISP-compliant behaviour (either deliberately or as a result of mistakes) when their organisations do not provide:

a) Strategic security plans.
b) Ongoing awareness campaigns to all employees to increase employee knowledge. An organisation should make it clear to employees that their behaviour has a role in securing the organisation data and they should know the security benefit and consequences for themselves and the organisations. It is essential that employees work securely. In addition, an organisation should ensure that their employees understand the threats caused by trust and not taking responsibility.
c) Ongoing identification of the current security threats and specific employee security behaviour vulnerabilities and providing training for specific skills. In addition, organisations should understand employees' current behaviours to target training more efficiently rather than wasting time focusing on good behaviours that already exist.
d) An information security policy that is understandable, available, up to date, fit for the culture and continually communicated to employees through different channels such as emails, posters, E-learning, and visiting them in their workplaces.
e) Commitment of top management and immediate managers to compliance with policy, and requiring employees to adhere to policy.
f) Centralised and decentralised information security management team members. They should have appropriate knowledge about the ISP and appropriate security skills.
g) Good communications between top management, all managers, IT security management team and employees to disseminate awareness, enforce the security policy, deter potential attacks and report security threats and incidents.
h) Continuous employee behaviour measurement to identify human influences on behaviour. The IT security management should deal with

these factors in positive ways to influence employees to comply with security policy.

i) The 14 Information security scenarios could be used as guidelines (available on the organisation's websites). For example, retesting the security scenarios keeps an organisation up to date with what employees do when they face specific security conditions. The survey questionnaires in this study could be used.

Chapter 8: CONCLUSION

8.1 Introduction

This chapter summarises the research undertaken, discusses its contributions, assesses its limitations, and offers suggestions for further work.

8.2 Summary of the research and its contributions

A study of the literature revealed that organisational management and employee behaviour play very important roles in securing an organisation's information assets and researchers have proposed a range of reasons for why employees do not comply with information security policies. In addition, the security literature shows that there are still challenges and difficulties associated with measuring employee behaviour. Therefore, a reliable measure of the intended information security behaviour of a large number of employees and analysis of the factors influencing that behaviour were needed to address these gaps.

The research set out in this thesis applied qualitative and quantitative methods in four studies of a large number of employees across a range of higher education institutions in Oman. The first study conducted interviews with eight IT staff and system administrators from four institutions. The second study used questionnaires to investigate the security behavioural intentions and motivations of 503 employees from 12 Omani higher education institutions. The third study used a combination of interviews and a quantitative scenario-based questionnaire to investigate the views and behavioural intentions of 17 IT staff and system administrators. The fourth study conducted focus groups with 21 employees to explore factors that may influence their behavioural intentions with regards to compliance with information security policy.

The empirical investigations were focused on the role of management in information security and the behavioural intentions of employees, together with the factors that influence that behaviour.

The results from the four studies allowed the construction of knowledge i) about the information security culture in Omani higher education institutions, ii) about

the security awareness levels of employees at those institutions, iii) about the level of employees' behaviour intentions in relation to information security policies, and iv) about the organisational and human barriers to policy compliance.

The research showed that authority, trust, responsibility and productivity are major factors that influence the way employees approach ISP compliance. For example, because of the authority of managers, more than two-thirds of the employees surveyed demonstrated motivation to share passwords with managers under various circumstances and more than a third would share passwords with co-workers because of trust.

The results of this investigation showed that organisational and human factors influence both positively and negatively the ways employees think about their behaviour relating to information security. Finally, it was recommended that the organisational and human factors should be understood and used in the development of information security policies to ensure that they work together to improve employees' security behaviour.

8.2.1 Contributions of this research

The research makes contributions in two areas: i) to knowledge about ISP compliance and the factors that affect it and ii) to methodology in terms of how to measure employee awareness and behavioural intentions and the factors and motivational theories that underpin these.

8.2.1.1 Contributions to knowledge

The purpose of this research was to identify factors that influence employee behavioural motivation and intention in relation to information security policies in Omani higher education institutions. Information is an increasingly important organisational asset. With the rise of cybercriminal activity, keeping information secure assumes ever greater importance. One way to increase information security is to develop appropriate information security policies and to ensure that employees comply with them.

The first study conducted in this research applied qualitative and quantitative methods in multiple organisations and the results allowed the identification of the

organisational and human factor barriers to policy compliance. The contributions of the work are as follows.

The first contribution this research makes is in a novel exploration of the internal and external threats to organisations' information security through the findings of interviews and questionnaires with IT staff and system administrators from higher education institutions across Oman. They highlighted the importance of management behaviour and attitudes on employee behaviour. It was found that many employees look to management rather than to formal policies to direct their behaviour.

Secondly, the scenario-based survey (which covered a wider range of security issues than previous research) revealed that policy compliance is not a single behaviour but a spectrum of behaviours, each with its own level of compliance and that each must be addressed individually (e.g., employees sharing passwords with co-workers, IT staff or managers). The large sample size of this study (503 participants of different nationalities drawn from 12 Omani higher education institutions) gives a high degree of confidence to the results and means the findings are more transferable than those of previous research which had small sample sizes (often focusing on a single institution) and which covered a much narrower range of security issues.

The third study revealed shadow security behaviours present in the organisations. That is, behaviours that conflict with the ISP but which, nevertheless, those responsible for the policy deem as acceptable.

The four studies combined contribute to knowledge by identifying the organisational and human barriers that influence how employees think about compliance with information security policies. The organisational barriers were:

- a lack of information security awareness and training not just for employees but also for IT staff;
- a lack of support from top management to promote compliance;
- employees' immediate managers giving permission to behave in a non-compliant way;

- a lack of good communications; and
- the absence of workable sanctions for non-compliance with the ISP.

In addition, it was found that when an ISP works against the key human factors of trust, authority, responsibility and productivity, employees will tend to display strong intentions to behave in a non-compliant manner. Therefore, an organisation needs to take organisational human factors into account when developing an ISP to maximise the likelihood of compliance.

From these findings a number of recommendations were formulated to help organisations implement effective information security policies and to set up effective communication channels and information security awareness and training to increase the likelihood of compliance. A major recommendation is that IT security management adopt a module of continuous assessment of employee information security behaviour with relevant and appropriate training and skills updating to be delivered in response to the findings.

8.2.1.2 Contribution to methodology

In addition to the contributions to knowledge above, this research makes an important contribution to methodology. Studying and measuring behaviour directly is problematic because people tend to alter their behaviour when being observed. Therefore, previous studies of security policy compliance have tended to focus on knowledge or awareness only. Where researchers did attempt to study behavioural intentions through the use of scenario questions (D'Arcy, 2009; Farooq et al., 2015; Kruger et al., 2010; Vance et al., 2012), phrasing the questions in the second person (such as "what would you do in this situation?") tends to lead to participants giving the answer they think the researcher is looking for rather than what they would actually (or likely) do.

The novelty of the approach taken in this thesis lies in the indirect measurement of intended behaviour. By asking participants what a third person should do, one is able to obtain a more reliable measure of what the participants themselves would do. The instrument used in the second study was found to be a reliable way of assessing knowledge, awareness, and likely behaviour of participants in a broad

range of information security scenarios. The provision of a single policy-correct answer plus three other incorrect, but nevertheless plausible, answers also avoided the problem of there being an obvious right answer. The plausible incorrect answers were designed so as to allow the discovery of what underlying factors were influencing participants' behavioural intentions (according to Protection Motivation Theory and the Theory of Planned Behaviour). Thus, the survey instrument designed for this research is a contribution to methodology and could be applied in future research.

8.3 Limitations

The research has several limitations which need to be taken into account. First, it is recognised that a small number of institutions took part in the first interview study. The interviews were conducted with IT staff and system administrators from four higher education institutions which is a small sample relative to the number of colleges and universities in Oman. It was beyond the scope of this research to extend this study but it would be instructive to study a larger sample to obtain more transferable results.

Secondly, participants in the interviews were not willing to reveal the number of the security breaches experienced at their institutions so it was not possible to quantify the size of the problem. However, this is consistent with previous research reported in the literature which also was not able to obtain exact breach counts.

A third limitation is that the scope of this research was higher education in Oman so the results may not be applicable to organisations in other sectors or, indeed, higher education institutions in other countries. However, the wide range of nationalities involved in the study might mean the results are more transferable than first appears. Therefore, future research is needed to assess how the results compare to organisations in other sectors and countries. Doing so was beyond the scope of this research.

It should also be noted that a few institutions had only a small number of employees participate in the questionnaire survey because the research was conducted at the end of the second semester and those institutions have a long

holiday period (June – September). For future research it is recommended to consider the timing of questionnaire distribution.

8.4 Future work

Based on the results and limitations of this study, there are several directions for further work. As this research was conducted in higher education institutions in Oman, it would be useful to conduct similar studies in different types of organisation, sector, and country (such as healthcare, government ministries, companies) and compare the result with the findings of this research.

The scenarios employed in the questionnaire survey could be used to compare organisations that practice sanctions and rewards systems to see whether such systems influence employee compliance with information security policies. The research could study similar organisations that differ only in whether they have sanction or reward systems.

Conducting interviews with top and middle management would be useful to explore the challenges from their perspective and to identify ways management could positively influence compliant behaviour and how their undermining of ISPs by encouraging employees to engage in non-compliant behaviour could be stopped.

The scenario questions could also be extended to cover more areas of information security and then deployed in a wider range of organisations. The results could then be fed back in order to refine and further develop the questionnaire with a view to it being used as a standard instrument for measuring employee information security behaviour.

Finally, some of the statistically significant findings of the demographic data from the employee survey could be explored in more depth to fully understand why these differences exist. For example, why is it that nationalities, gender, age group, work experience, qualification level and whether they have more privileges or not to have significant effects on policy compliance? Some of these results, while statistically significant, nevertheless had a very small effect size, and these could be explored further. For example, why was it observed that men had higher knowledge and compliance scores than women, and why did those employees with

administrative privileges on their computers perform worse than those who did not?.

REFERENCES:

Ahlan, A. R., & Lubis, M. (2011). Information Security Awareness in University: Maintaining Learnability, Performance and Adaptability through Roles of Responsibility. Paper presented at the IEEE 7th International Conference on Information Assurance and Security (IAS) 2011; 246-250.

Ahmad, A., Hadgkiss, J., & Ruighaver, A. B. (2012). Incident Response Teams–Challenges in Supporting the Organisational Security Function. Computers & Security, 31(5), 643-652.

Ajzen, I. (1991). The Theory of Planned Behavior. Organizational behavior and human decision processes, 50(2), 179-211.

Akhunzada, A., Sookhak, M., Anuar, N. B., Gani, A., Ahmed, E., Shiraz, M., Furnell, S., Hayat, A., & Khan, M. K. (2015). Man-at-the-End Attacks: Analysis, Taxonomy, Human Aspects, Motivation and Future Directions. Journal of Network and Computer Applications, 48, 44-57.

Akers, R. (2017). *Social learning and social structure: A general theory of crime and deviance*: Routledge.

Al-Awadi, M. (2009). A Study of Employees' Attitudes Towards Organisational Information Security Policies in the Uk and Oman. (PhD), University of Glasgow, Glasgow.

Al-Kalbani, A. (2017). A Compliance Based Framework for Information Security in E-Government in Oman. (PhD), Melbourne, Australia.

Al-Mukahal, H. M., & Alshare, K. (2015). An Examination of Factors That Influence the Number of Information Security Policy Violations in Qatari Organizations. Information & Computer Security, 23(1), 102-118.

Alarifi, A., Tootell, H., & Hyland, P. (2012). A Study of Information Security Awareness and Practices in Saudi Arabia. Paper presented at the 2nd International Conference on Communications and Information Technology (ICCIT): Digital Information Management, Hammamet.

Albrechtsen, E. (2007). Computers & Security, 26(4), 276-289. doi:10.1016/j.cose.2006.11.004

Albrechtsen, E., & Hovden, J. (2010). Improving Information Security Awareness and Behaviour through Dialogue, Participation and Collective Reflection. An Intervention Study. Computers & Security, 29(4), 432-445. doi:10.1016/j.cose.2009.12.005

Alexander, C. S., & Becker, H. J. (1978). The Use of Vignettes in Survey Research. Public opinion quarterly, 42(1), 93-104.

Alfawaz, S. M. (2011). Information Security Management: A Case Study of an Information Security Culture. (PhD), Queensland University of Technology, Australia.

Aliyu, M., Abdallah, N. A. O., Lasisi, N. A., Diyar, D., & Zeki, A. M. (2010). Computer Security and Ethics Awareness among Iium Students: An

Empirical Study. Paper presented at the Computer Security and Ethics awareness among IIUM Students: An Empirical Study. Journal of Information Technology.

Alotaibi, T., & Furnell, S. (2016). Assessing Staff Acceptance and Compliance with Information Security. Advances in Communications, Electronics, Networks, Robotics and Security Volume 13, 13, 9.

Aloul, F. A. (2010). Information Security Awareness in Uae: A Survey Paper. Paper presented at the IEEE International Conference for Internet Technology and Secured Transactions (ICITST) 2010, pp. 1-6.

Anderson, C. L., & Agarwal, R. (2010). Practicing Safe Computing: A Multimedia Empirical Examination of Home Computer User Security Behavioral Intentions. MIS Quarterly, 34(3), 613-643.

Aurigemma, S., & Mattson, T. (2017). Deterrence and Punishment Experience Impacts on Isp Compliance Attitudes. Information & Computer Security, 25(4), 421-436.

Baker, W. H., Wade, H. B., Linda, W., & Wallace, L. (2007). Is Information Security under Control?: Investigating Quality in Information Security Management. IEEE Security & Privacy Magazine, 5(1), 36-44. doi:10.1109/MSP.2007.11

Baranowski, T., Cullen, K. W., Nicklas, T., Thompson, D., & Baranowski, J. (2003). Are Current Health Behavioral Change Models Helpful in Guiding Prevention of Weight Gain Efforts? Obesity research, 11(S10), 23S-43S.

Bates, D. (1990). 1., Plog F. Cultural anthropology, 3rd edn. New York: McGraw-Hill.

Beautement, A., Becker, I., Parkin, S., Krol, K., & Sasse, A. (2016). Productive Security: A Scalable Methodology for Analysing Employee Security Behaviours. Paper presented at the 12th Symposium on Usable Privacy and Security (SOUPS).

Beautement, A., Sasse, M. A., & Wonham, M. (2009). The Compliance Budget: Managing Security Behaviour in Organisations. Paper presented at the Proceedings of the 2008 workshop on New security paradigms.

Biddle, R., Chiasson, S., & Van Oorschot, P. C. (2012). Graphical Passwords: Learning from the First Twelve Years. ACM Computing Surveys (CSUR), 44(4), 19.

Bogdan, R., & Biklen, S. K. (1992). Qualitative Research for Education: An Introduction to Theory and Methods. Boston: Allyn and Bacon.

Bosworth, S., & Kabay, M. E. (2002). Computer Security Handbook. New York: John Wiley & Sons.

Boulder, C. (2010). New Webroot Survey Reveals Poor Password Practices That May Put Consumers' Identities at Risk: Retrieved from https://www.webroot.com/us/en/about/press-room/releases.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. MIS Quarterly, 34(3), 523-548.

Caputo, D. D., Pfleeger, S. L., Freeman, J. D., & Johnson, M. E. (2014). Going Spear Phishing: Exploring Embedded Training and Awareness. IEEE Security & Privacy, 12(1), 28-38. doi:10.1109/MSP.2013.106

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.

Caulfield, T., & Parkin, S. (2016). Case Study: Predicting the Impact of a Physical Access Control Intervention. Paper presented at the Proceedings of the 6th Workshop on Socio-Technical Aspects in Security and Trust.

Chipperfield, C., & Furnell, S. (2010). From Security Policy to Practice: Sending the Right Messages. Computer Fraud & Security, 2010(3), 13-19.

Choi, M. (2016). Leadership of Information Security Manager on the Effectiveness of Information Systems Security for Secure Sustainable Computing. Sustainability, 8(7), 638.

Coe, R. (2002). It's the Effect Size, Stupid: What Effect Size Is and Why It Is Important. Paper presented at the Annual Conference of the British Educational Research Association, University of Exeter, England.

Cohen, J. (1992). A Power Primer. Psychological bulletin, 112(1), 155.

Colwill, C. (2009). Human Factors in Information Security: The Insider Threat–Who Can You Trust These Days? Information Security Technical Report, 14(4), 186-196.

Conway, D., Taib, R., Harris, M., Yu, K., Berkovsky, S., & Chen, F. (2017). A Qualitative Investigation of Bank Employee Experiences of Information Security and Phishing. Paper presented at the Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017).

Coventry, L., Briggs, P., Jeske, D., & van Moorsel, A. (2014). Scene: A Structured Means for Creating and Evaluating Behavioral Nudges in a Cyber Security Environment. Paper presented at the International Conference of Design, User Experience, and Usability.

Crossler, R. E. (2010). Protection Motivation Theory: Understanding Determinants to Backing up Personal Data. Paper presented at the System Sciences (HICSS), 2010 43rd Hawaii International Conference on.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future Directions for Behavioral Information Security Research. Computers & Security, 32, 90-101.

D'Arcy, J., & Greene, G. (2014). Security Culture and the Employment Relationship as Drivers of Employees' Security Compliance. Information Management & Computer Security, 22(5), 474-489.

D'Arcy, J., & Hovav, A. (2007). Deterring Internal Information Systems Misuse. Communications of the ACM, 50(10), 113-117.

D'Arcy, J., Hovav, A., and Galletta, D. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. Information System Research, 20(1), 79-98. doi:10.1287/isre.1070.0160

Dang-Pham, D., Pittayachawan, S., & Bruno, V. (2017). Applications of Social Network Analysis in Behavioural Information Security Research: Concepts and Empirical Analysis. Computers & Security, 68, 1-15.

David, J. (2002). Policy Enforcement in the Workplace. Computers & Security, 21(6), 506-513.

Dinev, T., & Hu, Q. (2007). The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies. Journal of the Association for Information Systems, 8(7), 386.

Dodge, R. C., Carver, C., & Ferguson, A. J. (2007). Phishing for User Security Awareness. Computers & Security, 26(1), 73-80.

Drevin, L., Kruger, H. A., & Steyn, T. (2007). Value-Focused Assessment of Ict Security Awareness in an Academic Environment. Computers & Security, 26(1), 36-43. doi:10.1016/j.cose.2006.10.006

Durgin, M. (2007). Understanding the Importance of and Implementing Internal Security Measures. SANS Institute Reading Room (https://www2. sans. org/reading_room/whitepapers/policyissues/1901. php).

Eining, M. M., & Christensen, A. L. (1991). A Psycho-Social Model of Software Piracy: The Development and Test of a Model. Ethical issues in information systems, 182-188.

Eminağaoğlu, M., Uçar, E., & Eren, Ş. (2009). The Positive Outcomes of Information Security Awareness Training in Companies–a Case Study. Information Security Technical Report, 14(4), 223-229.

Eyong, B. K. (2014). Recommendations for Information Security Awareness Training for College Students. Information Management & Computer Security, 22(1), 115-126. doi:10.1108/IMCS-01-2013-0005

Ezingeard, J.-N., & Bowen-Schrire, M. (2007). Triggers of Change in Information Security Management Practices. Journal of General Management, 32(4).

Farooq, A., Isoaho, J., Virtanen, S., & Isoaho, J. (2015). Information Security Awareness in Educational Institution: An Analysis of Students' Individual Factors. Paper presented at the Trustcom/BigDataSE/ISPA, 2015 IEEE.

Fatani, H. A., Zamzami, I. F., Aydin, M., & Aliyu, M. (2013). Awareness toward Wireless Security Policy: Case Study of International Islamic University Malaysia.

Field, A. (2009). Comparing Several Means: Anova (Glm 1). In Discovering Statistics Using Spss (3rd Ed., Pp. 347-394). London: Sage: Sage publications.

Florêncio, D., & Herley, C. (2010). Where Do Security Policies Come From? Paper presented at the Proceedings of the Sixth Symposium on Usable Privacy and Security.

Flores, W. R., & Ekstedt, M. (2016). Shaping Intention to Resist Social Engineering through Transformational Leadership, Information Security Culture and Awareness. Computers & Security, 59, 26-44.

Goo, J., Yim, M.-S., & Kim, D. J. (2013). A Path Way to Successful Management of Individual Intention to Security Compliance: A Role of Organizational Security Climate. Paper presented at the System Sciences (HICSS), 2013 46th Hawaii International Conference on.

Gross, J. B., & Rosson, M. B. (2007). Looking for Trouble: Understanding End-User Security Management. Paper presented at the Proceedings of the 2007 Symposium on Computer Human interaction For the Management of information Technology.

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model. Journal of Management Information Systems, 28(2), 203-236.

Gupta, S., Bostrom, R. P., & Huber, M. (2010). End-User Training Methods: What We Know, Need to Know. ACM SIGMIS Database, 41(4), 9-39.

Haeussinger, F., & Kranz, J. (2013). Information Security Awareness: Its Antecedents and Mediating Effects on Security Compliant Behavior.

Han, J., Kim, Y. J., & Kim, H. (2017). An Integrative Model of Information Security Policy Compliance with Psychological Contract: Examining a Bilateral Perspective. Computers & Security, 66, 52-65.

Hansen, J. M., Saridakis, G., & Benson, V. (2018). Risk, Trust, and the Interaction of Perceived Ease of Use and Behavioral Control in Predicting Consumers' Use of Social Media for Transactions. Computers in Human Behavior, 80, 197-206.

Hasan, M. R., & Hussin, H. (2010). Self Awareness before Social Networking: Exploring the User Behaviour and Information Security Vulnerability in Malaysia.

Heary, C. M., & Hennessy, E. (2002). The Use of Focus Group Interviews in Pediatric Health Care Research. Journal of pediatric psychology, 27(1), 47-57.

Hellqvist, F. (2014). Design of Business Information Security Policy: A Case Study on Orebro County Council´ S Work with Information Security.

Herath, T., & Rao, H. R. (2009). Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness. Decision Support Systems, 47(2), 154-165. doi:10.1016/j.dss.2009.02.005

Hina, S., & Dominic, D. D. (2016). Information Security Policies: Investigation of Compliance in Universities. Paper presented at the 2016 3rd International Conference on Computer and Information Sciences (ICCOINS).

Hina, S., & Dominic, D. D. (2017). Need for Information Security Policies Compliance: A Perspective in Higher Education Institutions. Paper presented at the 2017 International Conference on Research and Innovation in Information Systems (ICRIIS).

Hoppe, M. J., Wells, E. A., Morrison, D. M., Gillmore, M. R., & Wilsdon, A. (1995). Using Focus Groups to Discuss Sensitive Topics with Children. Evaluation Review, 19(1), 102-114.

Hovav, A., & D'Arcy, J. (2012). Applying an Extended Model of Deterrence across Cultures: An Investigation of Information Systems Misuse in the Us and South Korea. Information & Management, 49(2), 99-110.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture. Decision Sciences, 43(4), 615-660.

Hwang, I., & Cha, O. (2018). Examining Technostress Creators and Role Stress as Potential Threats to Employees' Information Security Compliance. Computers in Human Behavior, 81, 282-293.

Ifinedo, P. (2012). Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory. Computers & Security, 31(1), 83-95. doi:10.1016/j.cose.2011.10.007

Ifinedo, P. (2014). Information Systems Security Policy Compliance: An Empirical Study of the Effects of Socialisation, Influence, and Cognition. Information & Management, 51(1), 69-79. doi:10.1016/j.im.2013.10.001

ITA. (2017). Information Technology Authority Annual Report 2016, Information Technology Authority Oman. Retrieved from https://www.ita.gov.om/ITAPortal/MediaCenter/Document_detail.aspx?NID=115

Jaeger, J. (2013). Human Error, Not Hackers, Cause Most Data Breaches. Compliance Week, 10(110), 56-57.

Janes, P. (2012). People, Process, and Technologies Impact on Information Data Loss. SANS Institute InfoSec Reading Room.

Jansen, J. (2015). Studying Safe Online Banking Behaviour: A Protection Motivation Theory Approach. Paper presented at the HAISA.

Karjalainen, M., Siponen, M., Puhakainen, P., & Sarker, S. (2013). One Size Does Not Fit All: Different Cultures Require Different Information System Security Interventions.

Karlsson, F., Hedström, K., & Goldkuhl, G. (2017). Practice-Based Discourse Analysis of Information Security Policies. Computers & Security, 67, 267-279.

Katz, F. H. (2005). The Effect of a University Information Security Survey on Instruction Methods in Information Security.

Kaur, J., & Mustafa, N. (2013). Examining the Effects of Knowledge, Attitude and Behaviour on Information Security Awareness: A Case on Sme.

Kearney, W. D., & Kruger, H. A. (2016). Theorising on Risk Homeostasis in the Context of Information Security Behaviour. Information & Computer Security, 24(5), 496-513.

Khalfan, A. M. (2004). Information Security Considerations in Is/It Outsourcing Projects: A Descriptive Case Study of Two Sectors. International Journal of Information Management, 24(1), 29-42. doi:10.1016/j.ijinfomgt.2003.12.001

Khan, B., Alghathbar, K. S., Nabi, S. I., & Khan, M. K. (2011). Effectiveness of Information Security Awareness Methods Based on Psychological Theories. African Journal of Business Management, 5(26), 10862-10868. doi:10.5897/AJBM11.067

Kirlappos, I., Parkin, S., & Sasse, M. A. (2014). Learning from "Shadow Security": Why Understanding Non-Compliance Provides the Basis for Effective Security.

Kissel, R. (2009). Small Business Information Security: The Fundamentals: DIANE Publishing.

Klahr, R., Shah, J., Sheriffs, P., Rossington, T., Pestell, G., Button, M., & Wang, V. (2017). Cyber Security Breaches Survey 2017: Main Report. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/609186/Cyber_Security_Breaches_Survey_2017_main_report_PUBLIC.pdf

Knapp, K. J., Marshall, T. E., Kelly Rainer, R., & Nelson Ford, F. (2006). Information Security: Management's Effect on Culture and Policy. Information Management & Computer Security, 14(1), 24-36.

Knapp, K. J., Marshall, T. E., Rainer Jr, R. K., & Morrow, D. W. (2006). The Top Information Security Issues Facing Organizations: What Can Government Do to Help. Network security, 1, 327.

Knapp, K. J., Morris Jr, F., Marshall, T. E., & Byrd, T. A. (2009). Information Security Policy: An Organizational-Level Process Model. Computers & Security, 28(7), 493-508.

Krueger, R. (1994). Focus Groups: A Practical Guide for Applied Research 2nd Edn Sage. Thousand Oaks CA.

Kruger, H., Drevin, L., & Steyn, T. (2010). A Vocabulary Test to Assess Information Security Awareness. Information Management & Computer Security, 18(5), 316-327.

Kruger, H. A., & Kearney, W. D. (2006). A Prototype for Assessing Information Security Awareness. Computers & Security, 25(4), 289-296. doi:10.1016/j.cose.2006.02.008

Kruger, H. A., & Kearney, W. D. (2008). Consensus Ranking–an Ict Security Awareness Case Study. Computers & Security, 27(7-8), 254-259.

Kwon, J., Ulmer, J. R., & Wang, T. (2012). The Association between Top Management Involvement and Compensation and Information Security Breaches. Journal of Information Systems, 27(1), 219-236.

Kyobe, M. (2010). Towards a Framework to Guide Compliance with Is Security Policies and Regulations in a University. Paper presented at the Information Security for South Africa (ISSA), 2010.

Lacey, D., & James, B. E. (2010). Review of Availability of Advice on Security for Small/Medium Sized Organisations. Retrieved, 2(28), 2013.

Lang, M., Devitt, J., Kelly, S., Kinneen, A., O'Malley, J., & Prunty, D. (2009). Social Networking and Personal Data Security: A Study of Attitudes and Public Awareness in Ireland.

Lebek, B., Uffen, J., Breitner, M. H., Neumann, M., & Hohler, B. (2013). Employees' Information Security Awareness and Behavior: A Literature Review.

Lee, C., Lee, C. C., & Kim, S. (2016). Understanding Information Security Stress: Focusing on the Type of Information Security Compliance Activity. Computers & Security, 59, 60-70.

Li, H., Sarathy, R., & Zhang, J. (2010). Understanding Compliance with Internet Use Policy: An Integrative Model Based on Command-and-Control and Self-Regulatory Approaches. Paper presented at the ICIS.

Liginlal, D., Sim, I., & Khansa, L. (2009). How Significant Is Human Error as a Cause of Privacy Breaches? An Empirical Study and a Framework for Error Management. Computers & Security, 28(3), 215-228.

Locke, S. D., & Gilbert, B. O. (1995). Method of Psychological Assessment, Self-Disclosure, and Experiential Differences: A Study of Computer, Questionnaire, and Interview Assessment Formats. Journal of Social Behavior and Personality, 10(1), 255.

Lohrmann, D. (2014). Ten Recommendations for Security Awareness Programs. Retrieved from http://www.govtech.com/blogs/lohrmann-on-cybersecurity/Ten-Recommendations-for-Security-Awareness-Programs.html

Loster, P. C. (2005). Managing E-Business Risk to Mitigate Loss. Financial Executive, 21(5), 43-45.

Madigan, E. M., Petrulich, C., & Motuk, K. (2004). The Cost of Non-Compliance: When Policies Fail. Paper presented at the Proceedings of the 32nd annual ACM SIGUCCS conference on User services.

Mahabi, V. (2010). Information Security Awareness: System Administrators and End-Users Perspectives at Florida State University: Florida State University.

Mahfuth, A., Yussof, S., Baker, A. A., & Ali, N. (2017). A Systematic Literature Review: Information Security Culture. Paper presented at the 2017 International Conference on Research and Innovation in Information Systems (ICRIIS).

Mahmood, M. A., Siponen, M., Straub, D., Rao, H. R., & Raghu, T. (2010). Moving toward Black Hat Research in Information Systems Security: An Editorial Introduction to the Special Issue. MIS Quarterly, 34(3), 431-433.

Marks, A., & Rezgui, Y. (2009). A Comparative Study of Information Security Awareness in Higher Education Based on the Concept of Design Theorizing.

Masrom, M., & Ismail, Z. (2008). Computer Security and Computer Ethics Awareness: A Component of Management Information System. Paper presented at the Proceedings of International Symposium on Information Technology 2008, Kuala Lumpur Convention Centre, Malaysia (26-29 August 2008).

Maynard, S., & Ruighaver, A. (2006). What Makes a Good Information Security Policy: A Preliminary Framework for Evaluating Security Policy Quality. Paper presented at the Proceedings of the fifth annual security conference, Las Vegas, Nevada USA.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual Differences and Information Security Awareness. Computers in Human Behavior, 69, 151-156.

Meso, P., Ding, Y., & Xu, S. (2013). Applying Protection Motivation Theory to Information Security Training for College Students. Journal of Information Privacy and Security, 9(1), 47-67.

Mishra, S., & Dhillon, G. (2006). Information Systems Security Governance Research: A Behavioral Perspective. Paper presented at the 1st Annual Symposium on Information Assurance, Academic Track of 9th Annual NYS Cyber Security Conference.

Mwagwabi, F., McGill, T., & Dixon, M. (2014). Improving Compliance with Password Guidelines: How User Perceptions of Passwords and Security Threats Affect Compliance with Guidelines. Paper presented at the System Sciences (HICSS), 2014 47th Hawaii International Conference on.

Myers, M. D., & Newman, M. (2007). The Qualitative Interview in Is Research: Examining the Craft. Information and Organization, 17(1), 2-26. doi:10.1016/j.infoandorg.2006.11.001

NCSC. (2015). National Cyber Security Centre. The Problems with Forcing Regular Password Expiry. Retrieved from https://www.ncsc.gov.uk/articles/problems-forcing-regular-password-expiry

Ngoqo, B., & Flowerday, S. V. (2015). Information Security Behaviour Profiling Framework (Isbpf) for Student Mobile Phone Users. Computers & Security, 53, 132-142.

North, M., George, R., & North, S. (2006). Computer Security and Ethics Awareness in University Environments: A Challenge for Management of Information Systems.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' Behavior Towards Is Security Policy Compliance. Paper presented at the System sciences, 2007. HICSS 2007. 40Th annual hawaii international conference on.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining Employee Awareness Using the Human Aspects of Information Security Questionnaire (Hais-Q). Computers & Security. doi:10.1016/j.cose.2013.12.003

Pattinson, M., Pattinson, M., Butavicius, M., Butavicius, M., Parsons, K., Parsons, K., McCormac, A., McCormac, A., Calic, D., & Calic, D. (2017). Managing Information Security Awareness at an Australian Bank: A Comparative Study. Information & Computer Security, 25(2), 181-189.

Peltier, T., R. (2005a). Implementing an Information Security Awareness Program. Information Systems Security, 14(2), 37-49. doi:10.1201/1086/45241.14.2.20050501/88292.6

Peltier, T. R. (2004). Information Security Policies and Procedures: A Practitioner's Reference (2nd edition ed.). Boca Raton, Florida: Auerbach Publications. pp.8-47

Peltier, T. R. (2005b). Information Security Risk Analysis (2 ed.). Auerbach Publications, Boca Raton, Fla.

Podsakoff, P. M., & Organ, D. W. (1986). Self-Reports in Organizational Research: Problems and Prospects. Journal of management, 12(4), 531-544.

Posey, M. C. (2010). Protection-Motivated Behaviors of Organizational Insiders: Louisiana Tech University.

Puhakainen, P., & Siponen, M. (2010). Improving Employees' Compliance through Information Systems Security Training: An Action Research Study. MIS Quarterly, 757-778.

Rader, E., Wash, R., & Brooks, B. (2012). Stories as Informal Lessons About Security. Paper presented at the Proceedings of the Eighth Symposium on Usable Privacy and Security.

Raderman, L., & Markiewicz, D. (2015). Guidelines for Data Classification. Carnegie Mellon University. Retrieved from https://www.cmu.edu/iso/governance/guidelines/data-classification.html

Ramalingam, R., Khan, S., & Mohammed, S. (2016). The Need for Effective Information Security Awareness Practices in Oman Higher Educational Institutions. arXiv preprint arXiv:1602.06510.

Rezgui, Y., & Marks, A. (2008). Information Security Awareness in Higher Education: An Exploratory Study. Computers & Security, 27(7), 241-253. doi:10.1016/j.cose.2008.07.008

Rezmierski, V. E., Seese Jr, M. R., & St Clair II, N. (2002). University Systems Security Logging: Who Is Doing It and How Far Can They Go? Computers & Security, 21(6), 557-564.

Rhee, H.-S., Kim, C., & Ryu, Y. U. (2009). Self-Efficacy in Information Security: Its Influence on End Users' Information Security Practice Behavior. Computers & Security, 28(8), 816-826. doi:10.1016/j.cose.2009.05.008

Rhee, H.-S., Ryu, Y. U., & Kim, C.-T. (2012). Unrealistic Optimism on Information Security Management. Computers & Security, 31(2), 221-232.

Rimal, R. N. (2001). Longitudinal Influences of Knowledge and Self-Efficacy on Exercise Behavior: Tests of a Mutual Reinforcement Model. Journal of Health Psychology, 6(1), 31-46.

Ritchie, J., Spencer, L., Bryman, A., & Burgess, R. (1994). Analysing Qualitative Data.

Rogers, R. W. (1983). Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation. Social psychophysiologyJ. Cacioppo and R. Petty (Eds.), Guilford, New York,, 153-176.

Safa, N. S. (2017). The Information Security Landscape in the Supply Chain. Computer Fraud & Security, 2017(6), 16-20.

Safa, N. S., & Ismail, M. A. (2013). A Customer Loyalty Formation Model in Electronic Commerce. Economic Modelling, 35, 559-564.

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information Security Conscious Care Behaviour Formation in Organizations. Computers & Security, 53, 65-78.

Safa, N. S., & Von Solms, R. (2016). An Information Security Knowledge Sharing Model in Organizations. Computers in Human Behavior, 57, 442-451.

Safa, N. S., Von Solms, R., & Furnell, S. (2016a). Information Security Policy Compliance Model in Organizations. Computers & Security, 56, 70-82.

Safa, N. S., Von Solms, R., & Futcher, L. (2016). Human Aspects of Information Security in Organisations. Computer Fraud & Security, 2016(2), 15-18.

Scholl, M. C., Fuhrmann, F., & Scholl, L. R. (2018). Scientific Knowledge of the Human Side of Information Security as a Basis for Sustainable Trainings in Organizational Practices. Paper presented at the Proceedings of the 51st Hawaii International Conference on System Sciences.

Schultz, E. (2005). The Human Factor in Security. Computers & Security, 24(6), 425-426. doi:10.1016/j.cose.2005.07.002

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' Adherence to Information Security Policies: An Exploratory Field Study. Information & Management, 51(2), 217-224.

Skinner, B. F. (2014). *Contingencies of reinforcement: A theoretical analysis* (Vol. 3): BF Skinner Foundation.

Siponen, M., Pahnila, S., & Mahmood, M. A. (2010). Compliance with Information Security Policies: An Empirical Investigation. Computer, 43(2), 64-71. doi:10.1109/MC.2010.35

Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables Influencing Information Security Policy Compliance: A Systematic Review of Quantitative Studies. Information Management & Computer Security, 22(1), 42-75.

Sommestad, T., Karlzén, H., & Hallberg, J. (2015). The Sufficiency of the Theory of Planned Behavior for Explaining Information Security Policy Compliance. Information & Computer Security, 23(2), 200-217.

Sonnenschein, R., Loske, A., & Buxmann, P. (2017). The Role of Top Managers' It Security Awareness in Organizational It Security Management.

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information Security Management Needs More Holistic Approach: A Literature Review. International Journal of Information Management, 36(2), 215-225.

Spender, J.-C. (1998). The Dynamics of Individual and Organizational Knowledge. Managerial and organizational cognition, Sage, London, 13-39.

Spilling, J. M. H. a. P. (2009). Do Organisational Security Measures Contribute to the Detection and Reporting of It-System Abuses? Proceedings of the Third International Symposium on Human Aspects of Information Security & Assurance, 71-81.

Spruit, M. (1998). Competing against Human Failing. 15th IFIP World Computer Congress. 'The Global Information Society on the Way to the Next Millennium'. SEC, TC11, Vienna.

Srivastava, A., & Thomson, S. B. (2009). Framework Analysis: A Qualitative Methodology for Applied Policy Research.

Straub, D. W., & Welke, R. J. (1998). Coping with Systems Risk: Security Planning Models for Management Decision Making. MIS Quarterly, 441-469.

Talib, S., Clarke, N. L., & Furnell, S. M. (2010). An Analysis of Information Security Awareness within Home and Work Environments. Paper presented at the Availability, Reliability, and Security, 2010. ARES'10 International Conference on.

Tang, M., & Zhang, T. (2016). The Impacts of Organizational Culture on Information Security Culture: A Case Study. Information Technology and Management, 17(2), 179-186.

Tatu, T., Ament, C., & Jaeger, L. (2018). Lessons Learned from an Information Security Incident: A Practical Recommendation to Involve Employees in Information Security. Paper presented at the Proceedings of the 51st Hawaii International Conference on System Sciences.

Teodor, S., Jonas, H., Kristoffer, L., & Johan, B. (2014). Variables Influencing Information Security Policy Compliance. Information Management & Computer Security, 22(1), 42-75. doi:10.1108/IMCS-08-2012-0045

Thomson, K.-L., von Solms, R., & Louw, L. (2006). Cultivating an Organizational Information Security Culture. Computer Fraud & Security, 2006(10), 7-11.

Thomson, M. E., & Solms, R. v. (1998). Information Security Awareness: Educating Your Users Effectively. Information Management & Computer Security, 6(4), 167-173.

Tipton, H. F., & Krause, M. (2006). Information Security Management Handbook: Auerbach.

Trevino, L. K. (1992). Experimental Approaches to Studying Ethical-Unethical Behavior in Organizations. Business Ethics Quarterly, 2(02), 121-136.

Truss, K., Soane, E., Edwards, C. Y. L., Wisdom, K., Croll, A., & Burnett, J. (2006). Working Life: Employee Attitudes and Engagement 2006: Chartered Institute of Personnel and Development.

Tsai, H.-y. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding Online Safety Behaviors: A Protection Motivation Theory Perspective. Computers & Security, 59, 138-150.

Tsohou, A., Karyda, M., & Kokolakis, S. (2015). Analyzing the Role of Cognitive and Cultural Biases in the Internalization of Information Security Policies: Recommendations for Information Security Awareness Programs. Computers & Security, 52, 128-141.

Tsohou, A., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2008). Investigating Information Security Awareness: Research and Practice Gaps. Information Security Journal: A Global Perspective, 17(5-6), 207-227. doi:10.1080/19393550802492487

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating Is Security Compliance: Insights from Habit and Protection Motivation Theory. Information & Management, 49(3), 190-198.

Velki, T., Solic, K., Gorjanac, V., & Nenadic, K. (2017). Empirical Study on the Risky Behavior and Security Awareness among Secondary School Pupils-Validation and Preliminary Results. Paper presented at the Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2017 40th International Convention on.

Vroom, C., & Von Solms, R. (2004). Towards Information Security Behavioural Compliance. Computers & Security, 23(3), 191-198.

Walsham, G. (2002). Cross-Cultural Software Production and Use: A Structurational Analysis. MIS Quarterly, 359-380.

Walton, R. (2006). Balancing the Insider and Outsider Threat. Computer Fraud & Security, 2006(11), 8-11.

Waly, N., Tassabehji, R., & Kamala, M. (2012). Improving Organisational Information Security Management: The Impact of Training and Awareness.

Whitman, M., & Mattord, H. (2012). Principles of Information Security, Course Technology

Whitman, M. E. (2004). In Defense of the Realm: Understanding the Threats to Information Security. International Journal of Information Management, 24(1), 43-57.

Whitman, M. E., Townsend, A. M., & Aalberts, R. J. (2001). Information Systems Security and the Need for Policy.

Wiant, T. L. (2005). Information Security Policy's Impact on Reporting Security Incidents. Computers & Security, 24(6), 448-459.

Wilson, M., & Hash, J. (2003). Building an Information Technology Security Awareness and Training Program. NIST Special publication , Washington, U.S. Government Printing Office 800-50.

Wood, C. (1995). Information Security Awareness Raising Methods. Computer Fraud & Security Bulletin, 1995(6), 13-15.

Zhang, P., & Li, X. (2015). Determinants of Information Security Awareness: An Empirical Investigation in Higher Education.

APPENDIX A: ETHICS PROCEDURES

1. **Confirmation ethical approval by the standard Northumbria University Ethics:**

A. First study:

- Research ethics project number: RE-EE-12-130625-51c9a4e67b604
- Date ethical approval granted: 27/03/2014

B. **Second study**

- Research ethics project number: Submission code: SUB075_Al Mahri_040615
- Date ethical approval granted: 04/06/2015

C. Third study:

- Research ethics project number: SUB037_Almahri_14.12.15
- Date ethical approval granted: 14/12/2015

2. **Build relationships with people in universities and colleges in Oman**

Site visits were undertaken to universities and colleges in Oman to establish relationships for participant recruitment. In addition, several communications tools (mobiles phones and emails) were used to communicate with authorised people in the higher education institutions.

Letter to University and colleges' Deans (for interviews)

Dear …..

I am a PhD student at Northumbria University and would like to invite you to take part in a research project to assess how individuals use computers as part of their job role.

Researchers from the Psychology and Communication Technology Lab at Northumbria University are investigating employees' attitudes and behaviour towards using computers within their workplace in higher education sectors in Oman.

This is the last study and I would like to have interview with IT and network administrators to study employee awareness of information security in Omani educational establishments.
I hope that I can have interview more than five persons and the interview will take less than 30 minutes for each one.

If you have any questions, please email me as it is shown below. This study has received full ethical approval from the Faculty of Health & Life Sciences Ethics Committee at Northumbria University. The survey is available in Arabic and English language; please choose the appropriate language from the top of the page.

Your help would be very much appreciated!

Researcher details (name, address and email)

- Letter sent to contacts (e.g. Deans and assistant Deans) in the universities and colleges in Oman for participant recruitment (Online Survey)

Dear….

I am a PhD student at Northumbria University and would like to invite you to take part in a research project to assess how individuals use computers as part of their job role.

Researchers from the Psychology and Communication Technology Lab at Northumbria University are investigating employees' attitudes and behaviour towards using computers within their workplace in higher education sectors in Oman.

If you are in full time or part time employment and use a computer as part of your job role, you are eligible to participate. Participation is anonymous and simply involves completing an online questionnaire about your computer usage. You will be asked for some basic demographic information but no identifiable information will be requested. The information you provide will only be available to the researchers at Northumbria. The questionnaire will take you between (15) to (20) minutes to be completed.

Please visit this website to take part: (The link [Only the researcher has the authorisations for this link])

If you have any questions please email me as it is shown below. This study has received full ethical approval from the Faculty of Health & Life Sciences Ethics Committee at Northumbria University. By clicking "Next", you agree to participate in this survey.

Your help would be very much appreciated!

Researcher details (name, address and email)

3. Interview procedures

Faculty of Health & Life Sciences

Project Title:

Principal Investigator:

I hereby confirm that I give consent for the following recordings to be made:

Recording	Purpose	Consent
Voice recording	Interviews will be recorded for transcription	

Clause A: I understand that other individuals may be exposed to the recording(s) and be asked to provide ratings/judgments. The outcome of such ratings/judgments will not be conveyed to me. My name or other personal information will never be associated with the recording(s).

Tick or initial the box to indicate your consent to Clause A ☐

Clause B: I understand that the recording(s) may also be used for teaching/research purposes and may be presented to students/researchers in an educational/research context. My name or other personal information will never be associated with the recording(s).

Please read and tick the box below.

The investigator has explained to me the nature of the study, and what is required from me. They have given me a debrief sheet providing me with their contact details. I understand I am free to withdraw from the study at any time, without having to give a reason for withdrawing, and without prejudice. I agree to provide information to the investigator and understand that my contribution will remain anonymous and confidential

☐

Signature ofparticipant..... Date.....……..

Signature of researcher..... Date.....……..

PARTICIPANT INFORMATION

This information sheet provides you with sufficient information so that you can then give your informed consent. It is thus very important that you read this document carefully, and raise any issues that you do not understand with the investigator.

Name of Researcher:

Name of Supervisor:

Project Title:

1. The purpose of this study is to explore the relative importance of different security behaviours, whether there are suitable alternatives and what factors you think influence whether or not a member of staff will adopt those behaviours

2. You have been asked to take part because you are a member of IT or Network administration within an Oman University or College.

3. You will be asked to rank behaviours in order of importance to security, list acceptable alternative behaviours and discuss why you think staff in your organisation do – or don't – adopt these behaviours.

4. There is no physical or psychological discomfort or embarrassment associated with this task.

5. We will ensure your confidentiality by making sure that your name or other personal information is not be associated with any information you provide. All of the information you provide will be associated with the participant code at the top of your page. Only the research team will have access to your data.

6. You will NOT receive any financial rewards / travel expenses for taking part?

7. You can withdraw your data from the study up to a month after you have taken part by emailing the researcher (email)

8. If you require any further information about this project you should email the researcher (email) or his supervisor (Name) and (email).

If you have any concerns or worries concerning this research or if you wish to register a complaint, please direct it to the Department of Psychology Ethics (Name) (Post-graduate) at the address below, or by Email:…….

The data collected in this study will be used for a Post-graduate Psychology Thesis. It may also be published in scientific journals or presented at conferences. Any information and data gathered during this research study will only be available to the research team identified in the information sheet. Should the research be presented or published in any form, all data will be anonymous (i.e. your personal information or data will not be identifiable).

All identifiable paper records will be stored in a locked filing cabinet, accessible only to the research team and all electronic information will be stored on a password-protected computer. All of the information you provide will be treated in accordance with the Data Protection Act. This information will be destroyed 6 months after completion of the project. If the research is published in a scientific journal it may be kept for up to 7 years before being destroyed. During that time the data may be used by members of the research team only for purposes appropriate to the research question, but at no point will your personal information or data be revealed.

This study and its protocol have received full ethical approval from the Department of Psychology Ethics Committee (Post-graduate) in accordance with the School of Life Sciences Ethics Committee. If you require confirmation of this please contact the (Name) of this Committee, stating the title of the research project and the name of the researcher:

Chair of Department of Psychology Ethics Committee (Post-graduate) name and address

Debrief Sheet

Name of Researcher:

Name of Supervisor:

Project Title:

The purpose of this study is to explore the relative importance of different security behaviours, whether there are suitable alternatives and what factors you think influence whether or not a member of staff will adopt those behaviours

If you would like to see the overall results of this study please email me and I will send you the summary results (Email)

The information you provided will be analysed to look for overall answers to the question of what behaviours are the most important for security. The results will form part of my PhD thesis and may be published.

You have NOT been deceived in any way during the project.

If I change my mind and wish to withdraw your data from the study, you can do so up to a month after you have taken part by emailing the researcher (Email)

If you would like to discuss any issues further please do not hesitate to contact the researcher.

If you have any concerns or worries concerning the way in which this research has been conducted, or if you have requested, but did not receive feedback from the researcher concerning the general outcomes of the study within a few months after the study has concluded, then please contact the researcher via email at (researcher email) my supervisor (Name and email) or the chair of ethics (name and email)

FOURTH STUDY: FOCUS GROUP ETHICS PROCEDURES AND QUESTIONS

Faculty of Health & Life Sciences

Project Title: EMPLOYEES' INFORMATION SECURITY AWARENESS AND BEHAVIOUR IN HIGHER EDUCATION INSTITUTIONS IN OMAN

Principal Investigator: Mohammed al-Mahri

I hereby confirm that I give consent for the following recordings to be made:

Recording	Purpose	Consent
e.g. voice recordings	Interviews will be recorded for transcription	

Clause A: I understand that other individuals may be exposed to the recording(s) and be asked to provide ratings/judgments. The outcome of such ratings/judgments will not be conveyed to me. My name or other personal information will never be associated with the recording(s).

Tick or initial the box to indicate your consent to Clause A ☐

Clause B: I understand that the recording(s) may also be used for teaching/research purposes and may be presented to students/researchers in an educational/research context. My name or other personal information will never be associated with the recording(s).

Tick or initial the box to indicate your consent to Clause B ☐

Clause C: I understand that the recording(s) may be published in an appropriate journal/textbook or on an appropriate Northumbria University webpage. My name or other personal information will never be associated with the recording(s). I understand that I have the right to withdraw consent at any time prior to publication, but that once the recording(s) are in the public domain there may be no opportunity for the effective withdrawal of consent.

Tick or initial the box to indicate your consent to Clause C ☐

Please read and tick the box below.

The investigator has explained to me the nature of the study, and what is required from me. They have given me a debrief sheet providing me with their contact details. I understand I am free to withdraw from the study at any time, without having to give a reason for withdrawing, and without prejudice. I agree to provide information to the investigator and understand that my contribution will remain anonymous and confidential	☐

Signature of participant.....
Date.....……..

Signature of researcher.....
Date.....……..

PARTICIPANT INFORMATION

This information sheet provides you with sufficient information so that you can then give your informed consent. It is thus very important that you read this document carefully, and raise any issues that you do not understand with the investigator.

Name of Researcher: Mohammed al-Mahri

Name of Supervisors: Professor Lynne Coventry, Dr Paul Vickers

Project Title: EMPLOYEES' INFORMATION SECURITY AWARENESS AND BEHAVIOURAL INTENTIONS IN HIGHER EDUCATION INSTITUTIONS IN OMAN

1. The purpose of this study is to explore different security behaviours, which are the most important and whether there are suitable alternatives. This study will also explore what factors you think influence security behaviours in your workplace.

2. You have been asked to take part because you are a member of staff within an Oman University or College.

3. You will be asked to take part in a group discussion about your organisations information security policies, what you know about them, whether you think they are good and bad and why you think people follow (or don't follow) the policy. This will take approximately 1 hour.

4. There is no physical or psychological discomfort or embarrassment associated with this task.

5. We will ensure your confidentiality by making sure that your name and institution is not associated with any information you provide. All of the information you provide will be associated with the participant code at the top of your page. Only the research team will have access to your data.

6. You will NOT receive any financial rewards / travel expenses for taking part.

7. You can leave the discussion at any time if you wish to. You can also withdraw your data from the study up to a month after you have taken part by emailing the researcher (mohammed.al.mahri <mohammed.mahri@northumbria.ac.uk>)

8. If you require any further information about this project you should email the researcher (mohammed.mahri@northumbria.ac.uk) or his supervisor Prof. Lynne Coventry (lynne.coventry@northumbria.ac.uk

If you have any concerns or worries concerning this research or if you wish to register a complaint, please direct it to the Department of Psychology Ethics Chair (Post-graduate) at the address below, or by Email: (Post-graduate)

The data collected in this study will be used for a Post-graduate Psychology Thesis. It may also be published in scientific journals or presented at conferences. Any information and data gathered during this research study will only be available to the research team identified in the information sheet. Should the research be presented or published in any form, all data will be anonymous (i.e. your personal information or data will not be identifiable).

All identifiable paper records will be stored in a locked filing cabinet, accessible only to the research team and all electronic information will be stored on a password-protected computer. All of the information you provide will be treated in accordance with the Data Protection Act. This information will be destroyed 6 months after completion of the project. If the research is published in a scientific journal it may be kept for up to 7 years before being destroyed. During that time the data may be used by members of the research team only for purposes appropriate to the research question, but at no point will your personal information or data be revealed.

This study and its protocol have received full ethical approval from the Department of Psychology Ethics Committee (Post-graduate) in accordance with the School of Life Sciences Ethics Committee. If you require confirmation of this please contact the Chair of this Committee, stating the title of the research project and the name of the researcher:

Dr Nick Neave
Chair of Department of Psychology Ethics Committee (Post-graduate)
Northumberland Building,
Northumbria University,
Newcastle upon Tyne, NE1 8ST
UK

Debrief Sheet

Name of Researcher: Mohammed al-Mahri

Name of Supervisor: Professor Lynne Coventry, Dr Paul Vickers

Project Title: Exploring the importance and acceptability of individual security tasks in Oman Higher Education Institutions

1. **The purpose of this study is to explore where people find out about security behaviours, the relative importance of different security behaviours, whether there are suitable alternatives to what is written in the policy and what factors influence whether or not a member of staff will adopt those behaviours.**

2. **If you would like to see the overall results of this study please email me and I will send you the summary results (mohammed.mahri@northumbria.ac.uk)**

3. **The information you provided will be analysed to look for overall answers to the question of what behaviours are the most important for security. The results will form part of my phd thesis and may be published.**

4. **You have NOT been deceived in any way during the project.**

5. **If I change my mind and wish to withdraw your data from the study, you can do so up to a month after you have taken part by emailing the researcher (mohammed.al.mahri <mohammed.mahri@northumbria.ac.uk>)**

6. **If you would like to discuss any issues further please do not hesitate to contact the researcher.**

7. **If you have any concerns or worries concerning the way in which this research has been conducted, or if you have requested, but did not receive feedback from the researcher concerning the general outcomes of the study within a few months after the study has concluded, then please contact Mohammed al-Mahri via email at mohammed.mahri@northumbria.ac.uk; my supervisor**

Professor Lynne Coventry (Email) or the chair of ethics (Name) (Post-graduate email)

Procedure and Interview questions with employees

1. **First Part asking them scenario questions**
    i. Fahad's manager has forgotten his password and needs some important files. He asks Fahad for his user name and password so he can continue to work. What should Fahad do?
    ii. Ali has received an email that appears to have come from an IT technician asking him to go to a specific web link to confirm his personal details. What should he do?
    iii. Noor works in her own office, and is going to the staff room for a short tea break time. What he should do?
    iv. Ahmed wants to work on an important file at home but does not have access to the institutions network at home – what should he do?
    v. Soliman's computer is behaving strangely. He is worried that his computer has a virus. What should he do?
    vi. Mona computer is slow and she feels that the anti-virus software is slowing it? What should she do?

2. **Second part ask them general question (information security policy and behaviours)**
    i. Do you have information security policy? Get a count of those who say, yes/no/don't know.
    ii. Have you ever read the information security policy of your current institution?
    iii. Have you read other information security policies? What sort of institution?
    iv. What would you say are the good and bad things about this policy?
        - Only used if they say they have read it.
    v. Where else do you get information about information security?
    vi. What do you think influences people's security behaviours at work – both positively and negatively?
    vii. What advice/behaviours do you think are important to follow at work?
    (You could give them sticky notes to write down the topics and stick on a board)
    viii. Which of these advice/behaviours do you **always** follow? Why is do you follow this advice?
    ix. Which of these advice/behaviours do you not follow **sometimes**? In what circumstance do you not follow the advice?
    x. Is there any advice/behaviours that you **never** follow? What are your reasons for this?

xi. If you were to write a new information policy for the institution what advice would you put in it and why.

xii. How do you think your organisation could improve information security behaviours?

APPENDIX B: JOB TITLES

- Job titles of employees from multiple universities and colleges in Oman

From 503 participants, around 100 of them did not type their job title. The table below shows job title for more than one participant have same job title.

No	Job title
1	Lecturer
2	Assistant lecturer
3	Assistant professor
4	Researcher
5	Head of department
6	Head of section
7	Laboratory technician
8	Technician
9	Assistant Librarian
10	Secretary
11	Coordinator
12	Accountant
13	Financial
14	Store technician
15	Writer
16	Admission and registration
17	Data entry
18	Instructor
19	Pharmacist
20	Engineer

APPENDIX C: QUANTITATIVE AND QUALITATIVE METHODS WITH IT STAFF AND SYSTEM ADMINISTRATORS

1. Quantitative method: there are two parts

Part one: Ranking the most important behaviour from 1 to 14

Security is defined as maintaining the confidentiality, integrity and availability of information and systems. Please rank the following behaviours in order of importance to security. Place the numbers 1 – 14 next to the statements, where 1 is the most important behaviour and 14 the least. Order the statements by importance for security?

Behaviour	Rank Order
Adam wants to back up a confidential file. He does not email it to his Gmail account.	
Fatima is asked to create a new username and strong password to log in to a new service at work. She makes sure she does not write it down, save it on a device or tell it to anybody.	
Fahad's manager is very busy and asks Fahad to log into the college server using his own username and password to retrieve some files for him. Fahad refuses to do this.	
Ali is having a day off and refuses to give his co-worker his password in order to access an important email he has received.	
Sami works in his own office, and makes sure he locks the door, windows, and his computer's screen takes time even if he leaves the office for a few minutes.	
Khalfan received an email that appears to have come from administrator asking him for his username and password as the IT staff want to perform some troubleshooting. He deletes it.	
Said has received an email that appears to have come from an administrator asking him to go to a specific web link to confirm his personal details. He phones the administrator to report the email as it may be a phish.	
Aisha is working on her computer when the applications windows start to move around on their own and many new windows suddenly appear. She disconnects her computer from the network and informs the IT staff.	
Badr receives an email with an attachment from an unknown source. The email says that the attachment should be opened which will get rid of the virus. He deletes the email immediately without opening the attachment	
Ahmed is very busy and has a lot of work to do. He doesn't disable the antivirus software even though he thinks it slows down his computer.	
Hasan urgently needs to install some free software that he has downloaded from the Internet for work proposes. He waits until the technician has time to check this for him.	
Noor never uses her work email for her own commercial purposes.	

Bakhit has discovered that some files are missing from his computer and some changes have happened to his computer. He informs IT staff immediately.	
Mohammed and his colleagues in the department have shared access to some files needed for a joint project. When the project is finished Mohammed asks permission from all the colleagues to delete files that are no longer required.	

Part two: Acceptable and unacceptable behaviours in your organisation

- Thinking about maintaining security, please put Y in the box if the option is an acceptable behaviour in your institution and an **N** if it is not.
- Please if there are alternative **acceptable** behaviours in your organisation or **unacceptable** behaviours relating to those scenarios please add them in the table below.

1. Adam wants to back up a confidential file and is considering emailing it to his Gmail account. What should he do?

He should send the file to his Gmail account to have more copies.	
He shouldn't send the file to his Gmail account.	
He should ask the manager's permission to send the file to his Gmail account.	
He should email the file to a trusted colleague.	

2. Fatima is asked to create a new username and strong password to log in to a new service at work but she is worried about remembering a strong password. What should she do?

She should write it on paper and put it in her drawer until she remembers it.	
She should save it in her mobile phone or computer.	
She should remember it and should not write it down, save it in mobile phone or tell anyone.	
She should use a password she has for another service but change one of the characters in it.	

3. Fahad's manager is very busy and asks him to log into the college server using his username and password to retrieve some files for him. What should he do?

He should do what his manager asks.	
He should decline the order and remind his manager that is not allowed.	
He should do this if the manager agrees to take responsibility.	
He should perform the request if the files are not sensitive.	

4. Ali is having a day off. His co-worker phones him and asks for Ali's password in order to access an important email he has received. What should he do?

He should give him his password because his co-worker is a trustworthy person.	
He should not give him his password.	
He should give him it if the email does not contain sensitive information.	
If he is a close friend it is fine to give it to him.	

5. Sami works in his own office, and sometimes locking the door, windows, and his computer's screen takes time during the working day. What he should do?

He should lockup the office or work area (doors, windows) and his computer's screen even when he leaves for just a few minutes.	
If he leaves his office for a few minutes he should not lock the door just his computer's screen.	
If his colleagues are in the office he need not lock his computer's screen.	
He should lock his computer's screen but locking up the office or work area (doors, windows) is not his responsibility.	

6. Khalfan received an email that appears to have come from administrator asking him for his username and password as the IT staff want to perform some troubleshooting. What should he do?

He should do what the IT staffs have requested.	
He should check the email's source and, if it is correct, send the information.	
He should delete the email without replying to it.	
He should reply to the sender to ask who they are.	

7. Said has received an email that appears to have come from an administrator asking him to go to a specific web link to confirm his personal details. What should he do?

Click on the link to check what is there	
Delete the email	
He should check the email's source and, if it is correct, click on the link	
Phone the administrator to report the email.	

8. Aisha is working on her computer when the applications windows start to move around on their own and many new windows suddenly appear. What should she do?

She should make sure that antivirus is on.	
She should log out of her account.	
She should disconnect her computer from the network and inform the IT staff.	
She should call her co-workers over so they can witness what is happening.	

9. Badr receives an email with an attachment from an unknown source. The email says that the attachment should be opened which will get rid of the virus. What should he do?

Open the email attachment to see what it says.	
Delete the email immediately without opening the attachment.	
Reply to the sender and ask who they are.	
Forward the email to a co-worker and ask him what to do.	

10. Ahmed wants to disable the antivirus software in his computer when he is very busy and has a lot of work to do because he thinks it slows down his computer. What he should do?

Since it is only for a short time it is OK to disable the antivirus software.	
He should not disable the antivirus software.	
He should ask the IT staff to disable the antivirus software for a short time.	
He should ask the IT staff to have administrator privileges to save time.	

11. Hasan urgently needs to install some free software that he has downloaded from the Internet for work proposes. What should he do?

He should install the software immediately if he can.	
If he cannot install the software he should ask the technician for their username and password, in order to install it himself.	
He should make sure that the software does not have a virus and then install it himself.	
He should ask a technician to install the software.	

12. Noor wants to use her email for her own commercial purposes. What should she do?

She should not use her account for personal or commercial purposes.	
She should not sell products through her university email account but it is OK to use it to reply to her customers.	
It is fine for her to use her email with attached files as people would trust her more when they see her organisation's email address.	
She can send emails without an attached file.	

13. Bakhit has discovered that some files are missing from his computer and some changes have happened to his computer. What should he do?

He might have deleted the files by mistake and so he should wait until it happens again.	
He should inform the IT staff immediately.	

It is OK if he just informs his colleagues	
If the information was not important then he should just ignore it and not tell anyone.	

14. Mohammed and his colleagues in the department have shared access to some files needed for a joint project. When the project is finished Mohammed wants to delete the files because he no longer needs them. What should he do?

He should go ahead and delete the files he has access to.	
He should ask permission from all the colleagues he works with.	
He should delete the files but make sure he saves copies onto his USB memory stick first.	
He should delete only the unimportant files.	

2. Qualitative method: Procedure and Interview questions with IT staff and system administrators

1. Why those 5 questions on the top are important and on the bottom are not important?
    a. What is your experience for what happened when employees do not comply with bottom 5 questions?
        i. For each scenario have you experience of things going wrong
        ii. Are employees reporting information security incidents to **you?**
2. What factors influence employees to comply with ISP in an organisation?
    a. From your experiences, which factors do you think would encourage the employees to change their behaviour to comply with ISP?
        i. Do you think knowledge would change employees' behaviour positively or negatively? Do you have experienced or example you have seen knowledge change users' behaviour positively or negatively or negative behaviour in specific security area?

ii. Do you think when employees comply with ISP or not would change other employees' behaviour positively or negatively in same organisation? Do you have experienced or example you have seen others change users' behaviour positively or negatively or negative behaviour in specific security area?
iii. Do you think when managers would change employees' behaviour positively or negatively? Do you have experienced or example you have seen managers change users' behaviour positively or negatively or negative behaviour in specific security area?
iv. Do you think sanctions would change employees' behaviour positively or negatively? Do you have experienced or example you have seen sanctions change users' behaviour positively or negatively or negative behaviour in specific security area?
v. Do you think rewords would change employees' behaviour positively or negatively? Do you have experienced or example you have seen rewards change users' behaviour positively or negatively or negative behaviour in specific security area?

3. What are the main barriers to not comply with the information security policy?
4. Ranking important effects on employees' behaviour such as rewards, sanctions, awareness, knowledge or managers? What are your recommendations to improve information security policy compliance at organisation?

APPENDIX D: ONLINE SURVEY

English ▾

Information Security

Introduction:

I am a PhD student at Northumbria University and would like to invite you to take part in a research project to assess how individuals use computers as part of their job role.

Researchers from the Psychology and Communication Technology Lab at

Northumbria University are investigating employees' attitudes and behaviour towards using computers within their workplace.

If you are in full time or part time employment and use a computer as part of your job role, you are eligible to participate.

Participation is anonymous and simply involves completing an online questionnaire about your computer usage. You will be asked for some basic demographic information but no identifiable information will be requested. The information you provide will only be available to the researchers at Northumbria. The questionnaire will take you between (15) to (20) minutes to be completed.

If you have any questions please email me, name and email. This study has received full ethical approval from the Faculty of Health & Life Sciences Ethics Committee at Northumbria University.

Your help would be very much appreciated!

Researcher details (name, address and email).

If you want to withdraw your data in the future (within a month of your participation) please write your usercode* (letters and numbers) to identify yourself and keep it with you. (Optional)

*Usercode:In order to match your responses across questionnaires, we ask you to provide a user code on the questionnaires. This user code does not allow us to identify you. The usercode is the first four letters of your favourite name and the last three numbers of your favourite year. For example Ahmed's favourite name is "Suleiman" and favourite year is "1990". Ahmed's usercode would be (SULE990). But please make sure it is memorable as you will be asked to write it for withdrawal your data.

English ▼

Information Security

Introduction:

I am a PhD student at Northumbria University and would like to invite you to take part in a research project to assess how individuals use computers as part of their job role.
Researchers from the Psychology and Communication Technology Lab at
Northumbria University are investigating employees' attitudes and behaviour towards using computers within their workplace.
If you are in full time or part time employment and use a computer as part of your job role, you are eligible to participate.
Participation is anonymous and simply involves completing an online questionnaire about your computer usage. You will be asked for some basic demographic information but no identifiable information will be requested. The information you provide will only be available to the researchers at Northumbria. The questionnaire will take you between (15) to (20) minutes to be completed.
If you have any questions please email me, name and email. This study has received full ethical approval from the Faculty of Health & Life Sciences Ethics Committee at Northumbria University.
Your help would be very much appreciated!
Researcher details (name, address and email).

If you want to withdraw your data in the future (within a month of your participation) please write your usercode* (letters and numbers) to identify yourself and keep it with you. (Optional)

*Usercode:In order to match your responses across questionnaires, we ask you to provide a user code on the questionnaires. This user code does not allow us to identify you. The usercode is the first four letters of your favourite name and the last three numbers of your favourite year. For example Ahmed's favourite name is "Suleiman" and favourite year is "1990". Ahmed's usercode would be (SULE990). But please make sure it is memorable as you will be asked to write it for withdrawal your data.

#General Information:
- Please answer all questions below and thank you for participating in this research study

A) Organisation's name (University or College)

B) Category
- ❍ Academic
- ❍ Non-Academic

C) Job title (option)

D) What is your nationality?

E) What is your gender?
- ❍ Male
- ❍ Female

F) Please indicate your age group?
- ❍ 18-25 years
- ❍ 26-35 years
- ❍ 36-45 years
- ❍ 46-55 years
- ❍ 56-65 years
- ❍ 66 years or more

G) How many years have you worked at this organisation for?
- ❍ less than 1 year
- ❍ 1-5 years
- ❍ 6-10 years
- ❍ 11-15 years
- ❍ 16-20 years
- ❍ 21 years or more

H) What is your highest qualification level?

- ❍ High school
- ❍ Diploma
- ❍ Bachelor's degree
- ❍ Master's degree
- ❍ Doctorate

Other _____

I) Do you have administrator privileges in your organisation's network*?

*Note: administrator privileges allows you to disable antivirus and download software from the internet and run on your organisation's network.

- ❍ Yes
- ❍ No

J) Does your organisation have an information security policy*?

*Note: This outlines how you should use your computer and protect the organisation's information

- ❍ Yes
- ❍ No
- ❍ I don't know

***Note: Display This Question:**

If J) Does your organisation have an information security policy? Yes Is Selected

K) Please answer the following regarding Information security policy

	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
1. I understand the rules and regulations prescribed by the information security policy of my organisation.	❍	❍	❍	❍	❍

 # Questions about employees' behavior towards information security & what influences behaviours

- Please answer each of the following questions by selecting the answer that you think is correct. Select only one answer for each question.

1. Adam wants to back up a confidential file and is considering emailing it to his Gmail account. What should he do?

a) He should send the file to his Gmail account to have more copies.

b) He shouldn't send the file to his Gmail account.

c) He should ask the director's permission to send the file to his Gmail account.

d) He should email the file to a trusted colleague.

1.1 Thinking about your previous answer:

	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
1. I believe that this is the right way to behave in this situation	○	○	○	○	○
2. I believe this action will keep information secure	○	○	○	○	○
3. I believe that this is how other people in my organisation would behave	○	○	○	○	○
4. I believe this is how my manager would want me to behave	○	○	○	○	○
5. I believe this is what my organisation policy says I should do	○	○	○	○	○
6. I believe I will always behave in this way	○	○	○	○	○
7. I believe there would be disciplinary actions if I did not behave in this way	○	○	○	○	○
8. I believe there will be benefits to me if I behave in this way	○	○	○	○	○

2. Fatima is asked to create a new username and strong password to log in to a new service at work but she is worried about remembering a strong password.What should she do?

a) She should write it on paper and put it in her drawer until she remembers it.

b) She should save it in her mobile phone or computer.

c) She should try to remember it and not write it down, save it in mobile phone or not show it to anyone.

d) She should use a password she has for another service but change one of the characters in it.

2.1 Thinking about your previous answer:

	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
1. I believe that this is the right way to behave in this situation	O	O	O	O	O
2. I believe this action will keep information secure	O	O	O	O	O
3. I believe that this is how other people in my organisation would behave	O	O	O	O	O
4. I believe this is how my manager would want me to behave	O	O	O	O	O
5. I believe this is what my organisation policy says I should do	O	O	O	O	O
6. I believe I will always behave in this way	O	O	O	O	O
7. I believe there would be disciplinary actions if I did not behave in this way	O	O	O	O	O
8. I believe there will be benefits to me if I behave in this way	O	O	O	O	O

3. Fahad's manager is very busy and asks him to log into the college server using his username and password to retrieve some files for him. What should he do?

a) He should do what his manager asks.

b) He should decline the order and remind his manager that is not allowed.

c) He should do this if the manager agrees to take responsibility.

d) He should perform the request if the files are not sensitive.

3.1 Thinking about your previous answer:

	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
1. I believe that this is the right way to behave in this situation	O	O	O	O	O
2. I believe this action will keep information secure	O	O	O	O	O
3. I believe that this is how other people in my organisation would behave	O	O	O	O	O
4. I believe this is how my manager would want me to behave	O	O	O	O	O
5. I believe this is what my organisation policy says I should do	O	O	O	O	O
6. I believe I will always behave in this way	O	O	O	O	O
7. I believe there would be disciplinary actions if I did not behave in this way	O	O	O	O	O
8. I believe there will be benefits to me if I behave in this way	O	O	O	O	O

4. Ali is having a day off. His co-worker phones him and asks for Ali's password in order to access an important e-mail he has received. What should he do?

a) He should give him his password because his co-worker is a trustworthy person.

b) He should not give him his password.

c) He should give him it if the email does not contain sensitive information.

d) If he is a close friend it is fine to give it to him.

4.1 Thinking about your previous answer:

	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
1. I believe that this is the right way to behave in this situation	O	O	O	O	O
2. I believe this action will keep information secure	O	O	O	O	O
3. I believe that this is how other people in my organisation would behave	O	O	O	O	O
4. I believe this is how my manager would want me to behave	O	O	O	O	O
5. I believe this is what my organisation policy says I should do	O	O	O	O	O
6. I believe I will always behave in this way	O	O	O	O	O
7. I believe there would be disciplinary actions if I did not behave in this way	O	O	O	O	O
8. I believe there will be benefits to me if I behave in this way	O	O	O	O	O

5. Sami works in his own office, and sometimes locking the door, windows, and his computer's screen takes time during the working day. What he should do?

a) He should lock-up the office or work area (doors, windows) and his computer's screen even when he leaves for just a few minutes.

b) If he leaves his office for just a few minutes he should not lock the door just his computer's screen.

c) If his colleagues are in the office he need not lock his computer's screen.

d) He should lock his computer's screen but locking up the office or work area (doors, windows) is not his responsibility.

5.1 Thinking about your previous answer:

	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
1. I believe that this is the right way to behave in this situation	O	O	O	O	O

2. I believe this action will keep information secure					
3. I believe that this is how other people in my organisation would behave					
4. I believe this is how my manager would want me to behave					
5. I believe this is what my organisation policy says I should do					
6. I believe I will always behave in this way					
7. I believe there would be disciplinary actions if I did not behave in this way					
8. I believe there will be benefits to me if I behave in this way					

6. Khalfan received an email that appears to have come from administrator asking him for his username and password as the IT staff want to perform some troubleshooting. What should he do?

a) He should do what the IT staff have requested.

b) He should check the email's source and, if it is correct, send the information. c) He should delete the email without replying to it.

d) He should reply to the sender to ask who they are.

6.1 Thinking about your previous answer:

	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
1. I believe that this is the right way to behave in this situation					
2. I believe this action will keep information secure					
3. I believe that this is how other people in my organisation would behave					
4. I believe this is how my manager would want me to					

5. I believe this is what my organisation policy says I should do	○	○	○	○	○
6. I believe I can always behave in this way	○	○	○	○	○
7. I believe there would be disciplinary actions if I did not behave in this way	○	○	○	○	○
8. I believe there will be benefits to me if I behave in this way	○	○	○	○	○

7. Said has received an e-mail that appears to have come from an administrator asking him to go to a specific web link to confirm his personal details. What should he do?

a) Click on the link to check what is there

b) Delete the email

c) He should check the email's source and, if it is correct, click on the link.

d) Phone the administrator to report the email.

7.1 Thinking about your previous answer:

	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
1. I believe that this is the right way to behave in this situation	○	○	○	○	○
2. I believe this action will keep information secure	○	○	○	○	○
3. I believe that this is how other people in my organisation would behave	○	○	○	○	○
4. I believe this is how my manager would want me to behave	○	○	○	○	○
5. I believe this is what my organisation policy says I should do	○	○	○	○	○
6. I believe I will always behave in this way	○	○	○	○	○

7. I believe there would be disciplinary actions if I did not behave in this way	O	O	O	O	O
8. I believe there will be benefits to me if I behave in this way	O	O	O	O	O

8. Aisha is working on her computer when the applications windows start to move around on their own and many new windows suddenly appear. What should she do?

a) She should make sure that anti-virus is on.

b) She should log out of her account.

c) She should disconnect her computer from the network and inform the IT staff.

d) She should call her co-workers over so they can witness what is happening.

8.1 Thinking about your previous answer:

	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
1. I believe that this is the right way to behave in this situation	O	O	O	O	O
2. I believe this action will keep information secure	O	O	O	O	O
3. I believe that this is how other people in my organisation would behave	O	O	O	O	O
4. I believe this is how my manager would want me to behave	O	O	O	O	O
5. I believe this is what my organisation policy says I should do	O	O	O	O	O
6. I believe I will always behave in this way	O	O	O	O	O
7. I believe there would be disciplinary actions if I did not behave in this way	O	O	O	O	O
8. I believe there will be benefits to me if I behave in this way	O	O	O	O	O

9. Badr receives an e-mail with an attachment from an unknown source. The email says that the

attachment should be opened which will get rid of the virus. What should he do?

a) Open the e-mail attachment to see what it says.

b) Delete the email immediately without opening the attachment.

c) Reply to the sender and ask who they are.

d) Forward the email to a co-worker and ask him what to do.

9.1 Thinking about your previous answer:

	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
1. I believe that this is the right way to behave in this situation	O	O	O	O	O
2. I believe this action will keep information secure	O	O	O	O	O
3. I believe that this is how other people in my organisation would behave	O	O	O	O	O
4. I believe this is how my manager would want me to behave	O	O	O	O	O
5. I believe this is what my organisation policy says I should do	O	O	O	O	O
6. I believe I will always behave in this way	O	O	O	O	O
7. I believe there would be disciplinary actions if I did not behave in this way	O	O	O	O	O
8. I believe there will be benefits to me if I behave in this way	O	O	O	O	O

10. Ahmed wants to disable the antivirus software in his computer when he is very busy and has a lot of work to do because he thinks it slows down his computer. What he should do?

a) Since it is only for a short time it is OK to disable the antivirus software.

b) He should not disable the anti-virus software.

c) He should ask the IT staff to disable the anti-virus software for a short time.

d) He should ask the IT staff to have administrator privileges to save time.

10.1 Thinking about your previous answer:

	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
1. I believe that this is the right way to behave in this situation	○	○	○	○	○
2. I believe this action will keep information secure	○	○	○	○	○
3. I believe that this is how other people in my organisation would behave	○	○	○	○	○
4. I believe this is how my manager would want me to behave	○	○	○	○	○
5. I believe this is what my organisation policy says I should do	○	○	○	○	○
6. I believe I will always behave in this way	○	○	○	○	○
7. I believe there would be disciplinary actions if I did not behave in this way	○	○	○	○	○
8. I believe there will be benefits to me if I behave in this way	○	○	○	○	○

11. Hasan urgently needs to install some free software that he has downloaded from the Interne t for work proposes. What should he do?

a) He should install the software immediately if he can.

b) If he cannot install the software he should ask the technician for their username and password, in order to install it himself.

c) He should make sure that the software does not have a virus and then install it himself.

d) He should ask a technician to install the software.

11.1 Thinking about your previous answer:

	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
	○	○	○	○	○

1. I believe that this is the right way to behave in this situation					
2. I believe this action will keep information secure					
3. I believe that this is how other people in my organisation would behave					
4. I believe this is how my manager would want me to behave					
5. I believe this is what my organisation policy says I should do					
6. I believe I will always behave in this way					
7. I believe there would be disciplinary actions if I did not behave in this way					
8. I believe there will be benefits to me if I behave in this way					

12. Noor wants to use her e-mail for her own commercial purposes.What should she do?

a) She should not use her account for personal or commercial purposes.

b) She should not sell products through her university email account but it is OK to use it to reply to her customers.

c) It is fine for her to use her email with attached files as people would trust her more when they see her organisation's email address.

d) She can send emails without an attached file.

12.1 Thinking about your previous answer:

	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
1. I believe that this is the right way to behave in this situation					
2. I believe this action will keep information secure					
3. I believe that this is how other people in my organisation would behave					

4. I believe this is how my manager would want me to behave	○	○	○	○	○
5. I believe this is what my organisation policy says I should do	○	○	○	○	○
6. I believe I will always behave in this way	○	○	○	○	○
7. I believe there would be disciplinary actions if I did not behave in this way	○	○	○	○	○
8. I believe there will be benefits to me if I behave in this way	○	○	○	○	○

13. Bakhit has discovered that some files are missing from his computer and some changes have happened to his computer. What should he do?

a) He might have deleted the files by mistake and so he should wait until it happens again.

b) He should inform the IT staff immediately.

c) It is OK if he just informs his colleagues

d) If the information was not important then he should just ignore it and not tell anyone.

13.1 Thinking about your previous answer:

	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
1. I believe that this is the right way to behave in this situation	○	○	○	○	○
2. I believe this action will keep information secure	○	○	○	○	○
3. I believe that this is how other people in my organisation would behave	○	○	○	○	○
4. I believe this is how my manager would want me to behave	○	○	○	○	○
5. I believe this is what my organisation policy says I should do	○	○	○	○	○

6. I believe I will always behave in this way	○	○	○	○	○
7. I believe there would be disciplinary actions if I did not behave in this way	○	○	○	○	○
8. I believe there will be benefits to me if I behave in this way	○	○	○	○	○

14. Mohammed and his colleagues in the department have shared access to some files needed for a joint project. When the project is finished Mohammed wants to delete the files because he no longer needs them. What should he do?

a) He should go ahead and delete the files he has access to.

b) He should ask permission from all the colleagues he works with.

c) He should delete the files but make sure he saves copies onto his USB memory stick first.

d) He should delete only the unimportant files.

14.1 Thinking about your previous answer:

	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
1. I believe that this is the right way to behave in this situation	○	○	○	○	○
2. I believe this action will keep information secure	○	○	○	○	○
3. I believe that this is how other people in my organisation would behave	○	○	○	○	○
4. I believe this is how my manager would want me to behave	○	○	○	○	○
5. I believe this is what my organisation policy says I should do	○	○	○	○	○
6. I believe I will always behave in this way	○	○	○	○	○
7. I believe there would be disciplinary actions if I did not behave in this way	○	○	○	○	○
8. I believe there will be benefits to me if I behave in this way	○	○	○	○	○

PARTICIPANT DEBRIEF

Title of project: Exploring Employees' Information Security Awareness in Higher Education in Oman

Principal investigator: (researcher name)

Email: (researcher email)

1. What was the purpose of the project?

The aim of this research is to study employees' behaviour in information security in the workplace within the higher education sector in Oman.

2. How will I find out about the results?

If you have left contact details with the research team, you will be sent a summary of the findings within eight weeks of completing the research.

3. What will happen to the information I have provided?

Your data will be stored safely, will remain confidential and will be destroyed after 7 years. If required, the data from this project may be shared amongst the members of the research team but only for the purpose specified in the information sheet and consent forms. In all cases confidentiality will be ensured and you will not be personally identified.

4. How will the results be disseminated?

The data from this project might be published in a scientific journal or may be presented at conferences. The data may also be presented to peers at this and other Universities. All data will be generalised, and your data/personal information will not be identifiable.

5. If I change my mind and wish to withdraw the information I have provided, how do I do this?

If, for any reason, you wish to withdraw your data please contact the investigator at the email address above within a month of your participation and you will be asked for your usercode to identify your data. After this date, it may not be possible to withdraw your individual data as the results may already have been published. As all data are anonymised, your individual data will not be identifiable in any way.

If you have any concerns or worries concerning the way in which this research has been conducted, or if you have requested, but did not receive feedback from the principal investigator concerning the general outcomes of the study within a few weeks after the study has concluded, then please contact Chair of the School Ethics Committee, Dr XXXXX via email at XXXXXX.

Please print the page and keep it for you record (optional).