UNIVERSITY OF SOUTHERN QUEENSLAND

PSYCHOLOGICAL THEORIES AND THEIR APPLICABILITY IN RESOLVING ISSUES WITH UNAUTHRORISED COMPUTER ACCESS

A Dissertation submitted by

Angela A M Howard

For the award of

Master of Business Research

2011

Abstract

Literature has shown that technical solutions are not completely successful in securing information systems from intruders. Previous attempts to develop hacker profiles are still incomplete and time consuming to apply. Prior studies in social engineering and expectancy theory have shown that they can address some of the issues organisations are encountering, especially in employees disclosing sensitive organisational data. Therefore, using these studies in an organisational context may provide clues to how the disclosure of information can be contained. This aspect was posited in the main research question:

How can education affect the process of preventing social engineering to minimise the success of unauthorised intrusion?

While answering the main research question, due to time constraints, this study focussed only on social engineering as the main cause of disclosing organisational data. This aspect was determined using psychological theories and their applicability in resolving issues with unauthorised computer access. Qualitative approach was used as the main data collection technique and two focus groups were employed in collecting data. The University of Southern Queensland was used as the case organisation and suitable samples were drawn for a 2 x 90-minute focus group sessions. The qualitative data were analysed using two prominent text analysis applications, namely, Leximancer 3.5 and NVivo 8.

This qualitative data analysis identified 5 crucial themes. These themes are security awareness, unauthorised access, social engineering, policies and procedures, and education. It is inferred from the data that changes in the way policies and procedures implemented can have marked improvement in security aspects, especially in containing the leakage of organisational data. Thus, this research can assert that a change in policies and procedures can have an impact on unauthorised access.

New findings of the study include that staff are proactively looking for more secure ways in their processing and creating new procedures as they go, and that there seems to be a disconnect between access to information systems and the organisational data. Future research can expand on the model created for this research and focus on expectancy theory as well as quantitative methodology so that outcomes can be generalised.

CERTIFICATION OF DISSERTATION

I certify that the ideas, data collection, data analysis, discussion and conclusion reported in this dissertation are entirely my own effort, except where otherwise acknowledged. I also certify that the work is original and has not been previously submitted for any other award, except where otherwise acknowledged.

____________________________________ ______________________

Signature of Candidate Date

ENDORSEMENT

_____________________________________ _______________________

Signature of Supervisor Date

_____________________________________ _______________________

Signature of Associate Supervisor Date

Acknowledgements

I would like to use this opportunity to thank those people who have assisted me throughout this research dissertation.

My first appreciation goes to my supervisor Professor Raj Gururajan. It is through his support and expertise that I was able to make it through this dissertation. Guiding me through the early stages to find my feet, making the call to the Chief Information Officer was a first step in finding participants for the data collection, and answering the many questions I had. Raj’s reassurance, that I was on the right track with my dissertation, gave me the confidence to continue and complete this dissertation.

I would also like to thank my Associate supervisor Dr Abdul Hafeez-Baig, who was always there to provide support and encouragement, sharing his experience with focus groups and sitting in on the focus groups to support me.

Both my supervisors have allowed me the freedom to find my way while making sure that I did not get lost and have nurtured my growth in developing my research skills.

I would like to thank all staff members and students, whom I cannot name due to privacy and confidentiality, who have participated in the focus groups, for their generosity of sharing their experience and taking the time to participate.

I would like to thank Liz Whatson, for providing all administrative guidelines and kind reminders to keep me enrolled each semester.

I would like to thank Chris O’Reilly who, with her proof reading and feedback, has supported me in the last fiddly steps of completing this dissertation.

I would also like to thank Dr Dave Roberts, who planted the seeds for this study and encouraged me to combine my two passions, Information Technology and Psychology. My thanks also go to Dr Wui-Gee Tan, who pointed me towards books for my literature review.

However, much appreciation goes to my husband, Srecko Howard, who has fully supported my decision to undertake this study and endured the stressful times when I did not think I could keep going. I am very lucky to have had his support – without that I would have never started this research. It was his believe in me being able to complete this study that got me this far.

Table of Contents

Table of Figures

Table of Tables

1 Introduction

1.1 Background to the study

This is a dissertation for the Masters of Business Research, conducted at the University of Southern Queensland. The scope of this chapter is restricted to the problem of unauthorised access and the challenges with current solutions. The chapter also highlights the importance of the study and provides justification for the research. The research approach is then described, followed by an overview of the dissertation layout.

1.1.1 Description of the problem

Information systems have become an integral part of how organisations conduct their business (Choi et al. 2008). This is partly driven by the ability to access worldwide networks of varying computer systems and network infrastructures (Smith & Rupp 2002). Over time, access to the Internet has become easier and faster (Kwai-Sang et al. 2006; Smith & Rupp 2002), supporting the uptake (Oates 2001) of information systems to allow organisations to connect to other organisations and individuals. However, Kollmann et al. (2009) found that cultural differences either inhibit or drive the adoption process of information systems.

The continuing drive for easy access and better connectivity to the Internet has created a separate dilemma, namely, the vulnerability of unauthorised access (Nasheri 2003; Smith & Rupp 2002). Unauthorised access occurs when a person gains access to a computer system without having been given permission to do so (Walden 2005). While there is a possibility that this could happen by mistake, the majority of these instances occur with intention (Walden 2005).

Prior research and development of Intrusion Detection Systems (IDS) (Ragsdale et al.) and Intrusion Prevention Systems (IPS) (Fitzgerald & Dennis 2009) has been unsuccessful in providing strategies to eliminate the risk of unauthorised access (Smith 2004a). Despite continuing efforts to improve these systems by improving the underlying algorithms, unauthorised access continues unabated (Farid & Rahman 2010).

With these technical solutions failing to keep intruders out, some researchers realised the need to expand current knowledge on unauthorised access to determine the motivation behind the person causing the problem, namely the hacker. For this purpose the area of criminal profiling seemed ideal (Chantler 1995; Rogers 2006). The result consists of complex frameworks, categories, taxonomies, circumplex, and models that require

Information Technology (IT) security specialists to implement possible solutions to thwart access to organisational computing networks by hackers (Botha & von Solms 2001; Chantler 1995; Fötinger & Ziegler 2004; Kjaerland 2005; Kleen 2001; Rogers 1999, 2006).

Recently, a more managerial view considered that there is a gap in security that relates to human behaviour as a possible cause of unauthorised access, positing that some of the practices may put an organisation at risk (Choi et al. 2008). Choi et al. (2008) identified the need to raise security awareness within organisations at management level, and found that when all levels of management are security-aware, a higher chance exists that security measures are implemented into the various processes and practices of an organisation. Additionally, they suggested that the human aspect should be considered as a weak link in the chain of security. The level of security may impact on whether an intruder can successfully penetrate security as a result of an employee unwittingly divulging information (Choi et al. 2008). Some hackers use social engineering techniques to obtain information from an employee through social interaction (Mitnick & Simon 2002; Workman 2007, 2008). While these social interactions may be short and innocent at the time, they may assist an intruder with obtaining enough information to gain access and, therefore, circumvent costly security measures (Mitnick & Simon 2002).

1.1.2 Problems with current solutions

While IDS and IPS were developed to secure computer systems from unauthorised access, there are still situations where these measures may not work successfully (Botha & von Solms 2001; Workman & Gathegi 2006). Hacker profiling results such as complex frameworks, categories, taxonomies, circumplex and models are still partially incomplete or in need of refinement (Chantler 1995; Fötinger & Ziegler 2004; Kjaerland 2005; Kleen 2001; Rogers 2000, 2006; Van Beveren 2001). They also require an Information Technology (IT) security specialist to analyse activities to determine the type of the hacker. Kjaerland (2005) suggested that this process should be automated to mislead the intruder in different ways, depending on their level of expertise. At the same time, the existing need to raise security awareness among management within an organisation and the lack of training to provide security information have been clearly highlighted (Choi et al. 2008; Manjak 2006; Workman et al. 2008).

1.1.3 Importance of the study

There are still organisations and individuals who have not yet taken up the opportunity to connect to the Internet (Oates 2001), but may wish to do so in the future (Kollmann et al. 2009). Every year the number of new connections increases (Kvedar et al. 2010) and with it the level of unauthorised access (Oates 2001). Online presence provides an organisation with a convenient, around the clock access to their services for customers (Kollmann et al. 2009). It reduces the cost of staff and facilities, while allowing greater access to their services (Kollmann et al. 2009). For customers that are working during business hours, shift workers, workers at remote locations, and people who like to shop from home, it is a very convenient way to communicate without having to leave home.

This increased activity is accompanied by a steady increase in the accumulation of sensitive data, which is attractive to intruders (hackers)(Mitnick & Simon 2002). More and more individuals are at risk of being exposed as they trust the organisation enforcing security measures to protect the data. Organisations have an increasing need to block intruders from accessing their system, without disabling authorised users.

In addition, organisations also risk their reputation and goodwill of customers (Clark & Themudo 2006; Elson 2004) if their defences have been breached. However, the responsibility lies with an organisation to protect its systems, and ultimately the sensitive data of their customers (Dolan 2004). According to Choi (2008), it is essential to increase management's security awareness by keeping them informed about the consequences of security breaches. The increased security awareness may then result in change in procedures and policies (Choi et al. 2008). This change also has the potential to affect human behaviour as employees adopt the new practices (Choi et al. 2008). It is expected that studying issues associated with security awareness, coupled with aspects of human behaviours, will yield interesting findings. Thus, these issues form the basis of this research study.

1.1.4 Justification for the research

The current body of knowledge has already highlighted the need to raise security awareness at all management levels within organisations (Choi et al. 2008). It has also been identified that the body of knowledge requires statistical data analysis and the application of research methods and theories in this domain (Choi et al. 2008). To date, existing research has failed to include control groups or has used secondary data for their analysis (Workman 2007, 2008; Workman & Gathegi 2006).

New research in this domain will provide statistical information and has the potential to establish processes that are successful and repeatable. This would allow management an easier integration of security awareness into existing practices. Further research would also have the potential to provide organisations with a better understanding of the relevant issues and how they impact on unauthorised access.

1.2 Research approach

This dissertation used focus groups to obtain qualitative data in relation to security awareness of social engineering. The focus groups were recorded and transcribed. The researcher was very familiar with the focus group discussions by being the moderator, as well as listening to the recordings and reading the transcriptions.

Leximancer 3.5 was used to obtain an independent and unbiased analysis of the transcriptions. This ensured validity as the analysis process was not influenced by the researcher's own expectations. NVivo 8 was then used to read and code the transcriptions of the two focus groups.

1.3 Brief overview of thesis layout

Chapter 1 of this dissertation covers the background of the research, describing the problem, identifying problems with current solutions, and outlining the importance, justification and limitations of the research. Chapter 2 covers the literature review, with its historical background leading to the current problem, theory and research particular to this topic. Chapter 3 discusses the research model as it relates to social engineering. Chapter 4 outlines the research methodology applied to this study. Chapter 5 outlines the data collection using focus groups. Chapter 6 applies qualitative data analysis using the transcriptions of the focus groups. Chapter 7 discusses the results of the data analysis. Finally, chapter 8 provides the conclusion to the study.

2 Literature review

2.1 Introduction

This chapter will first provide an historical overview of the literature in relation to this study. It will outline the literature as it relates to the uptake of the Internet and information systems, the problems that organisations face with intruders and the protection mechanisms available. This will then be followed by the theories and research literature specific to the topic. This will describe the origin of the hacker and researchers' attempts to develop a way to profile hackers. The issues of security awareness and social engineering are then discussed. This will be followed by a critique of valid theories and research literature and close with a summary of what is known and unknown of the topic, together with the contribution this study will make to the literature.

2.2 Historical overview of the theory and research literature

Firstly, the reasons behind the Internet and information systems being taken up by businesses will be reviewed in regard to the literature. The problem of unauthorised access is considered, along with current solutions implemented by organisations. The literature highlights some of the problems that organisations encounter with these solutions, and the existing problem is identified.

2.2.1 The Internet and information systems

Information systems has become an integrated part of many organisations (Choi et al. 2008) with more organisations continuing to implement it (Levy & Powell 2000; Redoli et al. 2008; Smith & Rupp 2002). Primarily, globalisation (Oates 2001) has driven the need for organisations to find better and faster ways to communicate on a global scale (Clark & Themudo 2006; Kwai-Sang et al. 2006; Pearce 2006; Zuccato 2007). This, in turn, has been greatly supported by the development of the Internet and its technologies (Palmer 2001; Smith & Rupp 2002; Zuccato 2007). The Internet has now become a platform that allows organisations to trade online worldwide twenty-four hours per day (Kumagai 2001; Sassen 2003; Sirkemaa 2006; Smith & Rupp 2002). Nevertheless, Kollmann (2009) found that cultural differences in European countries are factors that support or inhibit the uptake of e-business.

The uptake of information systems, globalisation and Internet accessibility has also significantly altered the level of economic crime (Oates 2001). According to Oates (2001), fraud committed with credit cards was found to be 12 times higher when business was conducted over the Internet. Here, security and privacy are the most vulnerable components now that, increasingly, more sensitive data is stored on servers accessible through the Internet (Oates 2001; Rogers et al. 2006). In addition, the anonymity of the Internet, together with global access and organisations taking up information systems, provide more opportunities and create a suitable platform for hackers (Oates 2001; Rogers et al. 2006). This has the effect of electronic crime deflating customer confidence (Oates 2001) and the associated risks inhibit the development of online business (Oates 2001; Palmer 2001). Criminal activities range from fraud using online applications to employees embezzling electronic funds (Oates 2001). Subsequently, physical criminal activities have now transferred to the Internet (Oates 2001).

2.2.2 The problem with unauthorised access

Unauthorised access to computer systems and networks continues to be a problem (Kerr 2003; Nasheri 2003). Unauthorised access occurs when a person takes an action that leads to accessing a computer system or network without having been given permission to do so (Stoneburner et al. 2002; Tiller 2005). While this could occur unintentionally (Stoneburner et al. 2002), in the majority of situations a computer criminal would intentionally try all methods to gain access (Kerr 2003; Stoneburner et al. 2002; Walden 2005).

This brings to mind the term hacker, yet the meaning and description of a hacker varies. It ranges from the determined programmer who follows passionate curiosity in an effort to learn to the various levels of criminals of different skill levels (Warren & Leitch, 2009).

Unauthorised computer access commenced with the establishment of computers in the 1970s, when external access occurred by dialling into a computer over the telephone line (Kerr 2003). Denning (2011) reports that unauthorised access started to occur around the 1960, with a focus financial gain, followed by teenagers making their mark in the 1970s.

The Internet provides easy access on a global scale and individuals and organisations continue to make use of this connectivity (Zuccato 2007). This gradual increase in uptake is also reflected in more frequently occurring intrusions (Alanazi et al. 2010; Loveland & Lobel

2009; Potter & Beard 2010; Vadera et al. 2008), particularly in recent years (Potter & Beard 2010).

2.2.3 How organisations mitigate hacking

Organisations may choose a combination of a number of security solutions such as technical, manual intervention, and involve a variety of staff. Technical solutions can be in the form of hardware and software specifically targeted to determine unusual patterns and to respond in a predetermined manner. Manual intervention requires IT staff to manually observe servers and interrogate log files and audit trails to recognise unusual patterns. Irrespective of which combination of these solutions are implemented it requires IT staff, security specialists and senior management to be involved (Çakanyildirim et al. 2009). However, despite these solutions, unauthorised access continues.

2.2.3.1 Technical solutions

Organisations can implement technical solutions such as IDS (Ragsdale et al.) and IPS (Fitzgerald & Dennis 2009), or a combination of both (Doctor 2004) to mitigate unauthorised access (Çakanyildirim et al. 2009). However, for an organisation to implement secure technical solutions into their systems it requires the assistance of an IT security specialist (Baskerville 2003). This IT security specialist should have appropriate experience, not only in various systems and their vulnerabilities, but also knowledge of the various techniques hackers use to gain access, as well as expertise in the configuration requirements of the IDS and IPS (Fitzgerald & Dennis 2009). Additionally, senior management, in conjunction with IT management, may also be required to provide input into configuration requirements (Çakanyildirim et al. 2009) to ensure that appropriate actions are taken when issues are flagged by the relevant systems, as well as respond to reports (Raju 2005).

2.2.3.1.1 Intrusion detection systems

Vandenwauver et al. (1999) describe an intrusion as an action that would compromise an information system. When an intrusion occurs there is the possibility that the intruder’s aim is to disable the system, making it unavailable so that the business is unable to continue functioning properly (Vandenwauver et al. 1999). Furthermore, the intruder may aim to affect the integrity of the system (Vandenwauver et al. 1999). Considering that the intruder has broken into the system, it is now possible to change the functionality, remove access, etc. Any actions taken by the intruder could also affect authenticity of any transactions undertaken by the intruder themselves (Vandenwauver et al. 1999). This would result in sensitive data being exposed and the possibility of confidential information being sold, thereby affecting an organisation's ownership of the data relating to exclusive customers or business associates (Vandenwauver et al. 1999). To an intruder or hacker, any information is of great value, either directly or indirectly by allowing access into another system.

A detection system aims to defend the system from any outside attempts to gain unauthorised access. It uses complex algorithms to detect patterns that are not part of the day-to-day permitted activities (Vandenwauver et al. 1999).

2.2.3.1.1.1 How IDS works

The purpose of IDS is to monitor network activity so that anomalies that could lead to a compromise can be identified (Alanazi et al. 2010). Algorithms are used to differentiate normal activities from potential attacks (Yue & Çakanyildirim 2007). In this way, the IDS is reactive as it generates a notification for IT security specialists to investigate once a suspicious activity has been encountered.

Intrusion detection systems focus on host-based and network-based attacks. Host-based and network-based IDS monitor and analyse network activity (Raju 2005) using algorithms designed from traditional ways of detecting abnormal patterns (Çakanyildirim et al. 2009).

For a host-based attack, the intrusion detection systems execute routines that search for a pattern by interrogating log files and audit trails that contain user activities (Alanazi et al. 2010). These files are updated in the duration of normal daily activities by the relevant user. When the IDS interrogates these files it can determine abnormal behaviour that may have been caused by an intruder (Vandenwauver et al. 1999).

For a network-based IDS (NIDS), packet sniffers interrogate network traffic data (Alanazi et al. 2010; Doctor 2004). Behavioural or anomaly-based IDS detect any unusual behaviour patterns on the network. A normal pattern would be a sequence of expected and normal activities on the network. Unusual patterns would be a number of packets trying to open a port, or a fragmented packet (Doctor 2004).

In an active response-based IDS, the audit trail is analysed and if suspicious behaviour is detected, then the continuation of the attack is terminated. In a passive response-based IDS, details of the suspicious behaviour is forwarded to an authorised person or the system administrator (Raju 2005).

2.2.3.1.1.2 Shortcomings

The IDS may fail if the intruder's activities appear to be normal activities by an authorised user (Vandenwauver et al. 1999). Complications with host-based attacks are that the detection process becomes difficult when multiple and coordinated attacks occur at the same time (Zhou et al. 2009). For both the host-based and network-based attacks, the sensitivity level of the underlying algorithms can cause false alarms, referred to as false-positives (Doctor 2004; Farid & Rahman 2010). False-positives occur when a pattern match is regarded as suspicious (Doctor 2004). Every time an alarm is raised an IT security specialist is required to look at the patterns in either the network traffic or the log files and audit trails to determine if a real breach has indeed occurred and, if so, determine the seriousness of the breach and determine appropriate action (Botha & von Solms 2001). Setting the sensitivity at a higher level could result in more false-positives, resulting in an overhead of work for the administrator, as well as causing desensitization (Doctor 2004). On the other hand, lowering the level may achieve the opposite: that of more frequent intrusions that are not detected.

Signature-based mechanisms are needed to correctly identify known malicious patterns. They need to be kept up-to-date to include the latest threat. As processing slows down an intruder may have a chance to sneak through (Doctor 2004). The success rate of IDS and IPS depends on the sensitivity of the underlying algorithm. If the level of sensitivity is too high, too many false alarms may occur. On the other hand, a low level of sensitivity would be counterproductive if it allowed too many hackers to get through. In any case, both IDS and IPS require the assistance of a IT security specialist, with the IPS also involving management in regards to decisions on preventative action (Yue & Çakanyildirim 2007). According to Werlinger et al. (2008), past research in IDS mainly focused on how to improve the mechanism. However, it has been recognised that more support is needed for the IT security specialist who receives the alarms and is required to analyse the problems (Werlinger et al. 2008). Werlinger et al. (2008) investigated; (i) what security experts need from the IDS, (ii) difficulties in installing and configuring; and (iii) improvements to the usability. They found security experts encountered difficulties in installing and configuring the IDS, particular in complex systems.

2.2.3.1.1.3 Conclusion

While it is essential to protect a system from unauthorised access, there is a large overhead in post-mortem investigation through the large number of data files of the various systems affected (Doctor 2004). Any suspicious patterns would then need to be further investigated by the IT security specialist. This requires time and expertise on behalf of the IT security specialist to investigate on behalf of the organisation. The more complex and sensitive the technical measures are, the more likely they will raise a false alarm.

2.2.3.1.2 Intrusion prevention systems

Intrusion prevention systems respond to malicious activities on the network by taking preventative measures that will discontinue access or connections, as well as raising appropriate alerts for host-based and network-based attacks (Stanković & Simić 2010).

2.2.3.1.2.1 How IPS works

The purpose of IPS is to block an abnormal activity from reaching its target (Yue & Çakanyildirim 2007) by blocking the attack (Doctor 2004). There are two types of IPS, network-based and host-based (Fitzgerald & Dennis 2009). The network-based IPS is a device that has its own operating system (Fitzgerald & Dennis 2009). It is attached to the circuit of the network and monitors the packets of this circuit and reports to the IPS management console (Fitzgerald & Dennis 2009). The host-based IPS is a software package that is installed on the relevant server to be monitored (Fitzgerald & Dennis 2009). Any abnormal activities are also reported to the IPS management console (Fitzgerald & Dennis 2009). There are two methods of detection (Fitzgerald & Dennis 2009). One is comparing activities with the signatures of already known attacks, called misuse detection (Fitzgerald & Dennis 2009). When a signature is recognised, the packet is thrown away, and an alarm is raised (Fitzgerald & Dennis 2009). The other determines unusual activities such as a number of failed logins, called anomaly detection (Fitzgerald & Dennis 2009). The IPS first requires configuration to specify which subsequent actions it should take when detecting an abnormal activity. Such an action could be a termination of the malicious communication process (Yue & Çakanyildirim 2007). In a way, the IPS could be regarded as a proactive approach (Doctor 2004) in determining malicious activity and then, through the configuration, takes appropriate action. Intrusion prevention systems are able to drop suspicious packets, which is a more proactive approach (Scarfone & Mell 2007).

2.2.3.1.2.2 Shortcomings

An IPS configuration process may require senior management involvement. The IT department or a security specialist may propose certain actions that the IPS should be taking to senior management (Çakanyildirim et al. 2009).

However, an IPS needs to be configured by an IT security specialist in conjunction with management decisions to determine the appropriate actions (Farid & Rahman 2010). The organisation also needs to keep signatures up to date to cater for newer threats (Fitzgerald & Dennis 2009).

2.2.3.1.2.3 Conclusion

While the IPS is more proactive in its approach, organisations with highly crucial and sensitive data may opt for both IDS and IPS. Involvement of management and IT security specialists, again, has a high overhead on staff involvement in this technical solution (Botha & von Solms 2001).

2.2.3.1.3 Summary

While these technical solutions continue to be improved and their success evaluated, they are costly and elaborate mechanisms to detect and notify when anything out of the ordinary occurs (Jacobsson 2008; Thonnard & Dacier 2008). In addition, it is crucial that security measures are an ongoing process appropriately supported by procedures and policies relevant to the business of the organisation (Emanavin 2004).

2.2.3.2 Manual solution

The human cognitive process is more complex and able to pick up other suspicious signs that may not have triggered the technical solutions, IDS and IPS (Keneey et al. 2005). An additional manual solution that organisations may adopt is the frequent checking of servers and files by IT staff (Botha & von Solms 2001). One of the key findings in Keeney's (2005) research was that log files were a common way to identify an intruder. In this research, it was identified that in 75% of cases an intruder was identified through a manual process, with the majority through log files alone, compared to 19% through a combined automated and manual process (Keeney et al. 2005).

2.2.3.3 Staff involvement

From the analysis of determining a suitable IDS or IPS to the installation and configuration (Fitzgerald & Dennis 2009), an organisation would need an IT security specialist with appropriate experience in security and the relevant systems. Furthermore, once the IDS or IPS raises an alarm, it is again up to the IT security specialist to identify the cause of the alarm (Keeney et al. 2005). This requires a good understanding of the systems, as well as how attacks occur and how to interpret the relevant log files to come to a conclusion. The IT security specialist needs to know what the log files look like under normal activity to distinguish them from false alarms raised by the IDS or IPS (Keeney et al. 2005). This IT security specialist would be responsible for security and the organisation's computer systems and networks against unauthorised access through the information security management, which should provide guidelines and recommendations to implement security at physical, technical and procedural levels (Botha & von Solms 2001). Preventative measures require continuous vigilance, updates, upgrades and human intervention (Rogers 2006; Smith 2004a; Tryfonas et al. 2001).

In addition, management is required to provide input during the configuration of IDS or IPS to determine action when an alarm is raised (Fitzgerald & Dennis 2009). This requires management to understand implications and consequences.

Botta et al. (2007) confirmed that the management of IT security within an organisation may be spread across a range of employees. Driven by different aspects related to security, there is a variety of responsibilities within different units, and within different groups belonging to these units (Botta et al. 2007).

2.2.3.4 Problems in the contemporary environment

Over the years, improvements to IDS and IPS have continued, driven by the competitive search for better algorithms to increase precision and reliability (Farid & Rahman 2010; Gibbs et al. 2003). Efforts continue to correct interpretation of pattern recognition to reduce too many false alarms (Çakanyildirim & Yue 2007). However, they still do not prevent or detect all intrusions.

In addition to the technical solutions, organisations also have their IT professionals manually monitor systems, applications, log files and audit trails (Jacobsson 2008; Thonnard & Dacier 2008). With the increase of more organisations connecting to the Internet, this has not been successful in completely securing a system from unauthorised access (Emanavin 2004; Jacobsson 2008; Smith 2004a; Workman et al. 2008; Workman & Gathegi 2006; Yu et al. 2005).

As Vandenwauver et al. (1999) point out, employees of an organisation need to know what kind of data or information is crucial to protect, and the organisation needs to ensure that what should not be available to the public must be protected and stay private.

2.2.3.5 Summary

Unfortunately, the technical and manual solutions are a preventative approach with a post mortem activity that is largely time consuming (Doctor 2004). The disadvantage is that due to cumbersome analysis it also creates a delay that would allow an intruder to have already gained access before anything preventative can be done (Doctor 2004).

Furthermore, organisations have IT staff manually check log files and servers a number of times during the day, as human observation may pick up anomalies that are not obvious to the IDS and IPS.

Considering that all these methods require a certain level of IT security staff, as well as involvement of management, it leads to a potential threat to an organisation's internal security awareness (Baskerville 2003; Çakanyildirim et al. 2009; Fitzgerald & Dennis 2009). Not all levels of management of an organisation will be involved in this process (Yue & Çakanyildirim 2007) and, therefore, only a select number of managers will be security aware. It confirms Choi et al. (2008) findings that it is essential to communicate the security awareness to all levels of management.

2.3 The theory and research literature specific to the topic

The current technical and manual solutions aimed at protecting an information system from unauthorised access are not as successful as they were hoped to be. Unauthorised access continues to occur despite all the efforts. This now draws attention to the type of intruder, the hacker.

2.3.1 Source of the problem – the hacker

2.3.1.1 Early days

In the early days of computers, little documentation was available that would instruct IT administrators how to configure hardware and software (Botha & von Solms 2001) and the IT administrators had to learn how to get a system up and running, as well as how to configure it.

This required an IT administrator to spend considerable time learning to support the systems and correcting any problems. This process required a great deal of determination and patience using trial and error. It was a characteristic of an IT administrator in those days to have the drive, curiosity and desire to continuously look for a solution, particularly as there was not only missing documentation, but there were also fewer experts that could help. Through the 1960s when mainframes were extremely slow, people had to find clever solutions to increase performance. Those were also the early days of open source and development of the UNIX operating system (Leeson & Coyne 2006).

Consequently, in these early years the administrator was someone who would gain a deep understanding of the underlying system to be able to change how it works.

2.3.1.2 Hackers

Unfortunately, the 1970s brought changes that led to the term 'hacker'. Here was a person with the same type of dedication and drive as the administrator, but with a different purpose. Now, the person was no longer employed by or associated with the organisation and the aim was to understand a system well enough to access it for personal gain (Leeson & Coyne 2006; Palmer 2001). In addition, the Internet created an anonymous platform with access to worldwide computer networks. The anonymity of the Internet allowed the hacker to remain undetected as well as providing a library of resources to learn more about various systems and networks.

Slowly, over time, the level of unauthorised access grew, despite efforts to keep intruders out. There are varying degrees of skill levels and intentions, ranging from novice to expert and curiosity to malicious intent.

Despite all efforts to improve IDS and IPS as a continuing defence mechanism, unauthorised access continued to increase as more organisations went online (Workman & Gathegi 2006; Zuccato 2007).

2.3.1.3 Ethical or Grey Hackers

The age of the ethical or grey hacker began, as it was necessary to undertake in-depth studies of the vulnerabilities to understand a system and its risks to be able to protect it (Harris et al. 2005; Palmer 2001). The ethical or grey hacker is specialised in breaking into systems and gaining unauthorised access in the same way as the hacker, except the ethical hacker is employed by an organisation to find weaknesses in their systems. The purpose of the ethical hacker is to determine what these weaknesses are so that the organisation can take proactive steps to increase its security. Harris et al. (2005) takes it further in considering the ethical implications of publishing books detailing hacking, but disputes this concern as hackers have already gained the skills needed. Now, more than ever, IT security specialists need to have a deeper understanding of the systems and applications they are supporting. While a hacker can focus attention to one particular aspect of a system, the IT security specialist requires a wider focus and vigilance to protect all aspects of all systems of an organisation (Harris et al. 2005).

2.3.1.4 Profiling hackers

In an attempt to find a solution to the problem of continuous unauthorised access, it was thought that determining the motivation behind the intruder might lead to additional solutions. Researchers adopted already-established psychological and criminal profiling methodologies which had already been explored by psychologists and forensic experts to resolve physical crimes (Rogers et al. 2006). In addition, psychological theories of crime were influenced by criminology (Chantler 1995; Fötinger & Ziegler 2004; Kleen 2001; Rogers 2006).

However, complications arise when transferring criminal activities from the physical to computer crime. Physical criminal activities may operate within groups with their own social environment. Reasons for criminal activities could be combinations of environment or learning from observation (Van Beveren 2001). One other aspect is also that physical criminal activities have the potential to be observed. This is not the case with hackers, mainly due to the anonymity of the Internet. Hackers are more likely to hide their presence the more skilled they are, which makes it more difficult to determine that an intrusion has occurred (Rogers et al. 2006).

Still, researchers continued to profile hackers and created frameworks, categories, taxonomies, circumplex, and models. It was observed that a shift occurred, as hacker profiling is not solely a consideration of the IT profession. Rather, professions such as psychology, auditing, accounting, and management, which are involved in the post mortem process and in the cleanup of a security breach, are a likely source for this type of research. As existing security measures did not seem to be fully successful (Workman 2008) researchers were inadvertently compelled to explore this new domain. To find a solution, profiling or classifying computer criminals continued within the domain of psychology and criminology as a guide (Fötinger & Ziegler 2004; Pleskonjic et al. 2006; Workman et al. 2008; Workman & Gathegi 2006). Establishing the motivation behind a person’s behaviour raised the hope that this may lead to additional measures to reduce unauthorised access. At the time, the fields of psychology and criminology seemed to be an ideal source of knowledge as psychologists and forensic experts had already developed criminal profiling that might be suitable for adaptation (Fötinger & Ziegler 2004; Rogers 2006).

Psychological and criminological theories were applied by researchers in their process of categorising and profiling hackers (Chantler 1995; Fötinger & Ziegler 2004; Kleen 2001; Rogers 1999, 2006). The development of a hacker taxonomy and circumplex was suggested to be suitable for investigative purposes (Rogers 2006). It enables organisations to determine the type of intruder depending on the type of evidence. It may also assist in making assumptions about the intruder, but is highly subjective to the investigator's ability to identify signatures. As intruders are more likely to try and hide their presence, successful interpretation relies on the skills and experience of the investigator. An experienced IT security specialist would have this expertise. However, the model does not provide management with the ability to provide better policies or risk assessments (Rogers 2006).

Other categorisations focused on the steps a hacker would take to develop a more generic hacking methodology (Botha & von Solms 2001). Research by Botha and von Solms (2001) focused on finding a way to deal with intrusions proactively, but technical expertise to manually work through log files and audit trails is still required. This view is supported by Rogers (2006) who asserts that as well as taxonomy and frameworks, categories, taxonomies, circumplex, and models, certain levels of expertise are required to analyse the intruders behaviour pattern so that it can be translated into the profile.

Another approach by Kleen (2001) focused on military needs to create a hacker framework, using a case study to determine the profile and motivation of incarcerated hackers. This research recognises its own shortcomings in the data collection methods. The data was limited to hackers who have been incarcerated and who were self-reporting, and therefore may be affected by self-inflated perceptions.

While the development of frameworks to profile hackers continues, there is also a growing realisation that psychological theories are difficult to apply to a group of people who wish to remain anonymous. The many theories to explain conventional human behaviour are compounding the problem that researchers are confronted with when investigating unconventional activities by an unseen hacker (Van Beveren 2001).

Another branch of research took a different approach in trying to combat unauthorised access by considering ways to address the issue of human behaviour within an organisation. There is a common agreement among researchers in this area that suggests an increase in security awareness within all management levels would be crucial to the success of implemented security measures (Choi et al. 2008; Lawlor & Vu 2003; Smith 2004b; Trim 2005; Warren 2002; Workman 2008; Workman et al. 2008; Workman & Gathegi 2007). The implication is that an increase in security awareness would result in better policies and procedures, affecting risk assessments and continuity planning. It would also lead to a workforce that is more security aware and has an understanding of prudent behaviour, potentially creating an organisational culture that is more robust to social engineering threats.

2.3.1.4.1 Detection and prosecution

Detection and prosecution may be difficult, as some organisation may be unaware an intruder breached their system, while others may not publicise the incident for fear of losing customers (Roberts & Webber 2002).

While the definition of “unauthorised access” describes an act of accessing a system without permission, the law requires a lot more before someone can be successfully prosecuted. The law needs to more specifically describe what the act of “unauthorised access” exactly means. In the past, a hacker could not be prosecuted if they only “looked”, gained access and viewed the data without causing any harm or damage. And the interpretation of “unauthorised” and “access” are not always clearly defined in the law, leaving it to the interpretation and assumption of legal representatives (Maurushat & Yu 2009). The legal profession transferred from physical to cyber crimes, but due to the nature of information systems, it was necessary to change the law to accommodate the differences (Harris et al. 2005).

2.3.1.4.2 The problem with hacker profiling

The resulting frameworks, categories, taxonomies, circumplex, and models still require the expertise of an IT security specialist to analyse log files looking for patterns (Chantler 1995; Fötinger & Ziegler 2004; Kleen 2001; Rogers 2000, 2006; Van Beveren 2001). They also require further development more suitable for implementation in the industry (Rogers 2006). Knowing the profile of the hacker may assist in understanding the potential damage that could have been caused. However, it is a measure that occurs after the fact. The post mortem process of sifting through files reflects successful intrusion. It is not a preventative measure at this point in time. In addition, the methods of identifying the hacker profile are also still very complex. Considering that the hacker uses the transparency of the Internet and may be highly skilled, the correct profile may not always be divulged.

2.3.1.5 Security awareness

The varied foci by researchers have created a different way to look at the problem of unauthorised access. The focus of this research is looking at the human being, the employee, as the weakest link. It is essential that security awareness level is raised in individuals by the management of the organisation (Choi et al. 2008). This can be achieved through simple and clear communication, and one of the suggestions by Mann (2008) is to use induction training to provide an addition to the standard IT induction. Choi et al. (2008)

found that not only is it necessary to fight unauthorised access on a technical level, but also the level of security awareness must be raised at all levels of management. Choi et al. (2008) highlights the distinction between technical preventative measures and deterrent human interactions. This is based on the appropriate development of security policies through management, and the education of the organisation’s employees throughout. The aim of security in an organisation is to reduce the potential of data or information leaving the organisation to then be used by a hacker to access a system.

2.3.2 What is social engineering?

Social engineering is the process of interacting with and manipulating people for the purpose of gaining information (Anonymous 2001; Dolan 2004; Kvedar et al. 2010). It involves cajoling people into providing information that would help the hacker attack a system (Anonymous 2001). Social engineers are very skilled in deceiving people, and misusing people’s natural supportive attitudes (Mitnick & Simon 2006).

Members of groups with strong cohesion would feel safe to volunteer sensitive information (Workman 2008). People may feel that volunteering sensitive information would provide them with more attention from others. However, a potential hacker could take advantage of this and misuse this information in an attempt to break into an organisation’s computer system (Dolan 2004). Some research investigated the impact of punishment, ethics and security training on employee behaviour toward social engineering at an operational level. Unfortunately, this research failed to include a control group and did not address the impact of raising security awareness at a higher level of management (Workman 2007, 2008; Workman & Gathegi 2006). The need for attention in a social setting, for feeling important, or for being outgoing, social and kind could place people in a vulnerable position of being mislead into divulging sensitive information (Dolan 2004).

According to Workman (2008) there is significant reason why automation may not be able to solve all problems of intrusion, and lists financial, situational, cultural and technological as the four reasons why automation would not be entirely successful because of their influence on human perception and behaviour. A crucial factor in this situation is social engineering. A potential hacker could obtain information through casual social interaction with people who may have some information that could help in the process of intrusion (Fötinger & Ziegler 2004; Kjaerland 2005; Kleen 2001). These people may feel that volunteering sensitive information will provide them with more attention. Other opportunities for social engineering are groups with strong cohesion, where people feel they are in a safe environment and, therefore, voluntarily discuss sensitive issues without being prompted (Workman 2008).

While Workman's (2008) research investigated the impact on punishment, ethics training and social engineering training at the operational level, it neglected to use a control group. It also failed to address the impact that security awareness would have on management, policies and strategies generated, and the subsequent change in organisational culture. A crucial point was that the communication process by management of current and actually occurring security vulnerabilities may actually increase employees' perceptions of security threats as real. Showing the effectiveness of the implemented corrective measures may reduce lapses through the better understanding of the seriousness and reality of the threats (Workman et al. 2008). Further research clearly needs to focus on quantitative analysis to identify the significance that awareness of social engineering techniques has on intrusion. This is further echoed by the findings of Choi et al. (2008) that management concerns regarding security issues were low. Through interviews and surveys, Choi et al. (2008) found that an increase in security awareness by management would impact the effectiveness of control. Management levels need to address the security awareness of their employees so that security is viewed as a core activity. Frameworks, strategies, policies and procedures would then outline the requirements for emergencies and disaster recoveries (Trim 2005; Warren 2002).

Some of the simplest cases of social engineering occur when basic procedures are not adhered to, such as failing to obtain proof of identity (Volonino & Robinson 2004). Social engineering is successful because it is difficult to recognise deception (George et al. 2003). According to Whitman and Mattord (2008, p. 425) "most nontechnical attack involves people", and as a show of conviction they focus a large percentage of their textbook on communicating that security is an issue related to people.

2.3.3 How does social engineering relate to unauthorised access?

In accordance with social engineering, a person could glean information through social interaction with employees of an organisation. The person would be someone with the intention of gaining sensitive information that would assist in the process of unauthorised access. The employee would be misled or persuaded by this person to divulge information inadvertently (Fötinger & Ziegler 2004; Kjaerland 2005; Kleen 2001). For an adept hacker, using social engineering would be a successful way to obtain information. Education and training have been identified as strategies to reduce the success rate of social engineering

(Barrett 2003; Mitnick & Simon 2002). Workman et al. (2008) and Choi et al. (2008) suggest that training employees to raise their security awareness is a missing factor in organisations as it has the potential to alter an employee's perception and lead to more cautious handling of information (Beebe & Rao 2005; Mitnick & Simon 2002; Trim 2005).

Training and education is needed to clarify various social engineering techniques and consequences to employees and their organisation. These suggestions assume that an organisation educates all its employees to raise their security awareness, starting with upper management levels. This could have a cascading effect, as policies, procedures and risk management analysis would facilitate a change in employee behaviour over time.

Members of groups with strong cohesion feel safe in volunteering sensitive issues (Workman 2008). People may feel that volunteering sensitive information would provide them with more attention from others (Dolan 2004). A potential hacker could take advantage of this and misuse this information to attempt an attack on an organisation's computer system (Dolan 2004).

Some research investigated the impact of punishment, ethics and security training on employee behaviour toward social engineering at an operational level. The research failed to include control groups and did not address the impact of raising security awareness at a high level of management (Workman 2007, 2008; Workman & Gathegi 2006).

At the same time, another branch of research looked at the behaviour in workplaces. Workman et al. (2008) found significant reasons why automation may not be able to solve all problems of intrusion. This is further confirmed by Choi et al. (2008) who asserted that not only is it necessary to fight intrusion on a technical level, but it is also essential that management awareness and concern is raised at a higher level.

Using social engineering would be a successful way for an adept hacker to obtain information (Barrett 2003; Mitnick & Simon 2002). Education and training have been identified as strategies to reduce social engineering. Workman et al. (2008) and Choi et al. (2008) suggested that training employees to raise security awareness is a missing factor in organisations.

If training reached all levels within an organisation, including management, it would be an effective defence against social engineering (Beebe & Rao 2005; Mitnick & Simon 2002; Trim 2005).

2.4 Critique of the validity of appropriate theory and research literature

Despite the advancements in security, the need for information security and its assurance is still growing, as more sensitive data continues to be collected and stored (Rogers et al. 2006). IDS and IPS have been unable to eliminate all of the risks of electronic crime (Smith 2004a), and there is still a considerate amount of manual work required by IT staff within an organisation (Botha & von Solms 2001; Keeney et al. 2005).

While research has identified and posited the need for psychological theories to be used in this type of research with the focus on providing non-technical solutions, relatively few research projects have applied psychological theories to their analytical research methodologies (Choi et al. 2008; Rogers 2006; Workman 2008). This may be due to psychological theories being relatively new to this IT research domain.

At the same time, research highlighted a limited amount of data collection and data analysis in regard to these theories (Choi et al. 2008; Rogers 2006; Workman 2008).

Added to this, research within this domain is spread across different professions such as psychology, auditing, accounting, and management (Choi et al. 2008).

While research to determine the profile of a hacker is still ongoing, it is scant in providing feasible solutions for organisations to use the frameworks, categories, taxonomies, circumplex and models in an effective manner to prevent intrusion (Rogers et al. 2006).

Some researchers (Smith & Rupp 2002; Wilson 2001) utilised surveys in an attempt to determine the motivation and drives of a hacker. However, these surveys were only distributed to incarcerated hackers, leaving an unknown number of hackers unaccounted for.

Choi et al. (2008) and Workman and Gathegi (2006) agree in their observation that an increase in security awareness has shown an increase in security and provides a reduction in the number of incidents. Research still needs to provide more evidence that increasing an organisation's security awareness does have an impact and is an additional measure to the technical solutions already in place.

2.5 Summary of what is known and unknown about the topic

What is known about this topic is that researchers identified the need for a non-technical alternative to securing an organisation, and for more research on security awareness to provide additional qualitative and quantitative data analysis (Choi et al. 2008).

While it is also known that an increase in security awareness has decreased incidents of unauthorised access (Choi et al. 2008), it is not known how much of this security awareness incorporates social engineering, or to what extent social engineering is part of the knowledge.

While group experiments were conducted by Workman and Gathegi (2006) to determine the impact of punishment on secure behaviour of employees, they failed to use control groups.

Research in hacker profiling has also provided frameworks, categories, taxonomies, circumplex, and models that provide more details on the various types of hackers, but is still incomplete in its application. It is still unknown how the hacker profile can be used by an organisation to prevent unauthorised access.

2.6 The contribution to the literature

The contribution that this research study will make to the literature is providing a model that will assist other universities, as well as organisations, in raising security awareness.

This study aims to determine what the current awareness levels are within the university, and provide qualitative results that can be further used in quantitative research. With this, the study links into the niche for more recent research in security awareness and its impact on an organisation's occurrence of unauthorised access. This may provide an insight for future research to expand upon.

Furthermore, the results may lead to further qualitative research to discover wider aspects in relation to security awareness. This then may lead to a better understanding before delving into quantitative research.

The need for empirical data has already been expressed by the literature in regard to security awareness and the effect of social engineering (Choi et al. 2008; Choi et al. 2006; Workman & Gathegi 2006), particularly since the frameworks, taxonomies, circumplex, and models are still under development and too complex to implement (Kjaerland 2005; Rogers 2006). While they undergo a rigorous and thorough development, they do not provide guidelines on how an organisation can use them as preventative measures.

Raising security awareness at all levels of an organisation has been identified as an existing need (Choi et al. 2008; Manjak 2006; Workman et al. 2008). Parker (2007) acknowledges the difficult between the needs of risk management and the difficulty in defining cost of threads that are difficult to define.

2.7 Chapter summary

This chapter covered the historical overview of the theory and research literature, highlighting the continuous growth of businesses taking up information systems and the equally continuous growth of intrusions still occurring despite the technical measures adopted. The literature shows that the effort of profiling hackers has not yet provided a workable solution and that other professions have posited the need to increase security awareness and consider social engineering to find a non-technical solution that will reduce unauthorised access.

3 Research Model

3.1 Introduction

The sole focus of this research is social engineering. This chapter outlines the research model designed for this study. It explains the various elements of the model. The chapter then progresses to the research question and its propositions.

3.2 The research model

While the model describes expectancy theory and social engineering, only social engineering will be addressed in this research study. The scope of both theories is considered excessive for a Master's dissertation. Therefore, the propositions (P2a, P2b and P2c) of the sub question for expectancy theory are not described here.

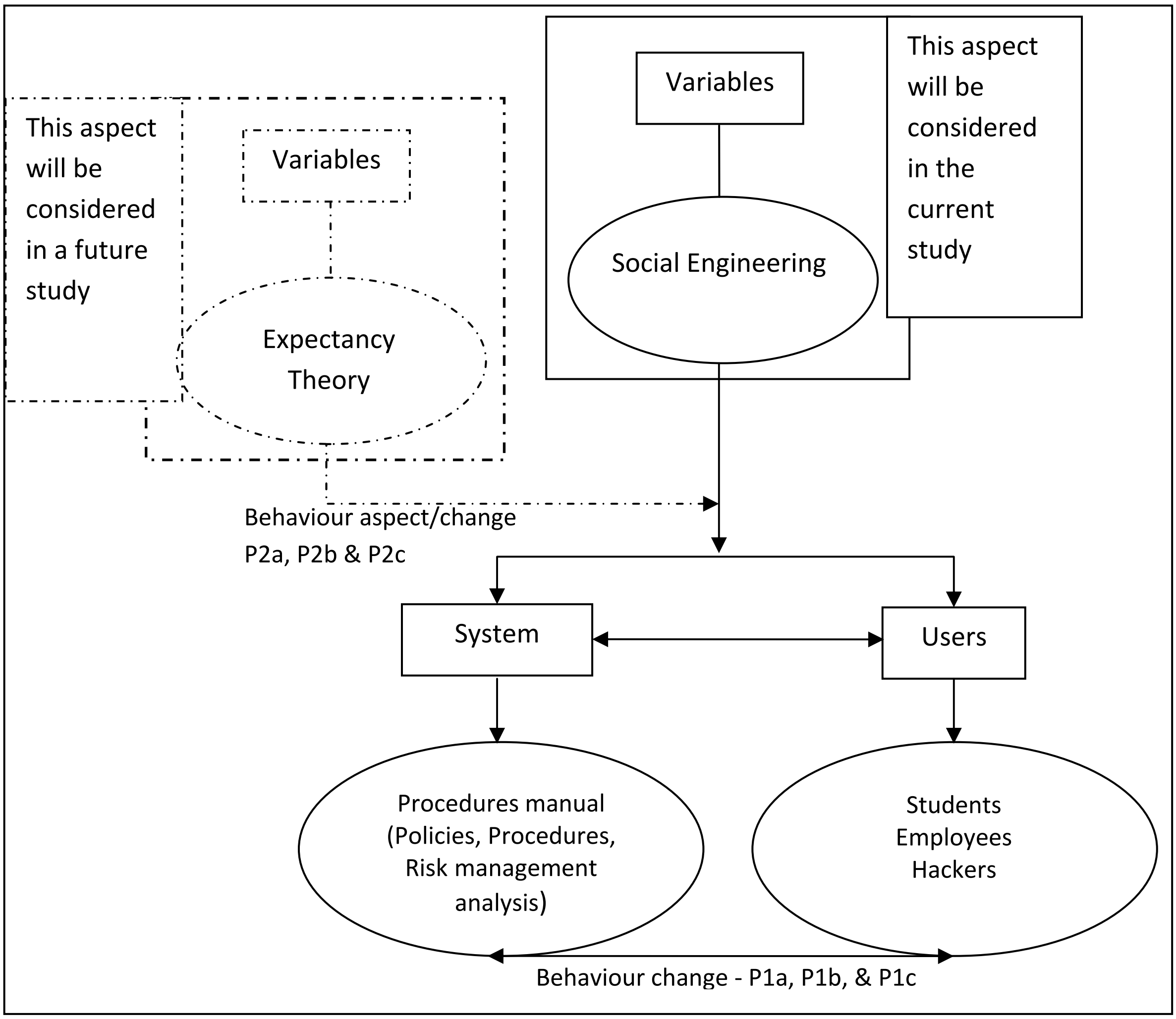

This aspect will be considered in a future study
Variables
Expectancy Theory
Variables
Social Engineering
This aspect will be considered in the current study
Behaviour aspect/change P2a, P2b & P2c
System
Users
Procedures manual (Policies, Procedures, Risk management analysis)
Students Employees Hackers
Behaviour change - P1a, P1b, & P1c

Figure 1: Model - minimize intrusion with propositions (P1a, P1b, P1c, P2a, P2b, and P2c)

3.3 The model

The research model in Figure 1 shows the connection between social engineering, the system, and users. The behaviour aspect or change in relation to expectancy theory will not be considered in this study, and thus excludes propositions P2a-c.

Social engineering is seen as targeting the user by way of communication. The hacker may have a conversation with someone who uses the system, and gain knowledge that may help in the process of intrusion. Interaction between the users and the system may lead to improvements affecting policies and procedures, however, changes have the potential to either weaken or strengthen the security of a system.

3.3.1 Social engineering

Social engineering in this model is targeted at the users. It focuses on gaining information regarding unauthorised access to the system.

3.3.2 System

The system represents the physical computer systems, as the rules and procedures would have been applied to the configuration and programming logic through organisational procedures and policies. Therefore, it is also a representation of the way information is being processed and business is being conducted. Business rules are implemented in either policies or procedures, and applied to computer software and hardware, as well as human processing.

The way that a user interacts with the computer system and applies the procedures and policies will have an impact on the integrity of the system. Changes in perception and understanding, problems with implementation, and improvements to procedures and policies will be driven by the user and impact the system.

Processing of information occurs through the use of software that is accessed by desktop PCs or laptops. Access to the software is determined by the login profile of USQ staff or students. Certain access permissions are applied to individuals so they can utilise the relevant software. Servers have monitoring capabilities, and auditing trails provide information on activities and access by users.

3.3.2.1 Procedures manual

The intention of the procedures manual is to provide the organisation with guidelines in implementing security awareness throughout the organisation. It will support the modification of procedures, policies and risk management. Any changes in procedures should be documented in the procedures manual. A procedures manual is meant to be maintained and should grow and change with future needs.

3.3.2.2 Policies

Policy makers need to refer to the procedures manual when compiling new policies or maintaining existing policies to ensure that new guidelines are adhered to.

3.3.2.3 Procedures

The way that certain processing is done occurs either through the implementation of software or through human processing. Software developers, system analysts, and business analysts must be aware of the guidelines outlined in the procedures manual to ensure that the software applies the required security measures. Procedures used by USQ staff are applied to a human process, not software, and must take into consideration the security requirements of the procedures manual.

3.3.2.4 Risk management

Security awareness is necessary at all levels within an organisation. This is particularly vital at high levels of management to ensure that the organisation continues to adhere and adjust to new security measures. It is also vital in the calculation of risk management to ensure adequate provisions are in place.

3.3.3 Users

Users encompass current students, USQ employees, as well as casual visitors to the USQ web portal. The web portal allows these users access to information and applications, depending on their login credentials. USQ students and employees are given login access depending on their profile and are able to access applications accordingly. All other users can browse public information on the USQ website, but not access any applications.

Part of the information processing relies on human communication, which cannot be reinforced and monitored in the same manner as on the servers. Human communication relies on correct adherence to policies and guidelines. It also relies on the diligence of the individual to do the right thing; and requires each individual to know what the right thing to do is. This is usually achieved in organisations through educational processes.

3.3.4 Behavioural change

The behaviour change indicated in the model occurs between the users and the system. Procedures and policies guide the security implementations that include the practices of employees, the access levels to the system, etc.

As management implements increased security awareness throughout the organisation and policies and procedures are revised accordingly, the more it impacts on what the users of the system can do. It changes their behaviour, their permissions, and influences what they can access and how they should adhere to policies and procedures. This may cause situations where users feel restricted in their ability to do their work and, thus, may result in circumvention of security measures. Subsequently, existing shortcomings are highlighted at an organisational level and result in ongoing changes to and awareness of security levels – and once security awareness has been raised, it will require further changes to existing policies and procedures to protect and maintain security.

3.4 The research question and propositions

Social engineering is a way to obtain information through social interaction (Choi et al. 2008; Dolan 2004; Workman et al. 2008). The model in Figure 1 indicates that educating employees has the potential to raise their security awareness and may positively affect their interaction with others. Employees with higher security awareness may then behave with more caution, reducing the potential for computer criminals to obtain information that may lead to unauthorised access.

In accordance with social engineering, a potential hacker could glean information through casual social interaction with employees of an organisation with the intention of finding a way to break into the organisation's computer system. Employees may be misled or persuaded to divulge information that could help a hacker in the process of intrusion (Fötinger & Ziegler 2004; Kjaerland 2005; Kleen 2001). Members of groups with strong cohesion would feel safe in volunteering information on sensitive issues (Workman 2008), or may feel that volunteering sensitive information provides them with more attention from others. However, the potential hacker could take advantage of this situation and misuse this information to attempt an attack on an organisation's computer system (Dolan 2004). Some prior research has investigated the impact of punishment, ethics and security training on employee behaviour toward social engineering at an operational level. However, it failed to include a control group and did not address the impact of raising security awareness at a high level of management (Workman 2007, 2008; Workman & Gathegi 2006) However, for an adept hacker, using social engineering would be a successful way to obtain information (Barrett 2003; Mitnick & Simon 2002). Education and training have been identified as methods to reduce social engineering.

The need for attention, for feeling important, or for being outgoing, social or kind could place people in a vulnerable position and being mislead into divulging sensitive information (Dolan 2004). Workman et al. (2008) and Choi et al. (2008) previously suggested that the training of employees to raise security awareness is a missing factor in organisations. It has the potential to alter employee perception and make them more cautious in protecting information. This training should reach all levels within an organisation, including management, and is an effective defence that an organisation can implement (Beebe & Rao 2005; Mitnick & Simon 2002; Trim 2005). The training needs to clarify what constitutes social engineering techniques and the consequences to all employees in the organisation. It is assumed that when an organisation educates all its employees in an effort to raise security awareness, it is possible to initiate a change. Raising security awareness in management can have a cascading effect, as policies, procedures and risk management analysis would change over time. Human resources would ensure that all training courses would be adjusted to educate people to adopt the appropriate behaviour. This has the potential to change perceptions and subsequent behaviour that is more appropriate in protecting the organisation's assets and make it more difficult for hackers to obtain information, thereby reducing the potential of intrusion.

These aspects address the research question of:

> How can education affect the process of preventing social engineering to minimise the success of unauthorised intrusion?

This subsequently leads to the following research propositions:

> **P1a.** Employees who are aware of social engineering techniques through education are less likely to divulge information than employees who are unaware of social engineering techniques.

P1b. Employees who are aware of the consequences through education of social engineering are less likely to divulge information than employees who are unaware of the consequences.

P1c. Employees who are aware of both social engineering techniques and the consequences through education of social engineering are less likely to divulge information than employees who are unaware of social engineering techniques and the consequences.

3.5 Chapter summary

This chapter firstly introduced the relationship of the elements in this module in relation to social engineering. It then provided information on the system and the users, and concluded with the formulation of the research question and subsequent propositions.

The following chapter describes in depth the methodology adopted for this research study.

4 Research Methodology

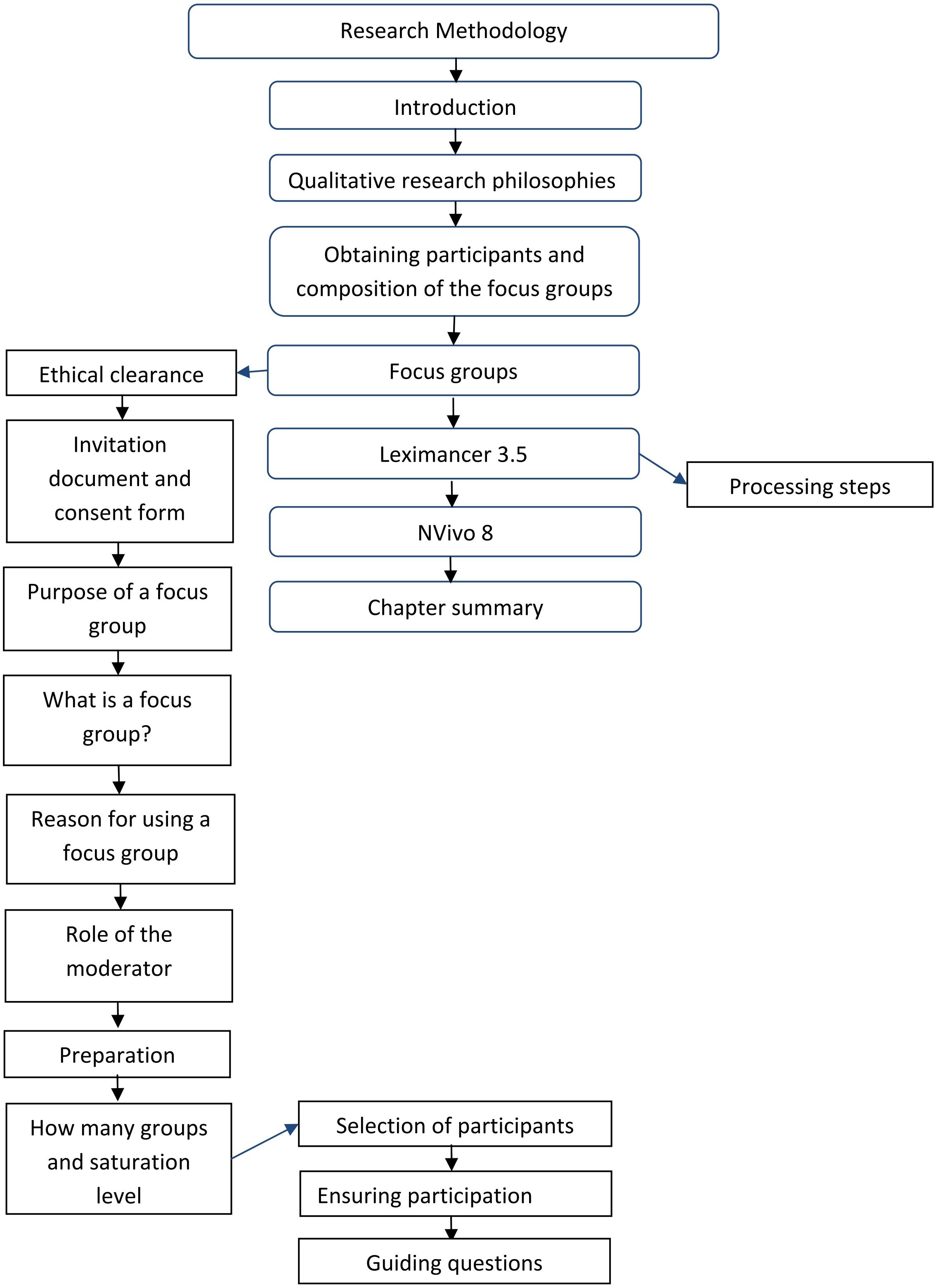


Figure 2: Chapter 4 Research Methodology

4.1 Introduction

The previous chapter described the research model to be used in this research, as well as the research question and the corresponding propositions. Figure 2 provides a graphical representation of how this chapter is structure. Firstly, this chapter describes in detail the research methodology adopted for this study. Here the philosophies will be discussed, leading into those suitable for qualitative research. Since the intention was to use focus groups for the data collection, the process and considerations of conducting focus groups will be described, together with details of how each focus group will be recorded, and the transcriptions analysed. The use of Leximancer 3.5 for an initial unbiased analysis, followed by NVivo, will allow the researcher to code the transcription. In addition, both software text analysis packages are explained.

4.2 Qualitative research philosophies

Qualitative research in Information Systems is mostly based on the behavioural-science paradigm, such as positivism and interpretivism, or the design-science paradigm.

Blackburn (1993) and Lee and Baskerville (2003) describe positivism as the understanding that human or social science should use the model of the natural-science. Positivism is using the scientific method as the best way to determine the processes between the physical and human occurrences (Blackburn 1993; Wikipedia). Positivism reflects the belief that an object and the real world exists independently to the researcher and the need for the researcher to factually report findings, disregarding any beliefs of what was assumed or expected to be there (Lee & Baskerville 2003). Positivism then uses logical thinking in developing hypotheses, and deduction reasoning to ensure that the propositions of the research questions are aligned with the theory and confirmed by empirical data (Lee & Baskerville 2003). Further confirmed by Trochim (2006), positivism uses empiricism, observation, measurement, deductive reasoning, as well as law of cause and effect. Lee and Baskerville (2003) suggested that positivism is used in Information Systems (IS) and this was confirmed by Dubé (2003), who found that from 210 IS case studies, 87% used positivism. In any research, validity ensures the certainty that data really does measure reality, and reliability ensures that the results can be replicated (Weber 2004). In positivism, researchers use lab or field experiments, or surveys to find large amounts of empirical data for their statistical analysis. As Silverman (2005, p. 9) points out "positivism is the most common model used in quantitative research" and "it sits uneasily within most qualitative research design" (Silverman 2005, p. 9).

Interpretivism, on the other hand, is used to find phenomena that "is not present in the subject matter studied by natural science" (Lee & Baskerville 2003, p. 230). Interpretivism focuses on case studies, studies concerned with ethnography, phenomenography or ethno methodology, to find the characteristics of a certain philosophical view (Tashakkori & Teddlie 2003; University of Queensland 2010b). Validity is ensured in that knowledge claims need to be defensible (Weber 2004). Reliability relates to the interpretive awareness, where a researcher identifies and handles the implications of being subjective (Weber 2004). With the research philosophy for this study based on interpretivism, the researcher uses focus groups to determine participants understanding of security risks. The aim is to better understand employees' awareness of security risks and unauthorised access, and how they may be affected by social engineering techniques is the interpretive process of understanding. The interaction of the participants within the focus group allows researchers to gain a better understanding of these issues (Hesse-Biber & Leavy 2006). It also allows the researcher to interpret the meaning that participants have about the topic (Creswell 2009).

Design-science emerged to balance the behavioural science paradigm with "more design-oriented science research" (Indulska & Recker 2008, p. 1). The reasoning is that human behaviour and Information Technology (IT) cannot be separated (Hevner et al. 2004). While behavioural-science paradigm is used to verify human behaviour, design-science paradigm on the other hand focuses on creating new artefacts (Hevner et al. 2004).

Qualitative research uses data that does not fit into a classification required by statistical analysis (Mauch & Park 2003). Here, the data is not in the form of numbers that can be used to calculate statistical formulas, but in words, meaning and understanding (Punch 2006; Tashakkori & Teddlie 2003). The researcher tries to understand the meaning of a phenomenon from words, observations, and stories (Mauch & Park 2003). The conclusion occurs through the process of deduction, by reasoning from the general to the more specific (Trochim 2006; Zikmund 2000). The researcher aims to gain a better understanding using communication by applying techniques such as focus groups. Participants provide ideas and information about the research topic within their area of expertise, and the researcher guides the communication process by using general questions. The aim is to understand the context of words and statements in an attempt to determine underlying assumptions (Mauch & Park 2003). For qualitative research, one of the main techniques is the use of focus groups (Statistics Solutions 2011a), therefore the aim is to identify factors that will assist in highlighting security awareness in relation to social engineering.

Exploratory research is a suitable method for areas where limited information is available. This allows the researcher to establish a better understanding of the topic, before delving into more rigorous scientific and quantitative research. It enforces validity so that the subsequent quantitative research is measuring what it should measure (Zikmund 2000).

4.3 Focus groups

The benefit of using focus groups is a free flowing discussion about the research topic (Krueger & Casey 2000; Ruane 2008). The aim for this free flowing discussion is to reveal any insights into the thinking of the participants about the research topic (Ruane 2008). The result could then have the potential to confirm the researcher's expectation as well as highlight any new trends (Morgan 1988).

Social interaction within the focus groups is essential in allowing participants to explore new ideas and directions as they appear (Breen 2006). One particular aspect of a focus group is that participants are allowed to interact with each other. As participants interact with each other and discuss the issues related to the research topic, a certain amount of trust may promote self-disclosure (Krueger & Casey 2000). Discovering that they have certain things in common, may lead participants to feel more comfortable in being open to discussing sensitive issues related to their area of expertise (Krueger & Casey 2000).

4.3.1 Ethical clearance

At the time of writing this chapter, the researcher obtained ethical clearance. As the ethical committee convenes only a number of times per year, it was crucial to obtain the application approval as soon as possible. The researcher was able to obtain the ethical clearance on 9 February 2010 from the Human Research Ethics Committee of the USQ (H10REA018).

4.3.2 Invitation document and consent form

For the purpose of finding participants for the focus group, the researcher requires an invitation document, which introduces the researcher and outlines the type of research being undertaken in the study. In addition, it should provide some general information such as what focus groups are, the anticipated duration, and provision of refreshments. To increase participation, the researcher used this opportunity to offer lunch to participants (Rodrigues et al. 2010). Furthermore, participants need to be aware that an ethical clearance had been obtained for conducting the focus group. An ethical clearance number and the contact details of the Ethics Committee should be included. The document also needs to communicate that the discussion will be treated with confidentiality, that no names or other information that may identify anyone would be published. Participants have the right to privacy and sensitive information needs to be safeguarded by the researcher (Ruane 2008).

A consent form should then be attached to the invitation document. This provides participants with more detailed information about informed consent. Individuals have the right to decide if they wish to participate or not, or even withdraw their consent and participation at any time (Ruane 2008). The participant will be required to sign the consent form. Making the consent form the second part of the invitation document allows the researcher to alert the participant early about these choices.

4.3.3 Purpose of a focus group

The purpose of a focus group is to freely discuss a particular topic. The aim is to gather as much information as possible while allowing participants to lead the discussion, but with the moderator ensuring that they stay within the topic (Krueger & Casey 2000; Ruane 2008). This unstructured, free flowing discussion is expected to provide an insight into what people think about the topic (Ruane 2008; Zikmund 2000). A focus group provides opportunities to explore new ideas as they are generated during the discussion (Breen 2006).

4.3.4 What is a focus group?

Focus groups are used in qualitative research and are a common tool in the study of human and computer interactions (Eysenbach & Köhler 2002). They consist of a mixture of participants from different areas of an organisation. It is anticipated that each participant would bring different levels of expertise that would link into the domain under investigation (Krueger & Casey 2000). Morgan (1988) suggests that focus groups are similar to group interviews. They differentiate in that group interviews would have fixed interview questions that may cover a number of topics, while focus groups are allowed to interact and discuss the topic. This allows the exchange of experiences, the generation of ideas, and unexpected information which would lead to identifying the factors that are influencing this domain (Morgan 1988).

4.3.5 Reason for using a focus group

The intention of using focus groups is to determine what people know, think, and are aware of or are able to deduct from a topic. This may confirm some of the expectations of the researcher, and allow any new factors to be detected. As participants are allowed to interact and discuss issues related to the topic, the format promotes self-disclosure between participants (Krueger & Casey 2000). When participants have something in common, they may feel more comfortable to openly discussing issues within their area of expertise. The resulting homogeneity allows the researcher to determine a range of information about the topic to gain an understanding of the different perspectives (Krueger & Casey 2000). By finding out what influences their thoughts and actions may provide a better understanding of their behaviour (Krueger & Casey 2000). In addition, participants from different areas of an organisation allow opportunities to generate ideas within the topic. The range of opinions gathered from the focus groups then allows the researcher to identify factors. These factors then provide the necessary qualitative data that the researcher can use to build the survey questions (Krueger & Casey 2000). This also allows the researcher to gain a better understanding of the issues, before engaging in quantitative research (Krueger & Casey 2000). The understanding of the topic through the focus groups then also provides the language and the words that feed into the questions for the survey (Krueger & Casey 2000).

4.3.6 Role of the moderator

The moderator of a focus group has an important role and therefore, needs to be a good communicator and understand the research topic well. Krueger and Casey (2000) believe that the quality of the focus group outcome would be greatly affected by the respect for the moderator by the participants. At the start of the focus group, the moderator needs to establish a good rapport with the group and to make participants feel comfortable in interacting within the group. While the topic is being discussed by the participants, the moderator needs to be actively listening, making the participants feel that they have been heard to stimulate spontaneous responses (Krueger & Casey 2000; Zikmund 2000). Krueger & Casey (2000) advocate that by a moderator showing real interest in participants, it can enhance communication within the focus group; and, moreover, the moderator's belief in the expertise of the participants will foster open discussion (Krueger & Casey 2000; Zikmund 2000).

The moderator’s understanding of the topic is essential. The moderator needs to start the focus group with an initial suggestion and to ensure that the discussion stays within the scope of the topic (Krueger & Casey 2000). The use of predefined questions prepared by the moderator will guide the participants. Should the discussion deviate from the topic, is it imperative that the moderator clearly understands the topic of the research and the purpose of the focus group, and inject corrective questions (Krueger & Casey 2000; Zikmund 2000).

The moderator needs to be a person who the participants feel comfortable in discussing issues freely and keeps the focus of the group within the topic (Zikmund 2000).

Preparations for conducting the focus groups aim at ensuring that the moderator will not be distracted. The moderator must be able to purely focus on the participants and the running of the focus groups. Therefore, all preparations must occur prior to conducting the focus groups (Krueger & Casey 2000).

Initial introduction and guiding questions will need to be prepared, so that the moderator can estimate the time required (Krueger & Casey 2000). The recording mechanisms must be in place, as well as the note taking equipment for the moderator.

4.3.7 Preparation

Planning of refreshments such as coffee, tea, water, biscuits, etc., needs to be organised before the participants arrive. It is essential to check the timeslot will not be interrupted by testing of fire alarms or similar unscheduled activities.

Before participants start arriving, all preparations should be completed, so that the moderator can focus on welcoming each participant. Guiding participants to the refreshments and introducing them as they arrive allows the moderator to act as a host. Through some initial small talk, it is anticipated that each participant would have been communicating with others prior to their seating. This atmosphere allows the participants to feel comfortable, and be more open to discussing the issues (Krueger & Casey 2000).

4.3.8 How many groups and saturation level

The literature recommends three to four focus groups, with six to eight participants in each group (Krueger & Casey 2000). However, the decision to continue conducting more focus groups is also determined by the saturation level. In the end, the saturation level is indicated by the amount of new information accumulated when going from group to group (Krueger & Casey 2000). When no further new ideas are forthcoming, the saturation level has been reached.

The group size recommended by Krueger and Casey (2000) of six to eight participants per focus group was targeted for this study. The participants are drawn from a wide area within the university to ensure an equal distribution of representatives of each section within each focus group.

4.3.9 Selection of participants

According to Morgan (1988), participants of a focus group must have something in common. The participants of this research have a number of things in common. They have been selected only from USQ. All participants have access to sensitive information. All participants have experienced the process of organisational restructure and change in procedures and responsibilities. ICT professionals have been and continue to be involved in securing computers and networks. The reduction and centralisation of staff at USQ resulted in loss of information and resources to cope with the demand. In addition, the compensation initiated new processes and system development. Staff members now have to learn about the new processes.

4.3.10 Ensuring participation

To ensure participation, the researcher made the process of inviting staff to participate as personal as possible. The study was described in a clear way, to avoid misunderstandings. Potential participants was made aware of the benefits and their experience to the study (Krueger & Casey 2000). Participation was purely voluntary, and followed the ethical clearance guidelines. The length of each focus group was set at between 60-90 minutes.

The setting of the date and time are essential in ensuring participation. The date must take into consideration business processing bottle necks that potential participants could experience as part of their work. Using the lunch hours would make potential participants more comfortable in volunteering their time, rather than using their working hours. Providing lunch at the focus group would also make it more inviting.

Location of the venue may also make a difference to participation levels. For instance, potential participants may not feel comfortable in rooms that have an observation mirror.

Rather, a normal meeting room that they would already be familiar with may be more suitable.

Assurance that participants would be able to withdraw their participation at any time may make them more inclined to initially volunteer to participate. Assurance of privacy and non-disclosure of sensitive information may also make them feel safer in participating.

Clear communication about these details, and follow up with participants prior to commencing the focus groups, may ensure increased participation (Krueger & Casey 2000).

4.3.11 Guiding questions

A focus group typically has a leader, called a moderator, who will have a list of questions and who monitors the discussion of the focus group. It is the responsibility of the moderator to ensure that the discussion does not divert from the topic, as well as ensuring that the flow of the discussion continues. It is essential though that the moderator does not in any way lead the discussion in a particular direction.

The introduction to the discussion aims to recapture the information that has already been provided to the participants through the invitation document. The following are examples of the guiding questions that the moderator may use:

- Social engineering is a technique whereby a person can gain information in a casual social setting that may help the person to gain unauthorised access to a computer system?
- What kind of situations could these be?
- How does this affect the sensitive data that we each work with?
- What kind of data is really sensitive?
- What would happen if this information would appear where everyone could access it?
- What kind of damage can social engineering cause?
- How could this be prevented?
- What are your experiences?

4.4 Leximancer 3.5

Leximancer is a software package that allows the researcher to pass a document through an automated analysis process. The result is available within minutes, providing a map that shows concepts, themes, and relationships between concepts. In addition to listening to the tape and reading the transcription, this is an efficient way to highlight and confirm general concepts and their themes.

Leximancer was developed by Dr. Andrew Smith from the University of Queensland, after seven years of research. This development was done by the ARC Key Centre for Human Factors and Applied Cognitive Psychology, through the ARC Key centre grant, between 1999 to 2004 (Drennan 2007; Martin & Rice 2007; University of Queensland 2010b).

It has been used by customers from various countries such as the USA, Canada, UK, Australia, New Zealand, Germany and Russia to name a few (University of Queensland). Its application has been used in diverse areas such as market research, defence, insurance, intelligence, law, pharmaceutical and health care (University of Queensland).

Leximancer was designed for the purpose of data mining and analysis, particularly for qualitative analysis, where data may be unstructured and textural (Blake 2008; Leximancer 2005; Martin & Rice 2007; Watson et al. 2005). Leximancer resolves the text into groups of words that form the seed concepts, where the seed concepts are linked to the relevant sentences within the text (Martin & Rice 2007). The machine learning optimisation approach of Leximancer uses the initial seed words to build the thesaurus using an iterative process to create the concepts (University of Queensland 2010a).

It is then determined how concepts are related to each other and what strength each relationship has. When concepts are close to other concepts within the text they are clustered concepts within themes (University of Queensland 2010a). This analysis process is not externally biased and allows the researcher to have a reporting mechanism that is not influenced by the researcher’s expectations (Drennan 2007; University of Queensland). The next process then determines how the concepts are related to each other and the strength each relationship has. Themes are concepts that are close to other concepts within the text (Drennan 2007). Connectivity of themes is indicated by related themes appearing together throughout the document. This relationship is shown by the concept map showing lines connecting circles, whereby the strength of the relationship is indicated by brightness of the line (University of Queensland 2005). Concept relevance is indicated by the proximity of the circles to each other. For example, if a large portion of a circle is shared with another circle, then the relevance of this circle is high compared to a circle that only shares a small amount with another circle (University of Queensland 2005).

Processing of large text files is automated and results are available within minutes. The result of the analysis is provided in the form of a visual concept map. It shows significant concepts in relationship to other concepts (University of Queensland 2005). The thematic circles containing the concepts are colour coded. The colour and its brightness, as well as the size of the circle, are indicative of the strength of the relationship (University of Queensland 2005). The area where circles overlap represents the relationship between these concepts.

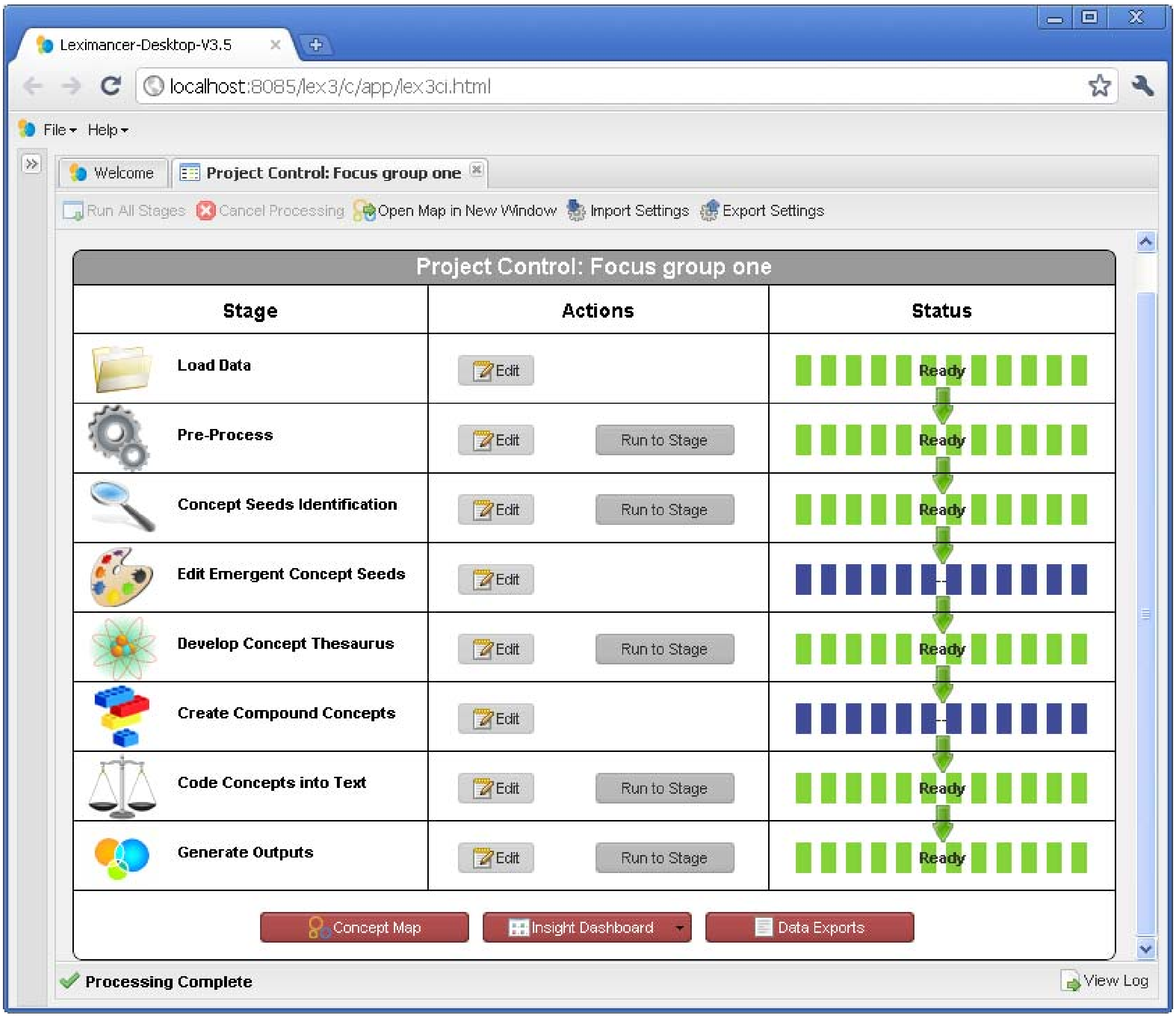
The brightness of the circle indicates the occurrence of the concept within the text (Leximancer 2005). The brightness of the link between the concepts reflects the strength of the association between these concepts (University of Queensland 2005). The colour green is used for names, such as people, and white for other objects.

On the concept map, the software provides the option to show more or less details of the concepts and the themes within the concepts by altering the setting of the percentage visible concepts, theme size, and degree of rotation bars.

4.4.1 Processing steps

The Leximancer software package uses predefined default settings for its analysis process. These default settings can be changed by the researcher to adjust for peculiarities in the data. For example, words that have the same meaning can be combined, and words that have no meaning can be removed.

When the project has been created in Leximancer, the software displays the Project Control Window, Figure 3. From here the researcher controls the processing of the analysis. The left column, Stage, shows the processing stages that Leximancer runs through. The column in the middle provides the control to the researcher on which action to take. The left button allows the editing of the settings, and the right button triggers the analysis process for the relevant stage. The researcher can either run each stage separately, or click on the last button to fully complete the analysis. The column on the right, Status, shows the researcher which stage is currently being processed.



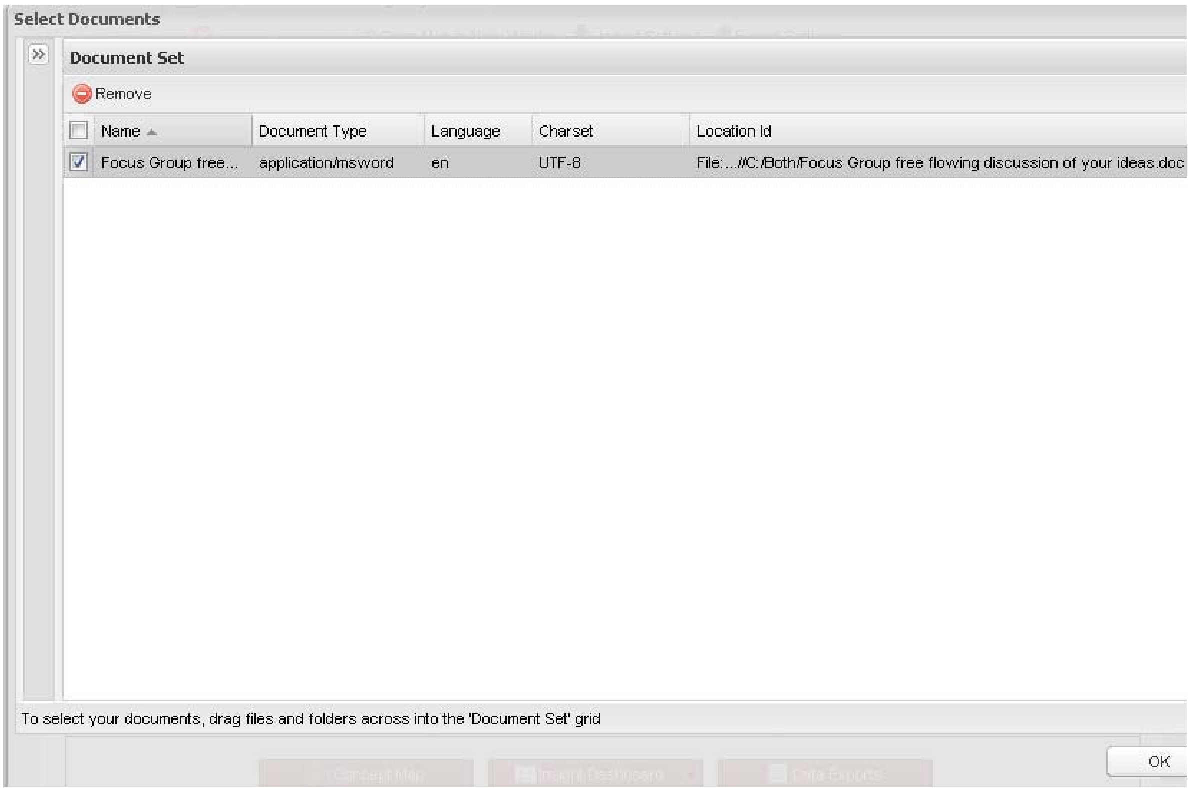
Project Control: Focus group one

Stage	Actions		Status
Load Data	Edit		Ready
Pre-Process	Edit	Run to Stage	Ready
Concept Seeds Identification	Edit	Run to Stage	Ready
Edit Emergent Concept Seeds	Edit		
Develop Concept Thesaurus	Edit	Run to Stage	Ready
Create Compound Concepts	Edit		
Code Concepts into Text	Edit	Run to Stage	Ready
Generate Outputs	Edit	Run to Stage	Ready

✓ Processing Complete

Figure 3: Leximancer - Project Control

The first step is to edit ‘Load Data’ where the researcher is required to point the analysis software to the relevant document. Here, the researcher must ensure that the correct file type is provided. The document is dragged from the directory into the Document Set window, Figure 4. At this stage, the checkbox needs to be ticked.

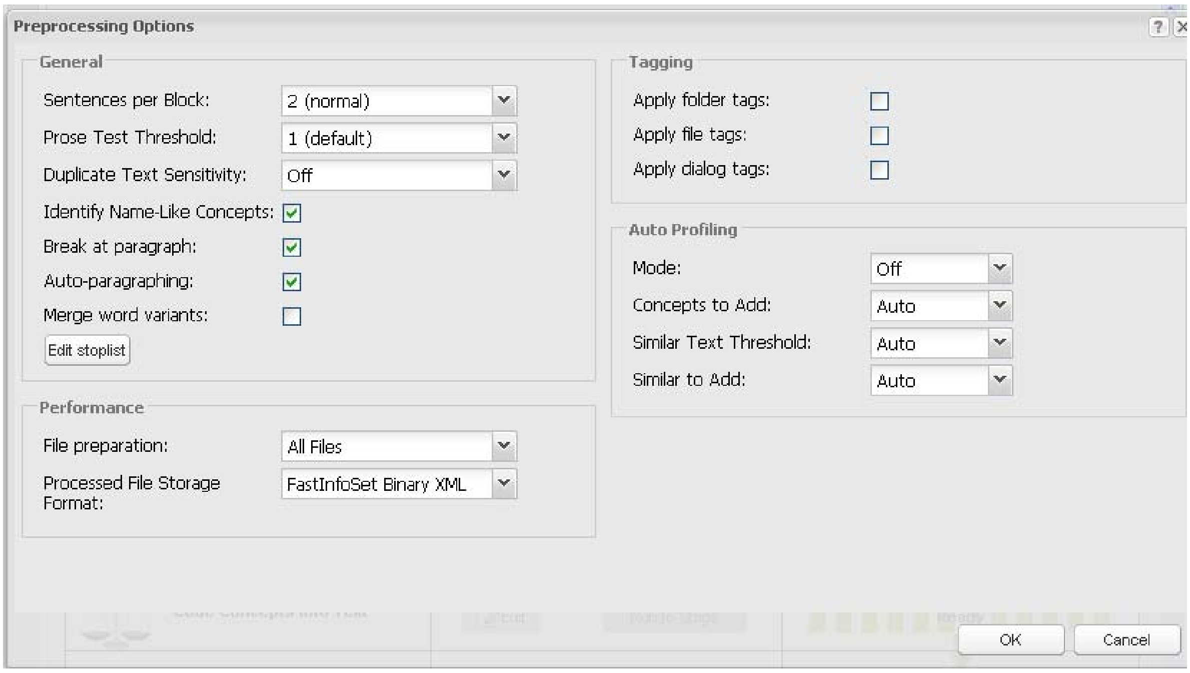


☐	Name	Document Type	Language	Charset	Location Id
☑	Focus Group free...	application/msword	en	UTF-8	File:.../C:/Both/Focus Group free flowing discussion of your ideas.doc

To select your documents, drag files and folders across into the 'Document Set' grid

Figure 4: Leximancer - Load Data

The second step is ‘Pre-Process’ where the document is segregated into sentences and paragraphs using the default settings shown in Figure 5. The document is transformed into an internal format suitable for Leximancer processing. Sections, such as sentences and paragraphs, are blocks that contain meaning. A block containing three sentences is regarded as limitation for relevant concepts. This step also removes punctuation and words with low semantic value that occur frequently. Any word within a sentence that starts with an upper case letter is interpreted as a proper name, such as company name. These are considered important in the mapping process. Non-text items are removed also, such as menus. As this also removes sentences containing less than one or two stop-list words, the option is recommended to be switched off when processing documents such as transcriptions.



General

Sentences per Block: 2 (normal)
Prose Test Threshold: 1 (default)
Duplicate Text Sensitivity: Off
Identify Name-Like Concepts: ☑
Break at paragraph: ☑
Auto-paragraphing: ☑
Merge word variants: □

Performance

File preparation: All Files
Processed File Storage Format: FastInfoSet Binary XML

Tagging

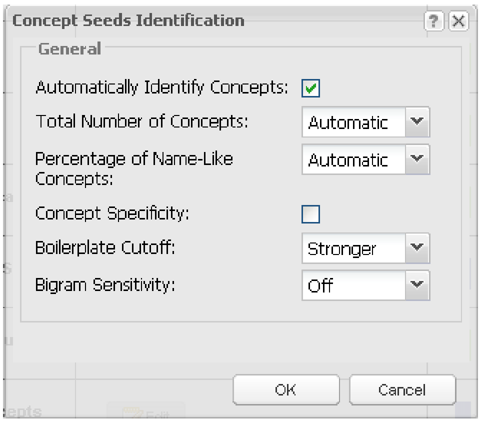
Apply folder tags: □
Apply file tags: □
Apply dialog tags: □

Auto Profiling

Mode: Off
Concepts to Add: Auto
Similar Text Threshold: Auto
Similar to Add: Auto

Figure 5: Leximancer - Pre-process

The third step is ‘Concept Seeds Identification’ which detects the seed words. Seed words are single words, and regarded as the starting point of a concept. They are automatically generated, but the researcher can also provide a list of seed words instead. The default settings shown in Figure 6 for this option can also be modified.

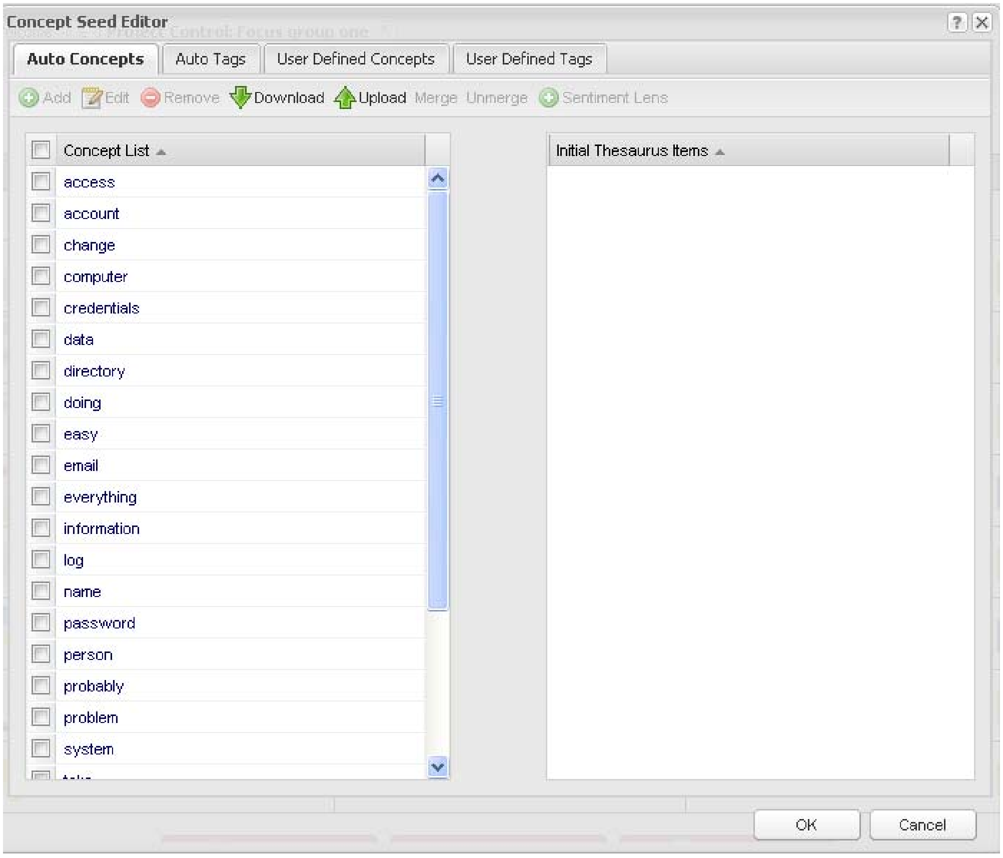


General

Automatically Identify Concepts: ☑
Total Number of Concepts: Automatic
Percentage of Name-Like Concepts: Automatic
Concept Specificity: □
Boilerplate Cutoff: Stronger
Bigram Sensitivity: Off

Figure 6: Leximancer - Concept Seeds Identification

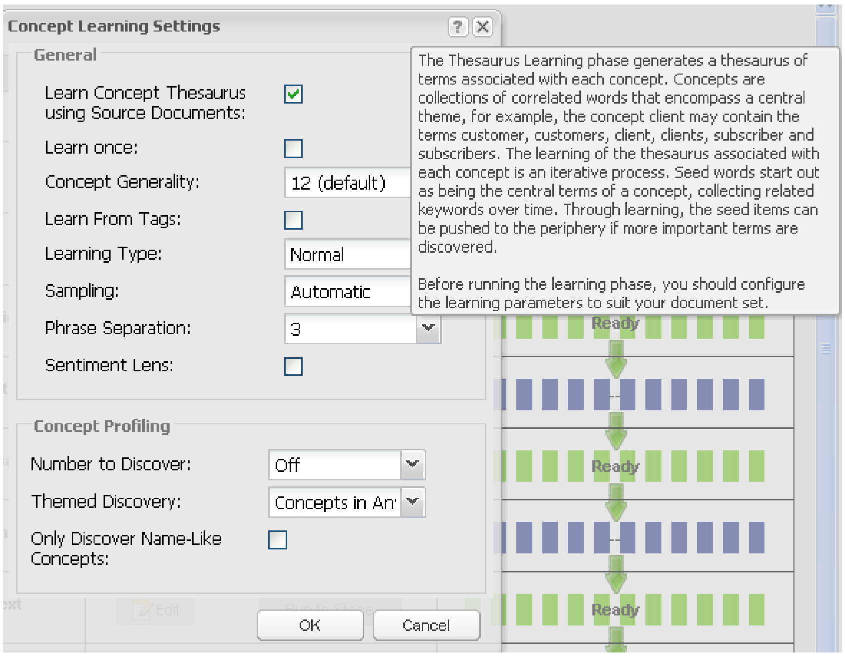
The fourth step is ‘Edit Emergent Concept Seeds’ and it provides access to the automatically generated seed words to allow the researcher to change these. Prior to the first run of the analysis process, this list is empty. It is generated from the words in the document under analysis. However, after the first and any subsequent processing, the concept seed list can be modified (Figure 7).



Concept List	Initial Thesaurus Items
□ access	
□ account	
□ change	
□ computer	
□ credentials	
□ data	
□ directory	
□ doing	
□ easy	
□ email	
□ everything	
□ information	
□ log	
□ name	
□ password	
□ person	
□ probably	
□ problem	
□ system	

Figure 7: Leximancer - Edit Emergent Concept Seeds

The fifth step is ‘Develop Concept Thesaurus’ and it builds a thesaurus from the seed words. As a seed word is the regarded as the point of a concept, subsequent repeat of running through the full analysis process then allows for other keywords to be collated. Here too, the researcher can modify the default settings (Figure 8).



Learn Concept Thesaurus using Source Documents: ☑

Learn once: □

Concept Generality: 12 (default)

Learn From Tags: □

Learning Type: Normal

Sampling: Automatic

Phrase Separation: 3

Sentiment Lens: □

Number to Discover: Off

Themed Discovery: Concepts in An

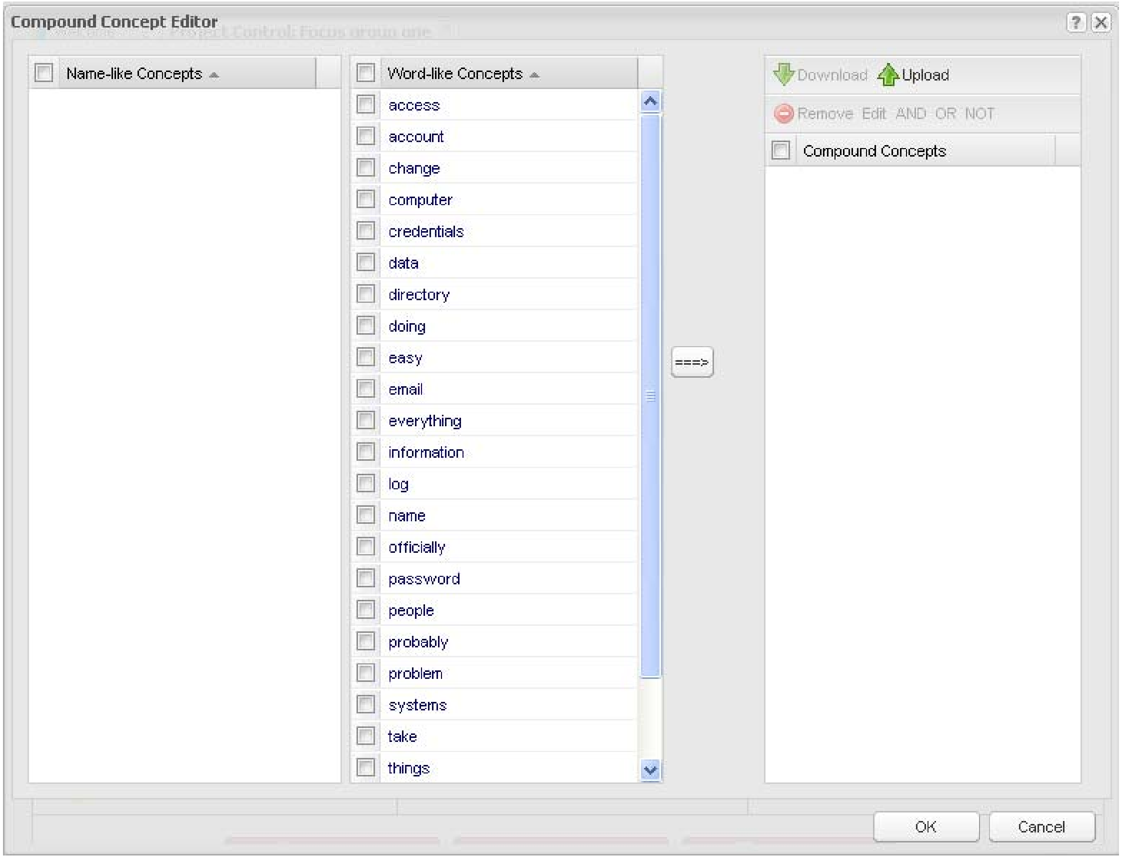
Only Discover Name-Like Concepts: □

The Thesaurus Learning phase generates a thesaurus of terms associated with each concept. Concepts are collections of correlated words that encompass a central theme, for example, the concept client may contain the terms customer, customers, client, clients, subscriber and subscribers. The learning of the thesaurus associated with each concept is an iterative process. Seed words start out as being the central terms of a concept, collecting related keywords over time. Through learning, the seed items can be pushed to the periphery if more important terms are discovered.

Before running the learning phase, you should configure the learning parameters to suit your document set.

Figure 8: Leximancer - Develop Concept Thesaurus

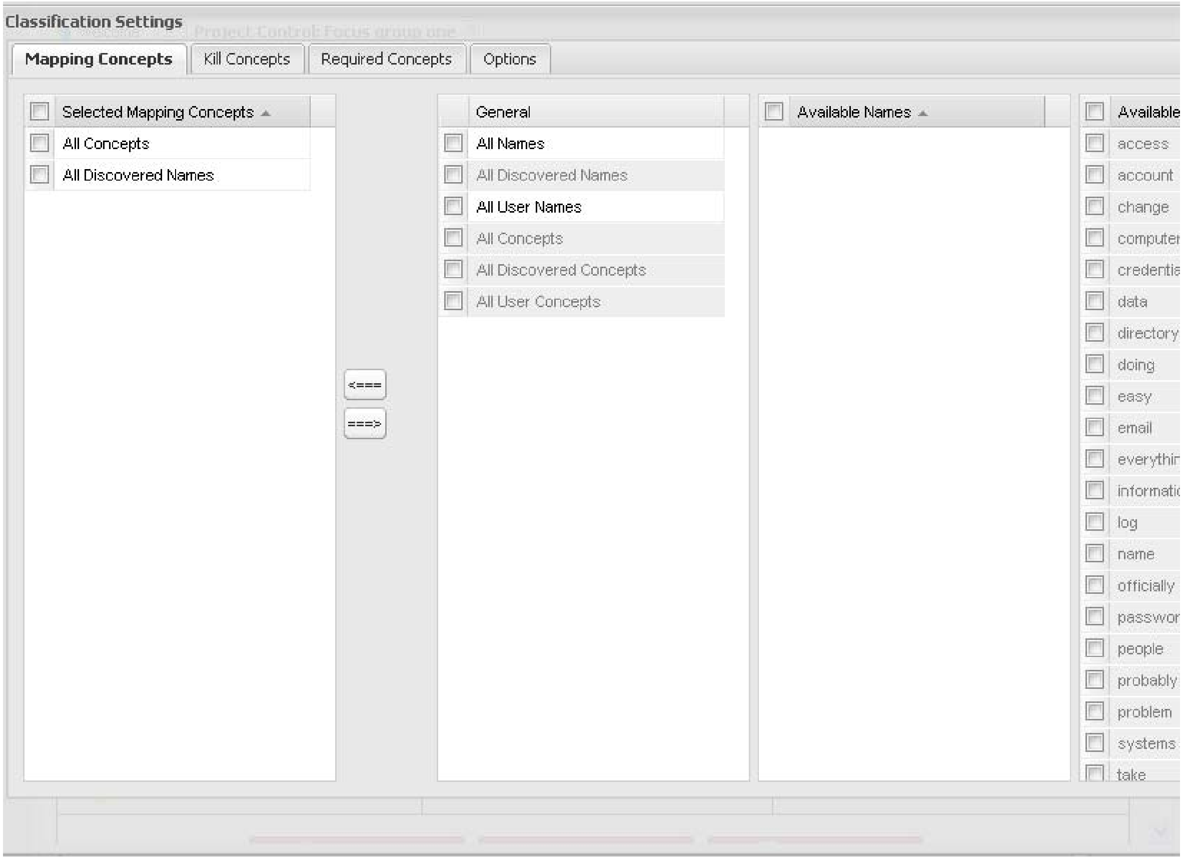
The sixth step is 'Create Compound Concepts' and it allows the researcher to manually combine concepts (Figure 9).



□ access
□ account
□ change
□ computer
□ credentials
□ data
□ directory
□ doing
□ easy
□ email
□ everything
□ information
□ log
□ name
□ officially
□ password
□ people
□ probably
□ problem
□ systems
□ take
□ things

Figure 9: Leximancer - Create Compound Concepts

The seventh step is 'Code Concepts into Text' and it refers to the concepts shown in the actual concept map. It allows the researcher to control automatically generated concepts or concepts provided by the researcher for display in the concept map (Figure 10).



Classification Settings

Mapping Concepts | Kill Concepts | Required Concepts | Options

□ Selected Mapping Concepts ▲

□ All Concepts

□ All Discovered Names

<===

===>

General

□ All Names

□ All Discovered Names

□ All User Names

□ All Concepts

□ All Discovered Concepts

□ All User Concepts

□ Available Names ▲

□ Available

□ access

□ account

□ change

□ computer

□ credentia

□ data

□ directory

□ doing

□ easy

□ email

□ everythir

□ informatic

□ log

□ name

□ officially

□ passwor

□ people

□ probably

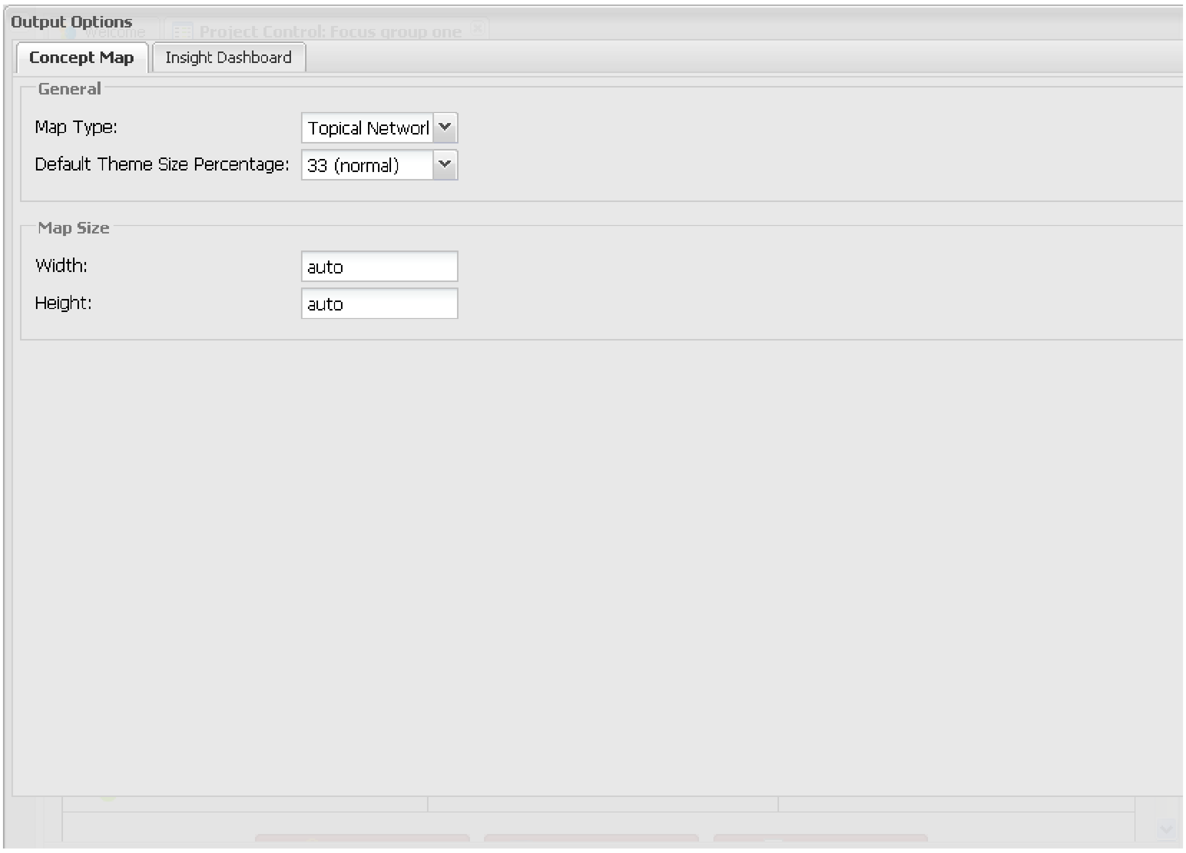
□ problem

□ systems

□ take

Figure 10: Leximancer - Code Concepts into Text

The eighth step is ‘Generate Outputs’ which builds the relationship between the concepts for the concept map. The default settings of the concept map output can be modified (Figure 11).



Map Type: Topical Networl
Default Theme Size Percentage: 33 (normal)

Width: auto
Height: auto

Figure 11: Leximancer - Generate Outputs

Once the researcher loads the document to be analysed, the first run of the analysis process through all the stages produces a concept map, the seed concepts and the thesaurus. This provides the initial underlying data analysis for the Concept Map, which the researcher can interrogate. The very first analysis allows the researcher to observe the unbiased result. For the document this is also the initialisation and learning process. If the researcher has identified certain data that needs to be edited, any of the corrective options can be used. The researcher can then use any of the editing functions to change the functionality. Once changes have been made, it is then necessary to re-run the analysis process in preparation for building the concept map. Each time the analysis is run, each of these steps is executed sequentially one after the other. This process can be started at the initial stage, or from any other stage onwards.

4.5 NVivo 8

NVivo is a software package that is used for qualitative research to help researchers organise their data (Basit 2003; Wong 2008). In qualitative research, the data is in written format, a result of a transcription of a focus group. The transcript is read and sections, sentences or paragraphs are organised. This process is called coding. In NVivo, the researcher has a software package that allows the researcher to import written material for the purpose of coding it. For the coding process the researcher will generate code names. These code names can either be created first or created as the researcher works through the document. The way to implement these codes can occur in two different ways, either by using a free node or a tree node.

NVivo is flexible in allowing the researcher to create the free nodes before the coding process or create free nodes during the coding process. The free node will need to be given a name that will identify the meaning of the section, sentence or paragraph from within the document. Any similar sections that reflect the meaning of the node name can then be added. This way the researcher can build a number of nodes that are free standing during the coding process. Free nodes have no logical connection.

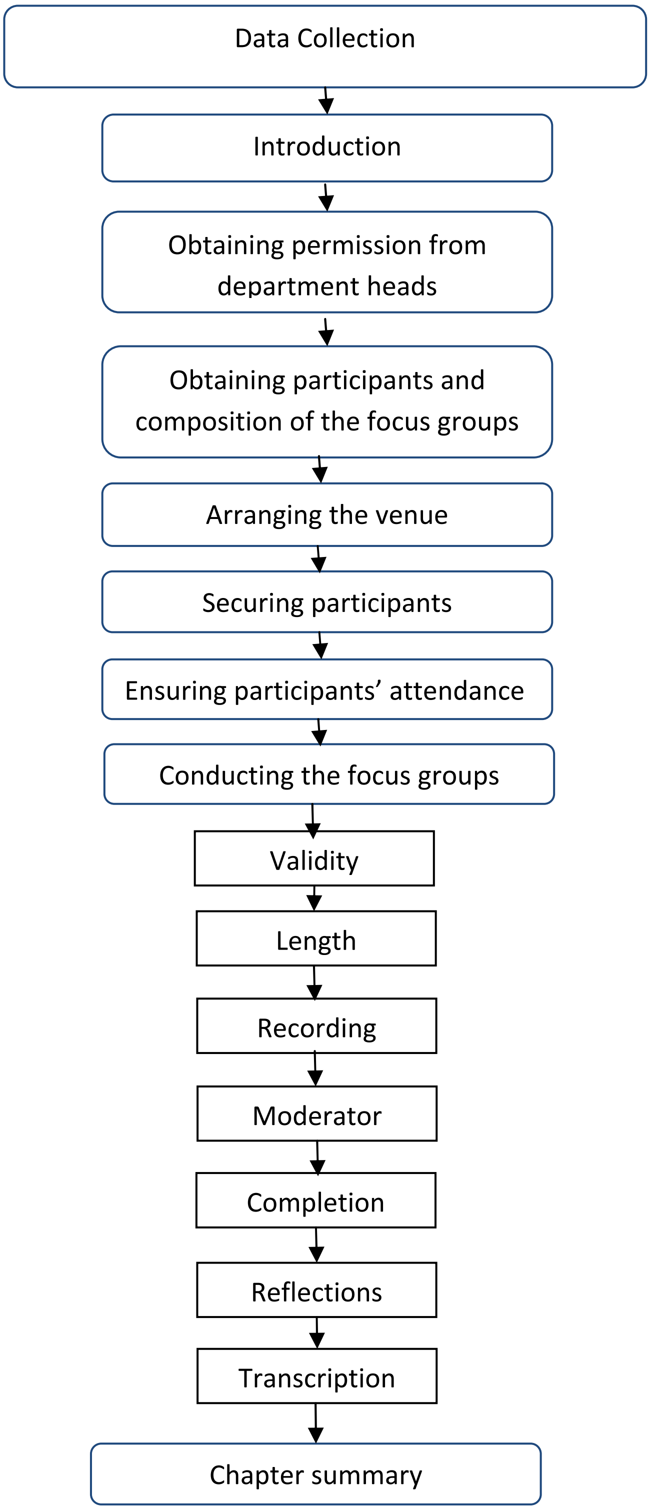
Tree nodes allow the researcher to create sub nodes in a hierarchical structure. This provides a means of organising the nodes as they related to each other. The tree nodes allow the creation of subsequent nodes that are hanging from the higher tree nodes. This way the nodes can provide a way of organising the data into various categories.

NVivo allows the researcher to use the software package in a flexible way. By either creating nodes before reading through the document, or by creating them as the researcher works through the document, the researcher has the freedom and flexibility of the manual process but with the benefit of electronic assistance. Depending on the need, the researcher can create free nodes first and then convert them into tree nodes.

4.6 Chapter summary

This chapter briefly outlined the philosophies considered for research in Information Systems. As this study attempts to determine an understanding of security awareness among staff members, the qualitative approach to the research methodology has been selected using interpretivism. Focus groups were identified as the most suitable data collection method for qualitative research. This chapter also discussed issues that a researcher needs to be aware of when conducting focus groups. It highlighted ways to ensure participation and the importance of providing an environment that will lead participants to be comfortable in discussing sensitive issues related to their work within the domain of this research. Other important considerations such as assurance of privacy, adherence to ethical clearance, and the freedom to withdraw from participation were also covered. As the discussions are intended to be recorded and then transcribed, two text analytical software packages, Leximancer 3.5 and NVivo8, were explained. Leximancer 3.5 will be used to obtain an unbiased initial analysis. NVivo8 will be used to conduct an in-depth pseudo manual analysis. As this involves slotting various transcript segments into themes, the mechanisms of free nodes (developing themes) and tree nodes (grouping themes) are explained. The next chapter describes the process of data collection in detail.

5 Data Collection



Data Collection
Introduction
Obtaining permission from department heads
Obtaining participants and composition of the focus groups
Arranging the venue
Securing participants
Ensuring participants' attendance
Conducting the focus groups
Validity
Length
Recording
Moderator
Completion
Reflections
Transcription
Chapter summary

Figure 12: Chapter 5 Data Collection

5.1 Introduction

Figure 12 provides a graphical representation of how this chapter is structured. Firstly, this research study uses focus groups to collect data for the qualitative data analysis. This chapter describes the steps taken in preparing and conducting these focus groups. As required for ethical clearance, permission to contact staff members was first obtained from department heads. The literature provided suggestions on the process of inviting participants and ensuring their attendance, the importance of the moderator, and the need for homogeneity of the groups. All discussions within the focus groups were recorded, and the number of focus groups was determined by the level of saturation. According to Breen (2006), saturation is achieved when the last focus group fails to generate any new ideas.

5.2 Obtaining permission from department heads

The research study is taking place at the University of Southern Queensland, in Toowoomba. It is a regional university in a large regional city located on the Darling Downs. It has a number of faculties and sections that provide services to the faculties.

The first step in the process of obtaining participants was to seek permission from the various department heads, listed in Table 1. These departments were chosen to ensure that each participant would have different levels of expertise while still being linked into the domain of this research (Krueger & Casey 2000). This approach ensures that each focus group consists of a similar mixture of participants, supporting homogeneity yet still sufficiently different to ensure generation of new ideas.

The Chief Technology Officer (CTO) was the first to be contacted by the researcher's supervisor. The CTO nominated two ICT staff members regarded as specialists in IT security matters. The researcher then called each subsequent department head listed in Table 1 personally. This allowed the researcher to establish good communication and be able to answer any queries immediately.

To ensure that each communication occurred in the same manner and each department head was given the same information, the researcher used the initial invitation document as a guideline for the conversation. As it was, the Principal Manager (Information Access) responsible for Library Administration requested that this invitation document and the consent form be sent through email. This document was immediately emailed to the Principal Manager, while the conversation was still fresh in the Principal Manager's mind. A written permission was then returned by the Principal Manager to the researcher. All other department heads gave their permission at the end of the respective telephone conversations.

Table 1: University department heads contacted

Department	Position
Division of Information and Communication Technology Services	Chief Technology Officer
Library Administration	Principal Manager (Information Access)
Faculty of Business Administration	Administration Coordinator (Academic Support/Assessment)
Student Management Division Marketing Services	Manager, eMarketing & Communication

5.3 Obtaining participants and composition of the focus groups

After all department heads had given their permission to contact their staff, the researcher generated an initial list of staff members. This initial list contained 20 staff to be contacted across these departments. Had the initial list not secured the appropriate number of participants, this list could have easily been extended. According to Morgan (1988) the participants for the focus groups must have something in common. This condition has been achieved, because the participants have access to information through the various corporate applications.

Each of the 20 staff members was contacted personally by the researcher through a phone call. From the initial 20 staff members contacted, 16 agreed to participate in the focus groups. As the presence and availability of the two nominated IT security specialists was crucial, the researcher called these two participants first. This lead to the nomination of the two dates for the focus groups. All subsequent participants were then assigned to one of these two dates, with the aim of equal distribution of staff members from the same areas across these dates. To ensure that each communication occurred in the same manner with each staff member, and the same information was provided, the researcher used the initial invitation document as a guideline for the conversation. Two of the staff members were unsure whether their professional knowledge would be helpful. However, after offering assurances that they were indeed experts within their own area of work increased their confidence, and they were then more inclined to participate.

While the process of personally calling each staff member took more time than sending a universal email, it did provide the researcher with a greater degree of control. Speaking with the participants allowed the researcher to immediately clarify any queries. It also allowed the researcher to determine which of the two dates would suit the participants, and retain control over an equal distribution of participants across the focus groups. The Student Management Division has only two staff members. Both staff members were working on the same project together and therefore both could only attend one of the focus groups. The researcher was also able to sign up two students to participate, one for each focus group. Overall, the researcher achieved the maximum recommended size of eight participants per group for both focus groups, as per the suggestion given by Krueger and Casey (2000). Each focus group had eight participants, with a representation of 3 male and 5 female for the first, and 4 male and 4 female for the second focus group (see Table 2).

Another benefit from personally calling each potential participant was that all participants were signed up within one working day. There was no delay in waiting for replies and sending reminders as would have occurred with email invitations. This allowed the researcher to immediately continue with further arrangements for the focus groups.

Table 2: Participants present at the focus groups

Department	**Tuesday** **31 August 2010**		**Wednesday** **1 September 2010**	
	Male	Female	Male	Female
ICT	1		1	
Library	1	2	1	
Faculty of Business Administration		3	1	2
Student Management Division				2
Student	1		1	
Total per gender	3	5	4	4
Total participants	8		8	

Once the participants were secured, steps were taken to ensure an uninterrupted continuation during the focus group discussion. The associate supervisor suggested enquiring whether there would be any fire drills on the days of the focus groups. Any fire drills occurring during the focus group session would have interrupted the flow of discussion, delayed the completion of the session or cut it short altogether as participants would be requested to return to their work stations. A telephone conversation with the appropriate professional staff member confirmed that there were no fire drills scheduled for the duration of these focus groups.

5.4 Arranging the venue

Once the participants were committed to the dates of the focus group, the researcher was then able to arrange the venue. On the same day as calling the participants, the researcher booked a suitable meeting room with sufficient space for the number of participants, and which would also convey a sense of a safe environment within which they could discuss issues freely.

At the same time, the researcher booked the recording devices. The associate supervisor suggested three recording devices to cater for problems such as battery failure, recorder malfunction, noise affecting clarity, etc.

For the convenience of the participants, the hot water urn and cold water jug were also booked. Tea, coffee, sugar, milk, and biscuits were also pre-arranged for these days. Through the university's refectory catering service, sandwiches and orange juice were ordered. To alleviate any complications it was requested the sandwiches and juice be delivered, as the researcher was also the moderator and had to be present at the time when participants arrived. The delivery of the lunch was also arranged toward the end of the focus group session to ensure there was a clean and focused start to the focus group and continuation of the discussion.

5.5 Securing participants

Once the venue was booked, the researcher set up meeting invitations with each participant individually. Rather than creating one meeting request with all participants, the researcher opted for a separate individual meeting request for each participant. While this took a small amount of effort, it also created a very personal invitation between the researcher and the participant. This prevented the participant knowing the size of the group, which may have made it easier to cancel their participation. It also created a very personal communication and agreement between the researcher and the individual participant.

Creating the individual meeting invitation allowed the researcher to control the participant's calendar, blocking out the relevant time slot to prevent future bookings impacting on the participant's availability. It also allowed control for an appropriate and timely reminder to be set on the invitation, as well as details about the venue of the focus group. In addition, the body of the meeting invitation presented itself as a perfect place for the invitation document and consent form to be copied into. Attaching the consent form also gave participants sufficient time to read and fill out the form prior to the meeting.

5.6 Ensuring participants' attendance

On the day prior to each focus group date, the researcher made another telephone call to each of the participants. This personal approach was another opportunity to show appreciation of their time and ensure their commitment. It also allowed the researcher to determine the day before the focus group meeting if there would be any cancellations on the day so that alternative replacements could be organised. This also reminded the participants of their commitment to the upcoming event, and prepared them so that the email invitation reminder on the day did not surprise them. There was only one participant who cancelled on the day.

5.7 Conducting the focus groups

The first focus group was conducted on Tuesday 31 August 2010, with 8 participants, and the second focus group was conducted on Wednesday 1 September 2010, with 8 participants.

5.7.1 Validity

To ensure validity in conducting the focus groups, the associate supervisor - who is experienced in moderating focus groups - attended both focus groups as an observer. As this was the first time the researcher acted as a moderator, the assistance created confidence and allowed for silent communication.

5.7.2 Length

The length of the focus group had been set to 90 minutes. For both focus groups, this seemed to have been a naturally appropriate time, as discussions continued strongly all the way through. Moreover, the researcher/moderator had to ensure that the focus group discussions would come to an end after 90 minutes so that participants could return to their duties.

5.7.3 Consent

Some participants had already emailed the signed consent form to the researcher, while others brought it along to the focus group session. The remainder were handed a consent form on the day of the focus group. This ensured that all participants had signed the consent form.

5.7.4 Recording

Three recording devices were equally placed across the table. The associate supervisor suggested using a book under each recording device to eliminate background noise transmitted from the table's surface. The researcher then welcomed each participant as they arrived. Required introductions were made, and small conversations started. This ensured that the participants felt comfortable with each other. The participants were offered refreshments of tea, coffee and biscuits, and then guided towards their seating.

5.7.5 Moderator

The moderator of these focus groups was also the researcher, which assured that the topic of research and the purpose of the focus group was clearly understood in accordance with the recommendation by Krueger and Casey (2000). As the participants began to settle in their seats, the associate supervisor started the recording devices, and the researcher/moderator started the focus groups with an introduction aimed to stimulate discussion among participants.

Participants had already been given the invitation document at the time of meeting invitation to provide them with an understanding of the research. Thus, the focus group was then lead into discussion without misleading or influencing their discussion.

As the discussion progressed, the moderator ensured that the participants stayed within the topics of the domain. When necessary, the moderator guided the participants by using relevant previously prepared questions to ensure continuation of the discussion and redirection when participants diverted away from the topic.

5.7.6 Completion

At the completion of each focus group (while the dialogue was still clear in the researcher's mind) notes and observations relating to the group's discussions were recorded by the researcher/moderator. Furthermore, to assist the researcher in the data analysis process, the seating allocation of each participant was also noted to assist in the recalling and interpreting of the discussions.

5.7.7 Reflections

Saturation was achieved with the second focus group, as there were no new ideas coming to light (Krueger & Casey 2000; Statistics Solutions 2011a). Both focus groups strongly focused on the same issues. While the first focus group differentiated its view about the issues through the experience of operational experience, the second focus group participants viewed the same issues from a managerial experience.

The researcher inferred from the conversation that some participants, due to their physical location, were isolated at work and this inadvertently resulted in others having access issues with data. Similarly, some participants expressed that due to custom applications, certain bottlenecks were encountered in communication aspects, resulting in breach of security protocols, commonly executed through email applications. These aspects are further discussed in the chapter 7.

5.7.8 Transcription

The researcher engaged a person who was skilled in transcribing focus group discussions. As this person had experience in transcribing, the risk of mistakes would be lessened. An experienced transcriber would also be able to produce the transcript at a much faster pace.

The digital recordings of the focus groups were handed over to the person transcribing. The recordings of the focus groups were stored on a USB drive. This drive was given to the person transcribing so that the transcriptions could be stored on it as well. In accordance with ethical requirements, the person was made aware that the material covered on these recordings was sensitive and highly confidential.

The transcriptions of the focus groups resulted in two separate Word documents, one for each focus group.

5.8 Chapter summary

This chapter explains the process of conducting the focus groups for the qualitative analysis of this research. Taking the extra effort to make the invitations personal allowed the researcher to quickly obtain a sufficient number of participants, within one working day. A good mixture of participants with similar skills and experience created homogeneity. Saturation was achieved with the second focus group as no new ideas were generated.

The next chapter will describe the process of the data analysis where, first, research concepts will be discussed followed by recapturing the concepts arrived from the literature, as well as formulating the research questions and propositions. This is followed by a detailed description of the data analysis procedures using Leximancer 3.5 and NVivo 8 for each of the focus groups followed by a combined analysis.

6 Data Analysis

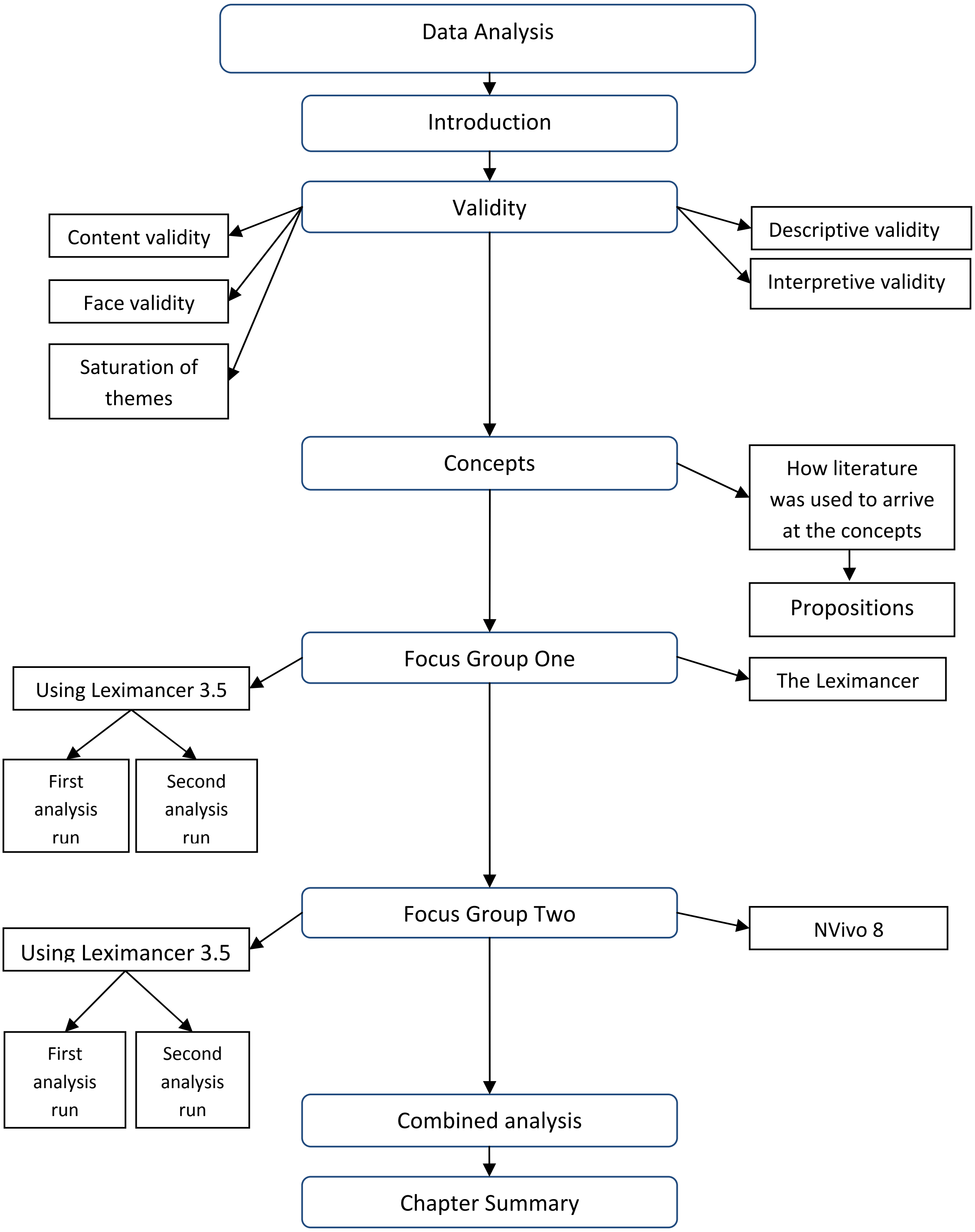


Figure 13: Chapter 6 Data Analysis

6.1 Introduction

Figure 13 provides a graphical representation of how this chapter is structured. Firstly, this chapter outlines the importance of validity to the process of data analysis. It then continues with describing the concepts as they relate to the literature, and then revisit the propositions to refocus on the research question.

The chapter then proceeds to the process of data analysis. Qualitative research uses content analysis, which means the written material is analysed to determine concepts. With the content analysis, the written material is evaluated for any words or phrases that may yield a concept. Rational analysis measures how the located concepts relate to each other, by showing them in a pictorial form. The resulting map therefore also shows the relationships between the concepts (University of Queensland 2010c).

Arriving at the data analysis stage, the researcher is already familiar with the transcriptions of the focus groups as they have been read by the researcher several times. The first exposure to these discussions by the participants occurred when the researcher conducted the focus groups. The researcher then listened to the recordings of the focus groups. Once the transcription process concluded, the researcher read through the transcription documents to obtain a deeper understanding in preparation for using Leximancer 3.5 and NVivo 8 for qualitative data analysis. Leximancer was used to first provide an independent and unbiased result of concepts extracted from the transcription documents (University of Queensland 2010c). NVivo was then used where the researcher manually coded sections while reading through the transcriptions. This dual process, using Leximancer and NVivo, aimed to ensure that the researcher reported the actual findings and thereby ensured descriptive validity (Hannes et al. 2010).

The analysis highlighted underlying ideas (Leedy & Ormrod 2005) and summarised the major findings of each focus group. Finally, the chapter concludes with an overall summary of the data analysis process.

6.2 Validity

In any research the researcher needs to continuously ensure that what is being measured is what the research should be measuring to ensure validity (Punch 2006). This requires constant vigilance on behalf of the researcher. Validity applies to many sections of research, such as research design, data collection, measuring instruments, and research reports (Punch 2006).

The moderator of focus groups is able to ensure validity by creating a neutral environment that will not influence the participants (Statistics Solutions 2011b). As this was the first time the researcher functioned as a focus group moderator, the associate supervisor attended all focus groups. To further ensure validity, great care was taken to create a good sample through the participants representing their section (Statistics Solutions 2011b).

6.2.1 Content validity

In order to conduct a proper content analysis, all material or content in written, audio, or visual format needs to be reliable and valid (Gurd & Palmer 2010; University of Texas 2010) and a vital part of this assurance is reliability and validity. Reliability can be ensured by verifying that different people arrive at the same concepts (Beattie et al. 2004; Weber 1990). Validity can be ensured by procedures of classification that reflects the researcher's expectation (Beattie et al. 2004; Weber 1990). Content validity ensures that the process of determining the concepts from the focus group is reflecting what the researcher is trying to measure (Ruane 2008).

6.2.2 Face validity

Face validity is the process of determining if the analysis of the concepts is correct (Ruane 2008; Zikmund 2000) and ensures that the researcher measures what is intended to be measured. Face validity, therefore, is a visual process to confirm that this is the case. According to Anastasi and Urbina (1997), "Face validity pertains to whether the test 'looks valid'" (1997, p. 117) and "what it appears superficially to measure" (1997, p. 117).

6.2.3 Saturation of themes

Saturation occurs when responses are consistent across focus groups (Krueger & Casey 2000; Statistics Solutions 2011b). This means that there are no further new ideas emerging in any subsequent focus group. Therefore, the saturation is an indicator for determining the number of focus groups required to ensure validity (Krueger & Casey 2000; Statistics Solutions 2011b).

In this research, saturation was achieved at the second focus group, as the second focus group discussed the same issues as the first focus group and did not generate any new ideas. The second focus group had the same responses to the guiding questions. Further, this research is exploratory in nature. Therefore, validity (Statistics Solutions

2011b), as well as the number of focus groups needed to be conducted, was ensured (Krueger & Casey 2000).

6.2.4 Descriptive validity

To ensure descriptive validity in qualitative research it is essential that the data is correct. This is done by avoiding distortion of data or misrepresenting it. Descriptive validity can be assured by providing the actual data from the transcription (Hannes et al. 2010). In this research, the transcripts were produced as they were, without any editing.

6.2.5 Interpretive validity

The researcher needed to ensure that interpretive validity was achieved during the analysis process and in this research this aspect was accomplished by reproducing the exact wording of the participants from the transcript (Hannes et al. 2010).

6.3 Concepts

A concept is sometimes described as being an idea or a construct about something that has been observed. The observation may be a process, an occurrence, or an object (Zikmund 2000).

Leximancer analyses textual data such as Word documents that contain the transcription of a focus group discussion. Leximancer then provides a concept map that shows the themes occurring in the document (University of Queensland 2010c).

6.3.1 How literature was used to arrive at the concepts

While a literature review was conducted, a number of themes pertinent to this study were identified. For example, Security awareness was identified by Choi et al. (2008) and the need to raise security awareness at management level within organisations was discussed by Manjak (2006) and Workman (2008). Similarly, the theme Unauthorised access was discussed in the literature by Nasheri (2003), Smith and Rupp (2002), and Walden (2005) as the process of gaining access to a computer system without having permission to do so. The Policies and Procedures with respect to security measures and their ongoing need, and appropriately supporting policies and procedures were discussed by Emanavin (2004). The concept Education and training was identified by Barrett (2003) and Mitnick and Simon (2002) as reducing the success rate of social engineering. Social engineering is used by hackers to obtain information from an employee through various social interactions (Mitnick & Simon 2002; Workman 2007, 2008).

6.3.2 Propositions

The research question and its propositions were covered in chapter 3. They are briefly repeated here to refresh the flow of thinking that is the background to this data analysis. The main research question raised in this study was:

> "How can education affect the process of preventing social engineering to minimise the success of unauthorised intrusion".

This research question resulted in the three following propositions, P1a, P1b, and P1c from the model depicted.

The proposition P1a identified employees' awareness of social engineering techniques and reads as follows:

> "Employees who are aware of the social engineering techniques through education are less likely to divulge information than employees who are unaware of social engineering techniques."

The proposition P1b identified consequences of employees' awareness of divulging information to unauthorised people and reads as follows:

> "Employees who are aware of the consequences through education of social engineering are less likely to divulge information than employees who are unaware of the consequences."

The proposition P1c combined the above two aspects and reads as follows:

> "Employees who are aware of both the social engineering techniques and the consequences through education of social engineering are less likely to divulge information to anyone than employees who are unaware of about social engineering techniques and the consequences."

The qualitative data analysis conducted in this study mainly targeted these propositions and the main research question posited. The theme generation and concept formation centred on the awareness in the participants about social engineering techniques and social engineering consequences, in other words, the giving away of data or information, and the need to educate staff on this aspect. The study initially used Leximancer to identify appropriate and relevant themes and then used NVivo to determine the presence of these themes as NVivo provided facilities for manual in-depth analysis (Statistics Solutions 2011b). The analysis procedures are described in detail in the following sections.

6.4 Focus Group One

The transcription from the first focus group was used in an analysis by Leximancer 3.5 to obtain an unbiased result. The text transcription was loaded into Leximancer and an analysis was conducted using the predefined default settings within Leximancer. This provided the first concept map for this focus group, visually highlighting concepts that allowed changes to the default settings. The changes were documented within the second analysis run. The final concept map was then analysed in accordance to the more relevant concepts identified on the concept map. The researcher then used NVivo 8 to manually code the same transcription of the first focus group, by creating free nodes. These free nodes were then converted into tree nodes. This allowed the researcher to create a tree node for this focus group.

6.4.1 Using Leximancer 3.5

Qualitative research uses content analysis, which means that written material is analysed to determine concepts. With conceptual analysis, the written material is evaluated for any words or phrases that may yield a concept. Rational analysis measures how the located concepts relate to each other. The resulting map also shows the relationships between the concepts (University of Queensland 2010c).

Leximancer was firstly used to obtain an independent and unbiased analysis. As the researcher had already worked through the literature and the research question and its proposition, obtaining an independent and more so unbiased analysis result would ensure the validity of this research.

The analysis process of Leximancer is unbiased because it builds concept seed words from the document itself. When Leximancer analyses a textural document for the first time it starts without a list of seed words. As Leximancer works through the document it gradually builds a new list of seed words from the contents of the textural document. The result of the analysis provides a concept map that shows themes as circles, and the concepts within the themes. The researcher can then interrogate the graphical representation of the textural document to gain a better understanding of its components. The concept map also has tabs to the right which provide more detailed statistical information to the researcher.

The use of Leximancer is relatively easy, as it comes with default settings. After providing the textural document to Leximancer, the whole analysis process runs fairly quickly. This provides the researcher not only with an unbiased result, but also a quick idea of the contents of the document.

As outlined in chapter 4, the researcher can interact with the map by changing the percentage of the theme size, degree of rotation and visible concepts within the themes. This does not affect the concepts or meaning in any way. It allows the researcher to either get a birds-eye view by decreasing the percentage, or obtain a much closer look and more detail by increasing the percentage. A subsequent re-run of the analysis process will then use the existing seed words and re-analyse the textural document producing a new concept map.

Each circle on the concept map represents a theme, and contains a number of concepts. The size and colour of the circle are indicators about the relevance of the theme. In addition to that, when circles overlap, they share some commonalities.

6.4.1.1 First analysis run

A new folder was created in Leximancer to contain the project for the first focus group. The Word document containing the transcription for the first focus group was added. The first run creates the list of concept seeds that can be accessed through the ‘Edit emergent concept seeds’.

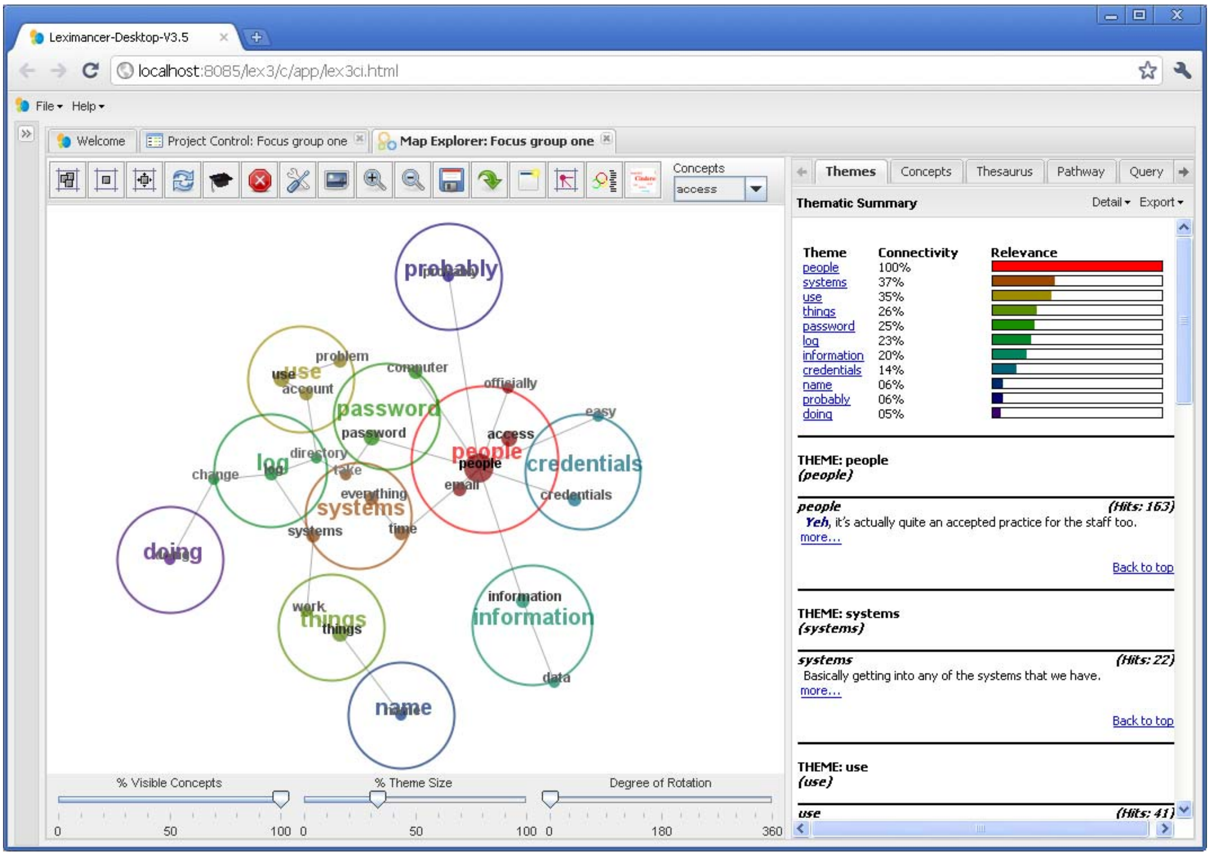
Running the transcription of the first focus group through Leximancer for the first time identified two words, ‘yeh’ (with a lower case letter y) and ‘Yeh’ (with an upper case letter y). The option ‘Edit emergent concept seeds’ was used to remove these two words from the analysis process. The reason that these two words were removed from the analysis process is that they do not have any meaning to this research.

Further investigation of the concepts resulted in additional changes. The concepts ‘email’ and ‘emails’ were merged into ‘email’. The concepts ‘guys’, ‘person’, ‘people’, ‘someone’, ‘staff’, ‘student’, and ‘students’ were merged into ‘people’. The concepts ‘stuff’ and ‘things’ were merged into ‘things’. The concepts ‘system’ and ‘systems’ were merged into ‘system’. The concepts ‘use’, ‘used’ and ‘using’ were merged into ‘use’. These concepts were merged together for the purpose of lemmatisation. This allows these merged words to be analysed as one word.

No other changes were made that would adversely influence the analysis.

6.4.1.2 Second analysis run

Running the analysis again resulted in the concept map shown in Figure 14. Each theme is represented by a circle. Each circle uses a different colour to differentiate between other themes. The brightness of the circle indicates how often it occurs within the document (University of Queensland 2010c). Warm colours such as red or orange indicate a high level of relevance, and cool colours such as blue indicate least amount of relevance (University of Queensland 2010c). The concept map with the 'Visible Concepts' was also increased to 100%, showing the concepts within each thematic circle.



Thematic Summary

Theme	Connectivity	Relevance
people	100%	
systems	37%	
use	35%	
things	26%	
password	25%	
log	23%	
information	20%	
credentials	14%	
name	06%	
probably	06%	
doing	05%	

THEME: people
(people)

people ***(Hits: 163)***
Yeh, it's actually quite an accepted practice for the staff too.
more...

Back to top

THEME: systems
(systems)

systems ***(Hits: 22)***
Basically getting into any of the systems that we have.
more...

Back to top

THEME: use
(use)

use ***(Hits: 41)***

Figure 14: Leximancer concept map - Focus group one - visible concepts

6.4.1.2.1 Theme 'people'

The Leximancer concept map in Figure 14 shows the theme 'people' as a circle in the warm colour red. In Leximancer, colours are used to communicate if a theme is least or most relevant. Warm colours such as red and orange in Leximancer are given to most relevant themes (University of Queensland 2010c). This theme 'people' is also positioned closer to the centre of the map, indicating importance (University of Queensland 2010c). In addition, it has lines radiating from it to other themes, showing the connections between themes, as well as the origin from which these other themes relate. The thematic summary, Table 3, shows 100% connectivity for theme ‘people’, and the ranked concepts, Table 4 shows 100% relevance with a count of 163.

Table 3: Leximancer thematic summary from Figure 14 - Focus group one

Theme	% of Connectivity
people	100
systems	37
use	35
things	26
password	25
log	23
information	20
credentials	14
name	6
probably	6
doing	5

The participants of this focus group have used various words representing ‘people’. When lemmatisation is applied, merging similar words into one word resulted in the theme ‘people’ as the most relevant as identified by Leximancer. For focus group one, the theme ‘people’ consists of ‘guys’, ‘person’, ‘people’, ‘someone’, ’staff’, ’student’, and ‘students’, as they had been merged into ‘people’ through the option ‘Edit emergent concept seeds’.

However, in the majority of cases, the theme ‘people’ would refer to either ‘student’ or ‘staff’ member. Where the word ‘student’ or ‘staff’ is used explicitly it clearly defines the category of people. The more general reference to ‘guys’, ‘person’, ‘people’, ‘someone’ may be related back to either ‘student’ or ‘staff’.

Table 4: Leximancer ranked concepts - Focus group one

Concept	Count	Relevance percentage
people	163	100
access	50	31
things	49	30
use	41	25
information	37	23
password	30	18
email	22	13
systems	22	13
time	22	13
credentials	20	12
work	19	12
data	19	12
log	18	11
everything	18	11
probably	18	11
name	17	10
account	16	10
computer	15	9
problem	15	9
doing	15	9
officially	14	9
change	12	7
directory	11	7
easy	11	7
take	9	6

In this example, the use of 'staff' refers to an IT staff member, and is also referred to as 'guys', implicitly related to as 'someone' and 'person', all referring explicitly or implicitly to the 'staff' member.

> [1]*How much checking is in place for IT staff as well? I know we're are all like yeh we're the good guys trying to protect everything, but if someone goes rogue, they can do a lot of damage and a lot of time they are the only one who has worked or this system and only person who knows how it works.*

[1] Participant discussions, presented to support the findings, are in italic and boxed, as per original transcription.

However, in some examples ‘guys’, ‘person’, ‘people’ and ‘someone’ could also be another group other than ‘staff’ and ‘students’. ‘Guys’ is a phrase used when someone refers to a non-specific person, as found in focus group one, when discussing the Russian Business Network.

> *So there’s these same guys Russian Business Network that actually built a great tool called EMPAC, which is an elmware packaging tool, they sell, I brought a copy for 5 Euros and it enables you to actually package up, launch this code and unique signature set so that, you know, it’s not going to get picked up by any virus signatures. They are very sophisticated guys that are vertically integrated within the government and they got their [2]*** together so you will see more intelligent spam*

When the word ‘person’ is used, again the participants were not referring to a specific person. In the following example though, it can be seen that the ‘person’ here would more likely be a staff member, as only staff members can access SharePoint.

> *It’s not only that, it’s SharePoint as well. We can say I want this person to have the same permission as me*

When the word ‘staff’ is used, then participants are directly referring to someone employed at the university.

> *Sometimes though when you get a new member of staff they don’t have access. We had a staff member join us for about a 4 week period, and nearly 3 of those 4 weeks she didn’t have any username or password, so it was pointless having her there because she couldn’t do anything.*

When the word ‘student’ is used then participants are directly referring to a student in their discussion.

> *What I see is 99% of the time simply students providing other individuals with their credentials. And that’s a commonly accepted practice, particularly with *** students, particularly with students from ***, ***, *** and those areas who have a community spirit of sharing what they have with their fellow students.*

[2] *** is used throughout this document to remove confidential information.

In summary, the Leximancer concept map in Figure 14 shows the theme ‘people’ central with other themes radiating from it. The thematic summary, Table 3, shows 100% connectivity for theme ‘people’, and the ranked concepts, Table 4, shows 100% relevance with a count of 163. Lemmatisation resulted in where ‘guys’, ‘person’, ‘people’, ‘someone’, ’staff’, ’student’, and ‘students’ being grouped into ‘people’.

The participants’ discussion using the word ‘people’ related to staff being referred to also as ‘guys’ or ‘someone’, ‘guys’ used to refer to people at a Russian Business Network, ‘person’ used when implicitly referring to a staff member, ‘staff’ used to refer to staff member, and student used to refer to students in general.

6.4.1.2.2 Theme ‘credentials’

The Leximancer concept map in Figure 14 shows that the theme ‘credentials’ is positioned to the right of the theme ‘people’. These two themes overlap and therefore are indicating a direct relationship. The more circles overlap the stronger their relationship as they share commonalities. The thematic summary, Table 3, shows 14% connectivity for theme ‘credentials’, and the ranked concepts, Table 4, shows 12% relevance with a count of 20.

When participants use the word ‘credentials’, it implies to mean the username and the password. A ‘credential’ is therefore a way to gain access to a system, as all systems require two parts to the identification, a ‘user name’ and the secret code, a ‘password’. The credentials are unique for each user to identify the individual. The credentials also have a specific combination of access levels and permissions assigned to this particular individual. In focus group one, a participant stated that:

> *So you know as a student, when you want to access the Internet, you open up the browser and you have to type in your user name and password first. Yeh, so that’s just logging in your credentials to property server to provide you access to the Internet.*

From the above statement, it can be seen that the word ‘student’ belongs to the theme ‘people’ and the ‘user name’ and ‘password’ are equivalent to the theme ‘credentials’.

Therefore, this confirms that the overlapping of the two circles representing the theme ‘people’ and ‘credentials’ indeed have something in common. It also highlights that it is inferred that ‘credentials’ are providing access to the Internet as considered from the ‘student’ point of view.

The participants of focus group one were very compassionate about people sharing their 'credentials'.

Participants discussed that staff would share credentials as a necessity to get their work done, as new 'staff' members "don't have access", as it took nearly 3 out of 4 weeks to get a 'username' and 'password'. Without sharing the credentials, the new staff member "couldn't do anything".

> *Sometimes though when you get a new member of staff they don't have access. We had a staff member join us for about a 4 week period, and nearly 3 of those 4 weeks she didn't have any username or password, so it was pointless having her there because she couldn't do anything.*

Some participants said they were aware that some staff would share their 'credentials' when going on leave.

> *Yeh, they go on holiday and they say here are my credentials.*

Participants said that a 'high degree of trust' was needed when providing 'credentials' to a new staff member to do the work they were employed to do.

> *So I guess the thing is in giving her somebody's credentials, so you give her your credentials you're then placing a high degree of trust in her. Which absolutely exposes you to risk and University risk.*

Participants highlighted that while 'sudo' (pseudo) accounts are available, staff members may not be aware of this option and instead give their own 'credentials' so that visiting scholars have access.

> *Even when you do have accounts available like those sort of 'sudo' type accounts. If staff members don't know about it, they do very freely give their credentials especially to visiting scholars to allow them to have access straight away.*

One participant suggested providing 'feedback' rather than sharing 'credentials' to resolve the problem of slow 'turn around'.

> *I agree with you 100% and one of the best ways to improve your situation is actually not provide people with your credentials but to give us feedback. Loud and clear 'hey the turnaround time is, ***, it's not good enough.*

Participants suggested a large percentage of students would share their ‘credentials’ with other ‘*** students’ due to ‘community spirit of sharing’.

> *What I see is 99% of the time simply students providing other individuals with their credentials. And that’s a commonly accepted practice, particularly with *** students, particularly with students from ***, ***, *** and those areas who have a community spirit of sharing what they have with their fellow students.*

Participants discussed that students using lab computers to print, may walk off to pick up their printout while still logged in. This would allow someone to gain unauthorised access by using the ‘credentials’ of that person.

> *It logs off after *** minutes but there is a window of someone sitting down on a continual basis and using that persons credentials. They’re real issue, from staff and students.*

The participants of focus group one related ‘unauthorised computer access’ to ‘credentials’.

> *So the majority of unauthorised computer access we see is just simply credentials being used.*

In summary, the Leximancer concept map in Figure 14 shows the theme ‘credentials’ is connected to the theme ‘people’, with both themes overlapping and indicating a relationship. The thematic summary (Table 3) shows 14% connectivity for theme ‘credentials’; and the ranked concepts (Table 4) shows 12% relevance with a count of 20.

Participants used the word ‘credentials’ when discussing issues related to students considering ‘credentials’ as access to the Internet, new employees who did not have their own credentials for three out of their four weeks of employment, staff on holidays passing their credentials to colleagues, how sharing of credentials is based on a high degree of trust, being unaware that sudo (pseudo) accounts exist leads to sharing of credentials, advice not to share credentials and reporting issues resulting from that, sharing of credentials among students with community spirit of sharing, someone else using a computer within the *** min log off period, and these issues constitute the majority of unauthorised computer access related to credential sharing.

6.4.1.2.3 Theme 'password'

The Leximancer concept map in Figure 14 shows the theme 'password' connected to 'people', with 25% connectivity, shown in thematic summary (Table 3); and 18% relevance and a count of 30 shown in the ranked concepts (Table 4). The theme 'password' is not connected to the theme 'credentials', which is connected to the opposite side of the theme 'people'.

Participants used the word 'password' when discussing crossed out passwords still being visible on the photocopier.

> *I've been getting copies of the refresh, and the password is crossed out, but the photocopier you can actually see the password still.*

Here the participants are using 'password' together with 'username' when discussing the benefit of knowing the students' 'password' and 'username' for situations where a staff member may need to resolve issues for the student.

> *I must admit it does help for troubleshooting but, yeh that would be one thing that I am aware of students sort of freely handing out their username/password.*

Participants indicated their understanding that to steal an 'identity' both 'password' and username are needed.

> *So that's what people are interested in though, stealing your identity.*
> *Getting the password.*

Participants also used the word 'password' when discussing the requirements of *** day password expiry as a result of an audit.

> *We did have an audit and one of the requirements was that we had to have an improvement in our password policy. One of those things was the *** day expiry.*

Participant also discussed students complaining about not having sufficient access and students being too free in volunteering their 'username' and 'password'.

> *I don't think we're aware of too much abuse. I know we get emails from students complaining they can't get into various things, and they will say I'm using my UConnect login which is: username and my password, and we think " no , no don't tell me this!"*

In the focus group discussion, participants also considered email as a way that someone could obtain a ‘password’.

> *So, it would be pretty easy for someone to say I’m from the USQ and send a few emails and then next email say, ‘what’s your password, what’s your address?’*

Participants also discussed the ‘password’ in conjunction with the process used to reset a ‘password’.

> *So her um, her Gmail account got hacked simply because the 3 questions that you use to password reset were things that were publically researchable information. So one of the questions was: What was your boyfriends, first boyfriends' name?*

In summary, the Leximancer concept map in Figure 14 shows the theme ‘password’ connected to ‘people’, with 25% connectivity, shown in thematic summary (Table 3); and 18% relevance and a count of 30 shown in the ranked concepts (Table 4). The theme ‘password’ is not connected to the theme ‘credentials’, which is connected to people on the opposite side to ‘password’. Participants used the word ‘password’ when discussing crossed out passwords still showing up on photocopiers, students freely handing out their username and password, stealing identity, audit review requirements, students’ complains about insufficient access, email as a potential source to obtain passwords and resetting of passwords.

6.4.1.2.4 Theme ‘systems’

The Leximancer concept map in Figure 14 shows the theme ‘systems’ as connected to theme ‘password’. The thematic summary (Table 3) shows ‘systems’ with a 37 % connectivity, and the ranked concepts, (Table 4) with 13 % relevance and a count of 22. The theme ‘systems’ is also shown by Leximancer in a light orange colour, where the colour is indicating more relevance. The theme ‘systems’ is connected to ‘password’ and from ‘password’ to ‘people’.

The participants of focus group one have used the words ‘system’ and the plural ‘systems’. When lemmatisation is applied, merging similar words into one word resulted in the theme ‘systems’ as the most relevant as identified by Leximancer. For focus group one, the concepts ‘system’ and its plural ‘systems’ have been merged into ‘systems’ through the option ‘Edit emergent concept seeds’. Participants are using the word ‘system’ or ‘systems’ when they are referring to software, desk top computer, server on the network, a systems person, operating system, web application, or corporate systems.

Participants stated that a ‘system’ can be sophisticated, and that the extent of its sophistication is based on the funding and resource made available to it, but that there is still the ‘education’ that can make a difference.

> *There’s the sophistication of the system which is one, which I believe is controlled to a certain extent obviously based on funding and resources. The flip side is education.*

The participants also refer to ‘systems’ during their discussion as the desktop computer.

> *But it’s for the desktop level that’s quite different though. As a desktop technician and we’re getting a lot of sub-contracting guys now who come in and refresh systems.*

The participants also used the word ‘systems’ to refer to a number of corporate applications.

> *It’s an evil sometimes we do have to live with but from our perspective we don’t do that at all internally. Yeh we need to have user’s identity, being either their *** or *** so say for example we have external contractors they come and have high level access to our corporate systems, so finance, HR, they will have 24/7 access.*

The participants also used the word ‘systems’ in conjunction with ‘password’ when referring to the refresh cycle.

> *So they should be getting this when their system is refreshed, by ICT, no matter how much you might trust that person, they should be changing the password. The biggest compromise, and what I’ve been wanting to talk to ICT about anyways is the MFD’s updaters.*

Alternatively, Leximancer shows that participants also used the word ‘systems’ to refer to a server.

> *You’re bang on there. It’s basically because prior to our new IBM system, we actually had a way of doing manual intervention, and you could come and say ‘hey look it’s really important, the person starting today, sorry can you do something about it right now?’*

In addition, participants also referred to staff working in the IT department as a 'systems' person.

> *Try it with a systems person. We have to go through hoops to get firewall access forms filled out for every piece of equipment they have to access.*

In another scenario, 'system' was used to refer to the operating 'system' of a computer.

> *But it would take away a lot of your academic freedom, and would mean that you wouldn't have freedom to you know experiment, with different operating systems and run whatever applications you choose being an administrator of your machine. There are a whole range of things.*

A web application is also sometimes referred to by the participants as a web 'system'.

> *I know you've got like a web system behind it, but you can still do everything from the email. So you don't need to go to the web system to log in and do all that.*

In summary, the Leximancer concept map in Figure 14 shows the theme 'systems' connected to 'password', with a 37% connectivity shown in thematic summary (Table 3); and 13% relevance with a count of 22, the ranked concepts (Table 4). The circle on the concept map for this theme is coloured in light orange indicating more relevance. Lemmatisation grouped 'system' and 'systems' into 'systems'. Participants used the theme when discussing system in general as opposed to education, using system to refer to desktop computer, corporate application, refresh cycle, server, system's person, operating system, and web systems.

6.4.1.2.5 Theme 'information' and concept 'data'

The Leximancer concept map in Figure 14 shows the theme 'information' connected to the theme 'people'. The theme 'information' also contains the concept 'data', at the far edge of the circle. The colour of the circle is light green, which in Leximancer is used for cooler colours indicating less relevance. The concept map also shows the circle to be fairly distant from the circle 'people'. The theme 'information' is not connected to any other circle. The thematic summary Table 3 shows 'systems' with a 20 % connectivity, and the ranked concepts, Table 4, with 23 % relevance and a count of 37, with ‘data’ 12% relevance and a count of 19.

Leximancer shows that participants were discussing that ‘information’ could be found on Facebook.

> *All the information is up there on Facebook.*

Participants also discussed ‘information’ in regards to it being harvested by a script from a web page.

> *So we have, we regularly see that one page being heavily attacked, from all over the world. Mostly through scripted lots that are trying to harvest information.*

Participants also used the word ‘information’ when they were referring to copying eBooks.

> *Our eBooks, was copying, you’re only supposed to copy so much, he had worked out a way of copying the books. We ended up getting notified, and said ‘Oh, I just kept on going, I just wiped out the information and put it back again” He copied most of the book.*

Participants also used the word ‘information’ when discussing the details needed for identifying a person.

> *Can’t find out more detailed information like address, contact numbers for them, you know things that are more detailed attributes that can truly validate the identity over the phone. It’s very difficult to successfully do that.*

Participants would also use the word ‘information’ when discussing the details required for identity theft.

> *Where is if I can get your date of birth, name, where you live, some banking information, then your three fifths of the way there to stealing your identity.*

One participant was concerned about the personal information available on the Internet.

> *It only stayed up for about a week and then I couldn't find it again, but it was quite scary that someone could collate all that information on you. It made you realise how easy it is.*

When data was used by the participants, it was mentioned in relation to 'information'.

> *Exactly what you are talking about how data has sensitive information embedded in there, and we don't realise.*

The participants also discussed 'information' in regard to 'data' being stored securely on network drives.

> *So often we find the system set up to store this data, are adequately secured and generally speaking storing private, sensitive, confidential information encrypted on a file share is not really what we would recommend.*

In summary, the Leximancer concept map in Figure 14 shows the theme 'information' connected to the theme 'people', but at some distance away from it. The theme 'information' is shown with 20% connectivity, (Table 3); 23% relevance and a count of 37, shown in the ranked concepts Table 4. The concept 'data' at the far edge of the circle themed 'information' has 12% relevance and a count of 19, shown in the ranked concepts Table 4. The word 'information' was used by participants when discussing information being available on Facebook, web pages being harvested by scripts, information being available showing how much someone has copied from an eBook, information needed, used or not being available when identifying a person, sufficient information being available leading to identity theft, personal information on the Internet, and sensitive information stored on secured network drives. However, the theme 'data' is used by the participants in conjunction with 'information', where participants' statements confirm the concept map showing 'data' at the far edge of the circle themed 'information'.

6.4.1.2.6 Summary

The Leximancer concept map in Figure 14 shows the theme 'people' central with other themes radiating from it. The thematic summary, Table 3, shows 100% connectivity for theme 'people', and the ranked concepts, Table 4, shows 100% relevance with a count of 163. Lemmatisation resulted in grouping 'guys', 'person', 'people', 'someone', 'staff', 'student', and 'students' into 'people'. The participants' discussion using the word 'people' related to staff being referred to also as ‘guys’ or ‘someone’, ‘guys’ used to refer to people at a Russian Business Network, ‘person’ used when implicitly referring to a staff member, ‘staff’ used to refer to staff members, and student used to refer to students in general.

The Leximancer concept map in Figure 14 shows the theme ‘credentials’ is connected to the theme ‘people’, with both themes overlapping and indicating a relationship. The thematic summary, Table 3, shows 14% connectivity for theme ‘credentials’, and the ranked concepts, Table 4, shows 12% relevance with a count of 20. Participants used the word ‘credentials’ when discussing issues related to students considering ‘credentials’ as access to the Internet, new employees who did not have their own credentials for three out of their four weeks of employment, staff on holidays passing their credentials to colleagues, how sharing of credentials is based on a high degree of trust, being unaware that sudo (pseudo) accounts exist thus leading to sharing of credentials, advising not to share credentials and reporting issues resulting from that, sharing of credentials among students with community spirit of sharing, someone else using a computer within the *** minute log off period, and majority of unauthorised computer access related to credential sharing.

The Leximancer concept map in Figure 14 shows the theme ‘password’ connected to ‘people’, with 25% connectivity, shown in thematic summary Table 3; and 18% relevance and a count of 30, shown in the ranked concepts Table 4. The theme ‘password’ is not connected to the theme ‘credentials’, which is connected to people on the opposite side to ‘password’. Participants used the word ‘password’ when discussing crossed out passwords still showing up on photocopier, students freely handing out their username and password, stealing identity, audit review requirements, students’ complaints about insufficient access, email as a potential source to obtain passwords, and resetting of passwords.

The Leximancer concept map in Figure 14 shows the theme ‘systems’ connected to ‘password’, with a 37% connectivity, shown in thematic summary Table 3; and 13% relevance with a count of 22, shown in the ranked concepts Table 4. The circle on the concept map for this theme is coloured in light orange indicating more relevance. Lemmatisation grouped ‘system’ and ‘systems’ into ‘systems’. Participants used the theme when discussing systems in general as opposed to education, using system to refer to desktop computer, corporate application, refresh cycle, server, system’s person, operating system, and web systems.

The Leximancer concept map shows the theme ‘information’ connected to the theme ‘people’, but at some distance away from it. The theme ‘information’ is shown with 20%

connectivity, Table 3, 23% relevance and a count of 37, shown in the ranked concepts Table 4. The concept 'data' at the far edge of the circle themed 'information' has 12% relevance and a count of 19, shown in the ranked concepts Table 4. The word 'information' was used by the participants when discussing information being available on Facebook, web pages being harvested by scripts, information being available showing how much someone has copied from an eBook, information needed, used or not being available when identifying a person, sufficient information being available leading to identity theft, personal information on the Internet, and sensitive information stored on secured network drives. However, the theme 'data' is used by the participants in conjunction with 'information', where participants' statements confirm the concept map showing 'data' at the far edge of the circle themed 'information'.

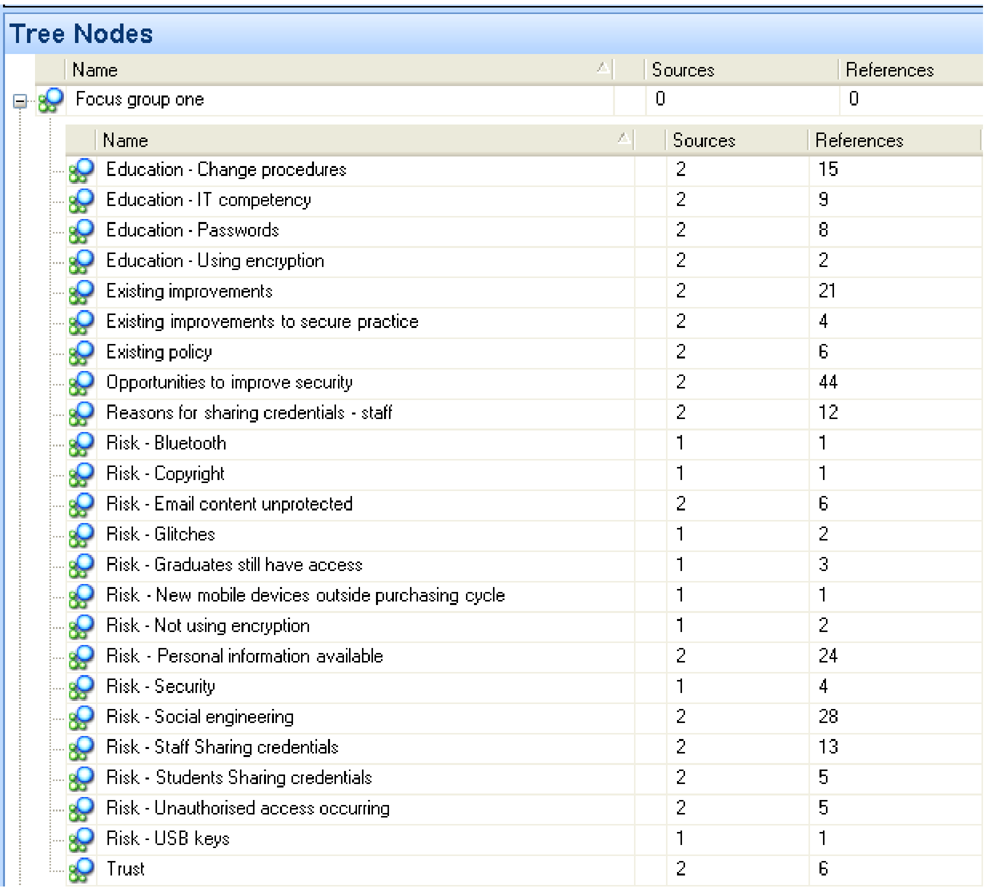
6.4.2 NVivo 8

For this research a project was created in NVivo 8 called Masters Focus Group. The project was created to contain all focus groups to allow comparison across the focus groups.

Through the 'Source' option button the two transcription documents were loaded into the NVivo project. The 'Nodes' option button then provided access to the 'Free nodes'. The first focus group transcription was then brought into view.

Reading through the documents one after the other, the relevant sections, sentences or paragraphs were then coded by the researcher. As the researcher had attended both focus groups, listened to the electronic recording and read through the transcription, the nodes were created during the coding process. This allowed the researcher to approach the coding with an open mind. The transcription of the second focus group was coded in the same manner. Where appropriate, existing free nodes created for the first transcription were used for the second focus group. This resulted in the list of free nodes shown in Figure 18 in the combined analysis.

The free nodes were then sorted using the tree nodes. One parent tree node was called 'Focus group one'. All the free nodes referring to this focus group were then copied under this parent tree node as shown in Figure 15.



Tree Nodes

Name	Sources	References
Focus group one	0	0

Name	Sources	References
Education - Change procedures	2	15
Education - IT competency	2	9
Education - Passwords	2	8
Education - Using encryption	2	2
Existing improvements	2	21
Existing improvements to secure practice	2	4
Existing policy	2	6
Opportunities to improve security	2	44
Reasons for sharing credentials - staff	2	12
Risk - Bluetooth	1	1
Risk - Copyright	1	1
Risk - Email content unprotected	2	6
Risk - Glitches	1	2
Risk - Graduates still have access	1	3
Risk - New mobile devices outside purchasing cycle	1	1
Risk - Not using encryption	1	2
Risk - Personal information available	2	24
Risk - Security	1	4
Risk - Social engineering	2	28
Risk - Staff Sharing credentials	2	13
Risk - Students Sharing credentials	2	5
Risk - Unauthorised access occurring	2	5
Risk - USB keys	1	1
Trust	2	6

Figure 15: NVivo tree nodes - Focus group one

There are 8 unique nodes to this focus group, such as nodes Risk – Bluetooth, Risk – Copyright, Risk – Glitches, Risk – Graduates still having access, Risk – New mobile devices outside purchasing cycle, Risk – Not using encryption, Risk – Security, and Risk – USB keys. However, saturation was achieved when 16 out of the total of 24 nodes were covered by both focus group one and two.

6.4.2.1 Education – Change procedures

Education was raised during the discussion by the participants of focus group one. Participants revealed that a change is only initiated when 'senior management' is aware of serious issues. Participants thought that this 'change' would result in changes to 'policies', 'procedures' and 'education'.

So some of the things that you're doing, changing procedures of how you do things Procedure and education yeh. One of the biggest things was, we generally as with most organisations. The only way you effect change is to hurt, for really bad things to happen, and it finally goes up to senior management level and they go ' why didn't' you know, and you go 'well I've been telling you this' So often unfortunately it takes something really bad to happen for there to be enough push from management. So right we need to change the way we are doing things, and then it's hey policy, procedures, education

Participants thought that while a system can be sophisticated, 'education' is reliant on people to have the 'desire' to be 'educated'.

No, but that is what is being done. In a nutshell yeh. There are two issues. There's the sophistication of the system which is one, which I believe is controlled to a certain extent obviously based on funding and resources. The flip side is education. It really doesn't matter how much education or material or things that you pump out people have to have that desire to be educated, and that's the harder battle.

6.4.2.2 Education – IT competency

Participants also thought that 'IT competency' needs to be part of 'education' for new staff members.

Like I say, one thing if you could do, will help you guys, also 2nd thing I think you need to do is education, you know previously becoming a staff member USQ part of your induction, is IT competency, which is no longer part of anything.

One view from a participant was 'introducing' it back at the faculty level, suggesting that this should be at corporate level.

We are introducing that back at faculty level, so unfortunately it's something that should be a corporate thing but it's not.

The participants discussed the issues of how emails that are generated by a web system can be falsified and lead to social engineering techniques to obtain student ‘credentials’. ‘Not all students would know’ better and would consider it sufficient that the email was coming from USQ, showing ‘lack of knowledge’.

> *Not really, maybe with USQ assist there might be pretty easy for someone to claim that they are from USQ assist to a student to get their credentials. Because all you have to do is in effect ***. I know you’ve got like a web system behind it, but you can still do everything from the email. So you don’t need to go to the web system to log in and do all that. So, it would be pretty easy for someone to say ‘I/m from the USQ and send a few emails and then next email say, ‘what’s your password, what’s your address?’*
>
> *Yeh, we have actually had issues with that in the past too. One of the ways that they wanted to get around it was actually sighting emails that went from other sources. Funding.*
>
> *So whole other ball game*
>
> *Yeh, well that’s quite complex in itself, but you know*
>
> *Not all the students would know that’s how they should receive it, so if they get an email, they just go okay that’s form the USQ that is fine*
>
> *So it’s lack of knowledge*

Participants were discussing how many emails are actually dropped, on a daily basis. One participant stated that a small sample of these dropped emails are used for the purpose of ‘education’.

> *As something you might find interesting, every day our external mail gateways receive around 1.1 million email address email coming inbound. So we actually drop 98.7% of that. It’s just a pile of ***, that’s dropped*
>
> *That’s similar for our as well, but on a smaller scale. I actually import a couple of them and send them through to everyone saying. ‘Hey look at this’ Education, check out the link hub, I took a picture and all that stuff*
>
> *.2% of that we would let through, mark as spam, because we are uncertain about it, because we don’t want to be, you know, basically Governing what comes in and outbound*
>
> *Well no, we have to do that, but there’s a grey area you know*

Participants voiced their concerns about applications that contain ‘meta data’ and ‘sensitive information’ that would be able to identify a ‘user name’ or GPS location into the data with the photo’ that would allow someone to identify an individual that people do not ‘realise’.

> *Even just stepping back and going into a, more of a user level sending out and sharing your documents like your word documents, they all have Meta data attached to them. I know a lot of people that just won’t, don’t even know about it, don’t care, documents principles, a lot of the time is set up with your alias so your actual user name for the computers is sent out. I’ve received emails with things, and I’m like, ‘ah that’s there user name’ with just from the document property on the side there. So you have that, you have their name, you can just build upon it.*
>
> *You have an iPhone?*
>
> *No, purposely don’t have an iPhone*
>
> *Good man, so like for example iPhones, Whenever you take a photo it actually embeds your PGS location into the data with the photo. I went to an excellent presentation last year, by the US drug enforcement agency on iPhone forensics, where they went through actually showing all the guys that they busted, so the gut would show a photo of him holding the stash and embedded in the photo was GPS location so they got hold of the phone tracked that location back found where the guy had his stash. Exactly what you are talking about how data has sensitive information embedded in there, and we don’t realise. Same concept*

6.4.2.3 Education – Passwords

Participants mentioned issues with passwords only in regards to ‘rule of change’ by a certain amount.

> *So you know about it, fair enough.*
>
> *I thought there was also a rule of change it by a certain amount now. You see people with password 1, password 2 literally password 1 , password 2*
>
> *It doesn’t let you do that. Unfortunately. That’s when I went to not actually change it. You can change it by one digit.*

Participants also discussed situations where someone may pretend to be from the university and send an email requesting a ‘password’ and other details.

Not really, maybe with USQ assist there might be pretty easy for someone to claim that they are from USQ assist to a student to get their credentials. Because all you have to do is in effect email headers and put a disclaimer at the bottom. I know you've got like a web system behind it, but you can still do everything from the email. So you don't need to go to the web system to log in and do all that. So, it would be pretty easy for someone to say 'I/m from the USQ and send a few emails and then next email say, 'what's your <u>password</u>, what's your address?'

Yeh, we have actually had issues with that in the past too. One of the ways that they wanted to get around it was actually sighting emails that went from other sources. Funding.

So whole other ball game

Yeh, well that's quite complex in itself, but you know

Not all the students would know that's how they should receive it, so if they get an email, they just go okay that's form the USQ, that is fine

So it's lack of knowledge

6.4.2.4 Education – Using encryption

Participants also discussed 'secure wireless access' that is 'not encrypted', issues that could be resolved through 'education'.

if they're connected to a <u>secure wireless access</u> point in Singapore there's <u>not</u> often <u>encryption</u>. It gives them free Internet access. Obviously they're probably going to do it. That's an <u>education</u> thing.

6.4.2.5 Existing improvements

Participants discussed the problems with 'sudo' (pseudo) accounts being 'reused' and by 'different people' making it difficult to 'track' and 'identify' a person through logs and 'audit trails' and that tying them down to a 'specific computer' would 'limit the damage'.

> *The other problem to this is what we often have, those sort of situations in place that we use to rectify like quickly providing individuals with "sudo" accounts or "sudo" access which is essentially just a generic login. That enabled people like yourself to get new staff members up and running really quickly the problem was it created a complete audit trail nightmare in that "sudo" account would be reused over and over again it could be shared by lots of different people and our ability to track and identify who that person really is when we our logs in our audit trail is completely hopeless.*
>
> *You can tie those down to specific computers at least to that there are only able to, you are limiting the damage.*

Participants pointed out that the library had already 'tied' down 'specific computers'.

> *That's why any we have in the library are tied down to specific computers only like the walk-ins' and the training labs. They are tied down to those.*

Participants also discussed already implemented security measures that are protecting an individual, but at the same time also make it 'difficult' to confirm a person's 'identity'.

> *It's a tricky thing; we have the same problem, that a lot of our ICT support staff that are on helpdesk. We have to over the phone do password resets. Due to privacy, they only have limited access to certain amount of common data which makes it very difficult to validate the identity over the phone. So all they can see is; student number, employee number and the date of birth. Can't find out more detailed information kike address, contact numbers for them, you know things that are more detailed attributes that can truly validate the identity over the phone. It's very difficult to successfully do that.*

Other participants experience phone calls from students 'parents' or 'partners', but do not provide any 'personal' 'information'.

> *A lot of our phone calls from students is not giving out personal information. It's just students ringing up saying "what can I enrol in? How many courses have I got left to complete?"*
>
> *So you're not providing them with private sensitive information?*

> No, I mean sometimes we get phone calls from parents, partners, we don't give out personal information. We can give them generic information on the degree that the person is enrolled in, but as far as personal

Participants cannot give information due to the 'privacy act'.

> "Has little Johnny passed last semester?"
>
> Yeh, we can't give that out because the privacy act and no one in the office would do that.

Participants explained how unscheduled 'test' is aimed at making ICT support staff 'more aware of the risks'.

> We sometimes like actually test out our ICT support staff on the front desk, just call up and a couple of guys who work for me, they're not Caucasian background there you know, ones from *** the other one is ***. So they can, you know utilise their accent to sound very much like an authentic *** student, but we just see how far we can push the staff. Which is often interesting. It sort of makes them a little more aware of the risk, somebody might be going to try it on. It also pisses them off. We normally follow it up by taking them down a bag of lollies or something. Carrot stick approach.

Some participants take implementation of certain security matters into their own hands by 'creating policies' and a 'database' to contain roles so that the right thing can be done when someone goes on holidays.

> I', forever, re-working or creating policies and unfortunately I've had to start up a, it's only just been started but a system that we basically it's a role base, web by where we can just search for a person role, so when they say, I'm leaving, or I'm going on holidays we will have a list of all the things that, that person, in that role, can access, But then on the flip side, there's things that, that role can do, then there's also things that, the person can do, because they might have specific involvement in things that
>
> That is within the system?
>
> Oh, that's just a little database, just a little access data base just to say what they should access. Nothing about there
>
> Just like a manual record

> *Yeh, unfortunately it's manual, because I don't yet know of an automated way that can give us the scope of everything that they get in, like J drive everything that they get on the intranet. If there is something, please let me know because*
>
> *It's not only that, it's SharePoint as well. We can say I want this person to have the same permission as me*

6.4.2.6 Existing improvements to secure practice

Participants are using a corporate application 'RightNow' to communicate with students, rather than their email application.

> *Not that I'm aware of, all of our correspondence with students is all done through 'RightNow' so it should be going through the students email account. Nobody should be sending an emails to students via their personal email, via personal outlook.*

6.4.2.7 Existing policy

Participants discussed the issue of 'credential sharing' to ensure that work continues while they are on 'holidays', but that staff members should be aware of a 'policy' .

> *I would say credential sharing is probably 95% of what we are aware of, put it that way.*
>
> *And just to share each others credentials.*
>
> *Yeh, it's actually quite an accepted practice for the staff too.*
>
> *Yeh, they go on holiday and they say here are my credentials.*
>
> *I was going to say exactly the same thing about staff.*
>
> *Most staff should be aware that there is a policy that states that's it's actually something you can be disciplined over*

6.4.2.8 Opportunities to improve security

Participants suggested to 'write' 'a clean up script' on the printer so that sensitive data is only available for a few seconds.

> *Can I suggest that you log out and the m to write out a clean up script.*
>
> *Well I think it does every 5 hours, or something like that but students need to, they shouldn't be leaving that there for more than a few seconds at the most.*

Participants discussed how a 'wireless laptop' might reduce some of the issues with overseas visitors.

> *Get yourself a wireless laptop, there's a possibility. We have them in the library.*

> *Yeh, we do have a fleet of loan computers.*
>
> *Are most of your staff, well most of the people that come to visit, are from Australian Universities?*
>
> *No*
>
> *China*

Participants pointed out ways to determine and register each person's 'access' levels, however, this may be something to be carried out over time as there is a question about who would be spending 'time maintaining' the register.

> *Because we can, then actually audit it and AD level and ensure that, that is reflected*
>
> *Yeh well, it's not been filled out, because I don't have the time to interview every single person that we have in the faculty and say 'what do you have access to' the resource is there it's been made, it's just basically it's a maintenance thing. Who is going to spend the time maintaining it?*

Participants discussed if 'job description' and 'maintain a record of the roles' would help, which highlighted that 'there are a lot of duties' with 'areas' that 'are very grey'.

> *From their perspective that should be all they need to ask*
>
> *I find that's a bigger issue, that people complain about. Not so much they're unauthorised access, it's what they think they should be able to access, that they can't*
>
> *Does that come down to, just keeping a decent job description, and maintain a record of the roles required for each job, and the location of maintaining. Like you can continuously maintain the roles within your organisation.*
>
> *That was the plan. It's pretty difficult to maintain in some areas because there are a lot of duties people undertake that are very grey. You know this area, for 3 days a week, then 2 days a week, I work here or, there's no black and white to sometimes. It's difficult.*
>
> *That's why you make common areas*

6.4.2.9 Reasons for sharing credentials – staff

In regards to sharing of credentials by staff members, participants discussed the situation where a new member of staff did not have 'access' for 'nearly 3 of those 4 weeks' of employment.

> *Sometimes though when you get a new member of staff they don't have access. We had a staff member join us for about a 4 week period, and nearly 3 of those 4 weeks she didn't have any username or password, so it was pointless having her there because she couldn't do anything*

Other participants highlighted that 'prior to the new IBM System' 'manual intervention' was possible to speed up the process of creating credentials.

> *You're bang on there. It's basically because prior to our new IBM system, we actually had a way of doing manual intervention, and you could come and say 'hey look it's really important, the person starting today, sorry can you do something about it right now?' and we could actually create the lady an account, create that job done. Now the whole work is triggered through HR.*

The participants estimated 'one' 'out of 30 appointments' would be affected, while those leaving and training the new staff member would 'handover' their 'username and password'.

> *One out of probably, oh I couldn't say, could be pushing it but out of 30 appointments, and it's really frustrating and the first thing someone says is when their training someone especially if they're doing a handover, and they only have a week until they leave, is 'here's my username and password so you can get in and do what you need to do, because I've only got a week to train you, by the time you get this on Thursday, maybe, you're not going to know anything to take over.'*

Some participants experienced the need to have access available immediately for someone that 'travelled' 'many days' from 'overseas', while processing to get new credentials would take '3 days', they might be here only 2 days.

> *Lead times is a tough one. I'm quite happy to say to people it's a 3 working day turnaround timeframe and that's it deal with it, but the notice that we sometimes get is 'here is my person that has travelled many, many days from somewhere overseas and they need a computer and they need a room now, and they need Internet access now. I can't tell those people 3 days, they might only be here for 2.*

Participants discussed that HR require ‘4 week’s notice’ to prepare ‘letters’ and other ‘correspondence’.

> *Mostly ***, yeh. It’s an interesting dilemma so we thought seeing it by resources seems to be the biggest thing that they want we will use that as the carrot to get them to follow the correct process, which is actually going through HR. I think they need, Oh, maybe 4 weeks notice, because they have to actually do proper letters and all sorts of invitational type of correspondence to those people and if they follow that process they also get set up with a ‘sudo staff account’ which gives then the access that they need.*
> *Not having to use our own faculty account.*
> *But then that account is their responsibility, and only theirs.*
> *That’s right, it’s a bit of a dilemma. As I say speed of getting resources is the biggest reason for credential sharing.*

The discussion continued with an understanding that ‘unless we know its a problem’ certain things take time and cannot be hastened.

> *People want to get the job done appreciate that. I guess that the thing is ultimately we are never going to end up at a position that we can, do things fast, unless we know it’s a problem. Unless certain people know it’s a problem.*

6.4.2.10 Risk – Bluetooth

Participants voiced their concern regarding Bluetooth devices and discussed disabling Bluetooth but staff exposing themselves to ‘blue staffing’ should they turn it on.

> *Um yeh. It’s pretty low. Most devices have Bluetooth disable body properties users power. If they turn it on, yeh, obviously exposing themselves to blue staffing.*

6.4.2.11 Risk – Copyright

Participants discussed the issues of copyright in regards to ‘eBooks’.

> *Our eBooks, was copying, you’re only supposed to copy so much, he had worked out a way of copying the books. We ended up getting notified, and said ‘Oh, I just kept on going, I just wiped out the information and put it back again” He copied most of the book. I told him I was going to kick him out totally, if he kept doing it.*
> *Good for you*
> *We have 10 people who copied 10% of the book.*

> *Yeh, overseas they used to do that. You would have 10 people copy 10% especially thesis they then collate it. That was very common overseas it hasn't happened so much. It was just a bit suspicious when they science, business you got to know who they were, got to know what they were doing.*

6.4.2.12 Risk – Email content unprotected

Participants voiced their concern that 'they seem to be de-sensitised' and that 'everyone thinks that emails are secure' and email 'passwords' believing it safe to do so.

> *Just thinking about emails, they seem to be de-sensitised everyone thinks that emails are secure, they are in my inbox, they don't think about the transmission of those emails, being intercepted anyone reading them. Once they are printed off, they can be forwarded to anyone. There is not always a log there are ways around everything. So emails seem to be, one of the big things that people go "ah, I'll just send an email, send you my password, log on details" Even things which, I know websites do say change it when you first log in, for the whole time just sits in the in box.*

6.4.2.13 Risk – Glitches

Participants also discussed a glitch where a 'request for leave' with details was emailed 'to half of the university' touching the realm of 'invasion of your privacy'.

> *There was a real incident just recently, where two of our library staff, the approval for leave has had a glitch. You put a request in for leave, putting the reason why you want your leave, submit it, and it gets sent to half of the University. I know that's happened 5 times. Those sorts of little glitches, very much an invasion of your privacy.*

Participants were concerned that 'requirements' by 'audit' is not satisfied due to a 'new identity management system'.

> *We did have an audit and one of the requirements was that we had to have an improvement in our password policy. One of those things was the *** day expiry. So previously we enforced that through active directory okay, which basically meant that anybody whose log in into our domain had to regularly reset their password. With the implementation of our new identity management system it's supposed to take care of that aspect, but it doesn't actually work. So we've got whole development team working on other issues, that's one of those things.*

6.4.2.14 Risk – Graduates still have access

Participants discussed the impact of changes to access for graduates. Previously, once graduated, 'the rule used to be' that a student lost access to all databases. Now, access remains in case students want to 're-enrol'. This change has inadvertently caused a 'copyright' issue, as access to material is only allowed to students.

> *don't know with the post, when a student graduates. When they are here they can log into our databases, not a problem here at the USQ. When they graduate and they finish officially the rule used to be that they not a student here at the USQ they shouldn't be able to get access to the databases. The rule now is they keep them up in case they want to re-enrol, and that means they can still. That has become a problem because officially they are not enrolled. So copyright wise, we always used to get told, that they shouldn't be using it because it is a copyright to the USQ students that are still enrolled, but there is that time span when they graduate, they have a great time getting into everything.*

Participants also discussed issues with 'systems' not being flexible enough to determine the correct status of a student, and only considering 'is a student active or inactive'. They report that this results in students 'stay active for 2 years without even enrolling'.

> *This is where a lot of our systems still only care about the fact that, a student account is active or inactive and they're not smart enough to actually look at attributes of that user so in our primary authentication source that system is using which is oracle directory it can have attributes of users that say 'no longer enrolled' but the system you're talking about specifically is either not configured or is not configurable enough, that you can tell it to look for those attributes all it cares about is 'is a student active or inactive' It's something that our project management is going to fix.*
> *Students can stay active for 2 years without even enrolling.*
> *That happens all the time.*

Participants discussed the scenarios where students 'add a course' and 'drop out of it', extending the timeframe of access.

> *They add a course and then drop out of it, then that extends their timeframe as well.*
> *We had one student who did that for 4 years. He would take up four then drop it.*
> *Hey get a student card, cheap rail, cheap bus ticket, you know cheap movies.*

> *And we expected it, He would enrol and then drop it a day before. He did it every year.*
>
> *And they still have access to everything.*
>
> *He was going to another university, so he was getting ours and the other university*
>
> *Ultimately, people are doing these things because it is a commodity they want.*

6.4.2.15 Risk – New mobile devices outside purchasing cycle

Participants discussed the implications of 'mobile devices' obtained 'outside the purchasing cycle' not being configured to ensure 'encryption'.

> *Yeh mobile devices, whether it be laptops, whether it be pda's. They're a nightmare, because they often also outside of purchasing cycle. So we regularly get you know people from VC division, on the way through from Singapore they'll pick up, the new whatever, you know upload am image onto it, start using it. A whole range of issues. The majority of it comes down to you know data aggressed devices mobile not being encrypted.*

6.4.2.16 Risk – Not using encryption

Participants discussed that 'education' may be required to alert staff that a 'secure wireless access point' may not be using 'encryption'.

> *If they're connected to a secure wireless access point in Singapore there's not often encryption. It gives them free Internet access. Obviously they're probably going to do it. That's an education thing.*

6.4.2.17 Risk – Security

Participants discussed the situation where people send 'confidential' material to the printer, so that by the time they arrive at the printer to retrieve it, the printing is compled. This creates the risk of others having the opportunity to read 'confidential' material.

> *Just the thing about photocopiers. I've seen people standing, waiting for jobs to come out, and have been looking at other ones, that have been struck with 'confidential' pick them up, give them a quick read and then just stick them back down again. I know you can say, your mailbox, you've got to type in your password to get them all out that, but a lot of the time that doesn't happen. People are 'that's just an extra step I would rather print it out and walk there.' In that time people have read it. Another thing we have was when we had to digitise our records, a lot of paper based, and all that sort of stuff, how do you compact was wide open during the day, our records staff are busy. We can just walk in there pull something out and walk off again. Keeping track of records, is really hard.*

Participants discussed the issue of accessing being driven by role rather than person, and 'private, sensitive or confidential' information being stored on the network drives. They voiced their concern that this secured and 'encrypted' information is not an ideal place to be stored on a 'file share'.

> *The flip side of that, is that we're all talking about option we use in the J drive, store private, sensitive or confidential information.*
>
> *Ball parts, not so much private, confidential for the individual but for their role. I say for their role because that's the direction that we take.*
>
> *Okay so do you know what I'm getting at here? So often we find the system set up to store this data, are adequately secured and generally speaking storing private, sensitive, confidential information encrypted on a file share is not really what we would recommend.*

6.4.2.18 Risk – Social engineering

In regard to another social engineering technique, participants believe that being 'dressed in corporate gear' may facilitate access to buildings and, by showing familiarity and confidence, their presence is not questioned.

> *Even just standing back from the University focus, If you are dressed in corporate gear you can pretty almost walk into any office building and basically no one questions you. I remember working at the council before I knew anyone form the fire department, walked into their main head office walked into the communications gear and started moving stuff around because that's where our comms were as well and just not a question. You walk in and go "Hi, how are you going" just pretend you're supposed to be there and you can do whatever you want. They've got police radios, fire, and all secure bands. Just sitting there, you can hear them when I'm working in the comms room.*

Participants also discussed challenging situations involving access to buildings and facilities where appropriately dressed people or those looking 'angry' or claiming to be 'late for a meeting' might gain access.

> *So that's often quite challenging for us, from building and facilities perspective it's just another query. So yeh, that's similar line of thing, but yeh. If you look the part, yeh you can squeeze in. Particularly if you look the part and you're angry.*
>
> *Waiting for someone, perhaps whose not shown up, you know, "somebody let me in I'm late for a meeting", you know al that sort of garbage. Anyway.*

Participants perceived the main danger in social engineering comes from someone 'stealing your identity' rather than someone trying to get login access.

> *The reality is, most people are wanting to do malicious things, couldn't really care about the USQ login. They want personal information so they can actually do identity theft on people. So the USQ login gets you to an email account, you know, maybe some file hosting space. You could change, you know, someone's, you know role information. That doesn't make you any money if you know what I mean. Where is if I can get your date of birth, name, where you live, some banking information, then your three fifths of the way there to stealing your identity.*

One participant discussed their own experience when one of their children discovered the participant's 'name', 'address', 'phone number', place of 'work', and office 'room' number online.

> *It mustn't be hard to find information because one day my kids were just playing with my name and the next think popped up my name, my address, my phone number, where I worked, what room I worked in. What else was it? There was just all of this private stuff that wouldn't just be in something from work, even my home phone number and things like that. It only stayed up for about a week and then I couldn't find it again, but it was quite scary that someone could collate all that information on you. It made you realise how easy it is. I don't know who did it. I've got no idea but, it only lasted a week.*

Participants discussed how 'bureaucracy' and 'slow work time frame' inadvertently leads to people making 'compromises' and creating 'breaches' in order to perform their work.

> *Yeh coming back, completely so social behaviour on this one they do that specifically because of, the bureaucracy and the slow work time frame in getting things done, so they do all of these compromises and breaches because that they perceive as being risk is quite minimal to whatever else they perceive as the benefits of giving it to them at that time. I don't reckon they even think, about what the personal or ramifications will be. They are just in such a culture at the moment of that's how we get stuff done quickly. This is what we will do.*
>
> *For sure*
>
> *So I don't think it even is part of the thought process anymore. It may have been a long time ago but definitely not at the moment. It's just a here you go.*

Participants discussed their concern with 'sub-contracting' staff refreshing computers, having admin access, and therefore access to every hard drive in the university.

6.4.2.19 Risk – Staff sharing credentials

Participants discussed the issue of sharing 'credentials' being a practice to overcome issues when staff go on holidays.

> *they go on holiday and they say here are my credentials*

Participants discussed the issue of having to provide 'username' and 'password' to get 'computers refreshed'.

Our biggest problem in the library is from the, well one that I've just noticed just recently is getting the computer refreshed. Every staff member has to give their username and password. I'm just about to email all the staff who are getting them done in the library. When their computer is refreshed the desktop support get the username/password so they can copy their profiles and everything across.

Participants believe that 'passwords' need to be changed after a 'system is refreshed'.

So they should be getting this when their system is refreshed, by ICT, no matter how much you might trust that person, they should changing the password.

Participants discussed people leaving their 'screens' 'unlocked', thus creating the risk of unauthorised access.

Just further, on leaving unlocked even at work people tend not to lock their screens and they get up to go to the photocopier or something like that, leave it open and you can do whatever you want, you can send a malicious email off. There is no way of pinning it down to anyone

6.4.2.20 Risk – Students sharing credentials

Participants stated 99% of the time students would be willing provide their credentials to others.

99% of the time simply students providing other individuals with their credentials

Participants thought that 'students' who 'have a community spirit of sharing' would be passing their credentials on to 'fellow' students.

*particularly with *** students, particularly with students from ***, ***, ***and those areas who have a community spirit of sharing what they have with their fellow students.*

Participants discussed that students would be too willing to volunteer 'username and password' for 'troubleshooting' purposes.

> *I don't think we're aware of too much abuse. I know we get emails from students complaining they can't get into various things, and they will say I'm using my UConnect login which is: username and my password, and we think " no , no don't tell me this!" So they will give that to us as a way of trying to help us troubleshoot whatever their problem is. We just delete it and don't pass it on anywhere else. I must admit it does help for troubleshooting but, yeh that would be one thing that I am aware of students sort of freely handing out their username/password.*

Participants discussed the possibilities of students using the 'walk in systems' and then 'walk off and leave the computer logged in' while the automatic lock activates after *** minutes.

> *The other big one we have and its with any of the student computers anywhere I suppose, but we cop it with the walk in systems is students can log in, then do some printing, and they walk off and leave the computer logged in, and that is just happening all the time. Students just don't realise the danger of leaving a computer logged in. It logs off after *** minutes but there is a window of someone sitting down on a continual basis and using that persons credentials. They're real issue, from staff and students*

6.4.2.21 Risk – Unauthorised access occurring

Participants stated clearly that 'unauthorised computer access' they encounter is related to sharing 'credentials'.

> *So the majority of unauthorised computer access we see is just simply credentials being used.*

6.4.2.22 Risk – USB keys

Participants voiced their concern regarding USB keys that may contain 'important files' being left on the desk.

> *USB keys are a nightmare for me.*
>
> *Yeh absolutely*
>
> *Everybody running around with all sorts of important files on USB keys. Go to lunch leave it on the desk with your car keys*

6.4.2.23 Trust

Participants explained how providing 'credentials' to colleagues so that they are able to do their work also means 'high degree of trust'.

> *So I guess the thing is in giving her somebody's credentials, so you gave her your credentials your then placing a high degree of trust on her. Which is absolutely exposes you to risk and University risk.*

Participants voiced the question 'who is watching watchers' when considering those in IT who implement security.

> *Yeh, so I guess. I was going to ask who is watching watchers?*
> *Yeh, there's actually a really good Spanish phrase which describes that. I can't remember what it is but, I used to have it on my desk. That exact thing 'who is watching watchers?' and yeh, look you've got to trust somebody.*

6.4.2.24 Summary

Overall, the focus group discussion revealed the following concepts.

'Education - change procedures' brought to light by the participants that change is only initiated by 'senior management' when they are made aware of serious issues. Participants believe that 'really bad things' need to happen for a change in policies, procedures and education to occur. At the same time, participants also said that people have to have the desire to be 'educated'.

'Education - IT competency' highlights the participants' understanding that 'IT competency' is needed for new staff members and, as a result, some are already reintroducing it at faculty level, believe it should be at a corporate level. Similarly, for students, IT competency would also be beneficial when it comes to distinguishing between real USQ email and spam mail. Some participants thought that providing staff members with a couple of bad emails, including pictures, would help educate them. There also needs to be an increased level of awareness that metadata hols sensitive information from accompanying documents which may allow identification of individuals.

'Education – Passwords' highlights the problem of reusing similar passwords or changing only one digit. Participants also discussed the possibility of someone pretending to be from the university sending an email asking for a 'password'.

‘Education - Using encryption’ shows that participants discussed the issue of secure wireless access point, possibly in a country not using encryption, to be an issue, that could be resolved through education.

‘Existing improvements’ related to discussions of 'sudo' (pseudo) accounts to resolve the issue with audit trail by tying them to specific computers. Some participants pointed out that current security measures prevented help desk staff verifying someone's identity over the phone. Existing awareness about 'privacy act' ensures that no information is given to partners or parents of students. Furthermore, ICT front desk staff members are 'tested' to ensure they are aware of techniques and risks. Other staff members are re-working or 'creating policies' in relation to a person’s role and access in the event of holidays when someone else needs to perform their tasks.

‘Existing improvements to secure practice’ showed that participants are using a corporate application to communicate with students, rather than their email application.

‘Existing policy’ showed that some participants thought that staff members should be aware of a policy regarding credential sharing.

‘Opportunities to improve security’ showed that participants supported writing a clean up script to ensure that sensitive data is only available for a few seconds. Participants suggested the use of a 'wireless laptop' to address issues with overseas visitors, and to determine each person’s access level and store it in a register which, in turn, raised the question of who would have the time to maintain it. Discussing whether ‘job description’ and ‘maintain a record of the roles’ would help, highlighted that ‘there are a lot of duties’ with ‘areas’ that ‘are very grey’.

‘Reasons for sharing credentials – staff’ highlighted that a new member of staff did not have access for nearly 3 out of 4 weeks of employment. Participants discussed the use of ‘sudo’ (pseudo) accounts as a temporary solution, but this creates a difficult situation in regards to audit trails and determining who the person is. Prior to the new IBM system, manual intervention allowed the speed up of creating new credentials. The participants estimated one out of 30 appointments would be affected, and those leaving and training the new staff member would voluntarily handover their username and password. Some participants experienced the requirement for immediate access for someone who has travelled many days from overseas, where processing to get new credentials would take 3 days, but that person might be here only 2 days. Participants also discussed the usual timeframe of 4 weeks required by HR to prepare letters and other correspondence relating to new staff. Participants believe this is the usual of processing timeframe unless it was known to be a problem.

‘Risk – Bluetooth’ highlighted participants concern of staff turning Bluetooth on and exposing themselves to ‘blue staffing’.

‘Risk – Copyright’ touched the issues with eBooks.

‘Risk – Email content unprotected’ highlighted participants concerns about people thinking that emails are safe in general and that emailing passwords is safe specifically.

‘Risk – Glitches’ highlighted a scenario of a leave application being emailed to half the university, touching on invasion of privacy, and that a requirement by audit is not satisfied due to a new identity management system.

‘Risk – Graduates’ still having access highlights the implications of changes in access for graduates resulting in copyright issues. Participants also reported on students being able to stay active for 2 years without being enrolled, due to systems inflexibility, and that students would add a course then drop it to extend the timeframe of access.

‘Risk – new mobile devices’ obtained outside the purchasing cycle highlighted issues of these devices not being configured to ensure encryption.

‘Risk – Not using encryption’ highlighted the need for educating staff that secure wireless may not have encryption.

‘Risk – Security’ highlighted that some people tended to risk having confidential documents exposed on the printer rather than use their mailbox. Also, participants discussed access driven by role on network drives and file share not being ideal for secured and encrypted information.

‘Risk – Social engineering’ highlighted the belief that dressing in corporate wear may facilitate access to buildings, and that by demonstrating familiarity and confidence, their presence may not be questioned. Some suggested that identity theft may be greater danger than just stealing login details. One participant actually experienced finding her personal information on the Internet. The group also discussed bureaucracy and how slow work timeframes inadvertently lead to compromises and breaches when staff members were trying to get their work done.

‘Risk – Staff sharing credentials’ highlighted holidays as one of the reasons for this practice, as well as having to provide user name and password to have the computer refreshed. Participants believed that passwords should be changed after the computer is refreshed, and leaving computer screens unlocked and unattended posed the risk of allowing others to gain access.

‘Risk – Students sharing credentials’ highlighted that participants believed 99% of the time students would provide their credentials to others.

6.5 Focus Group Two

The transcription from the second focus group was used in an analysis by Leximancer 3.5 to obtain an unbiased result. The text transcription was loaded into Leximancer and an analysis was conducted using the predefined default settings within Leximancer. This provided the first concept map for this focus group, visually highlighting concepts that allowed changes to the default settings. The changes are documented within the second analysis run. The final concept map is then analysed in accordance with the more relevant concepts identified on the concept map. The researcher then used NVivo 8 to manually code the same transcription of the second focus group by creating free nodes. These free nodes were then converted into tree nodes. This allowed the researcher to create a tree node for this focus group.

6.5.1 Using Leximancer 3.5

Qualitative research uses content analysis, which means that written material is analysed to determine concepts. With the conceptual analysis, the written material is evaluated for any words or phrases that may yield a concept. Rational analysis measures how the located concepts relate to each other. The resulting map therefore also shows the relationships between the concepts (University of Queensland 2010c).

Firstly, Leximancer was used to obtain an independent and unbiased analysis. As the researcher has been working through the literature and the research question and its proposition, obtaining an independent and unbiased analysis result would ensure the validity of this research.

The analysis process of Leximancer is unbiased because it builds concept seed words from the document itself. When Leximancer analyses a textural document for the first time it starts without a list of seed words. As Leximancer works through the document it gradually builds a new list of seed words from the contents of the textural document. The result of the analysis provides a concept map that shows themes as circles, and the concepts within the themes. The researcher can then interrogate the graphical representation of the textural document to gain a better understanding of its components. The concept map also has tabs to the right which provide more detailed statistical information to the researcher.

The use of Leximancer is relatively easy, as it comes with default settings. After providing the textural document to Leximancer, the whole analysis process runs fairly quickly. This provides the researcher not only with an unbiased result, but a quick understanding of the contents of the document.

As outlined in chapter 4, the researcher can interact with the map by changing the percentage of the theme size, degree of rotation and visible concepts within the themes. This does not affect the concepts or meaning at all. It allows the researcher to either get a birds-eye view by decreasing the percentage, or obtain much more detailed information by increasing the percentage. A subsequent re-run of the analysis process will then use the existing seed words and re-analyse the textural document producing, a new concept map.

Each circle on the concept map represents a theme, and contains a number of concepts. The size and colour of the circle are indicators about the relevance of the theme. In addition to that, when circles overlap, they share some commonalities.

6.5.1.1 First analysis run

A new folder was created in Leximancer to contain the project for the second focus group. The Word document containing the transcription for the second focus group was added. The first run creates the list of concept seeds that can be accessed through the 'Edit emergent concept seeds'.

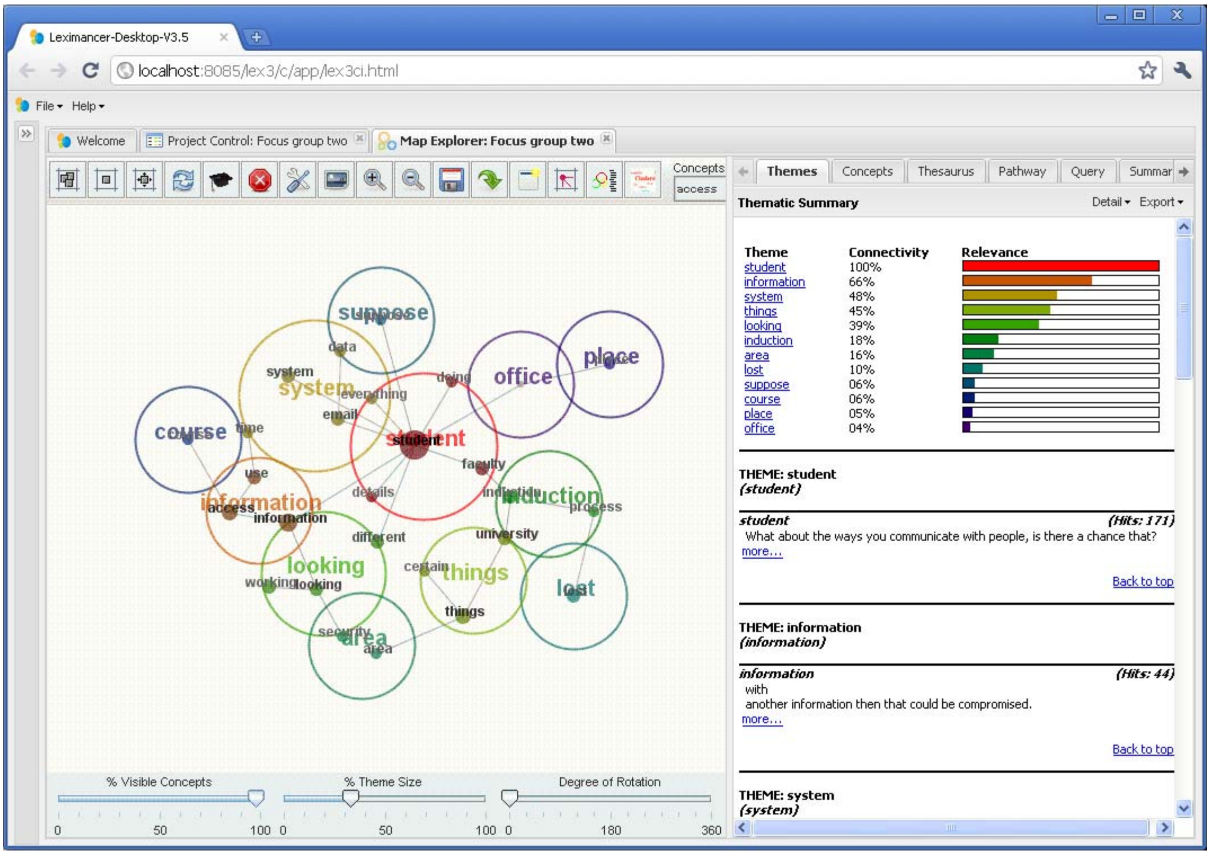
Running the transcription of the second focus group through Leximancer for the first time identified one word, "yeh". The option "Edit emergent concept seeds" was used to remove this word from the analysis process. The reason this word was removed from the analysis process is it does not have any meaning to this research.

After further investigation of the concepts the following changes were made. The concepts 'look' and 'looking' were merged into 'look'. The concepts 'people', 'person', 'somebody', 'someone', 'staff', 'student' and 'students' were merged into 'people'. The concepts 'system' and 'systems' were merged into 'systems', and the concepts 'use' and 'used' were merged into 'use'. These concepts were merged together for the purpose of lemmatisation. This allows these merged words to be analysed as one word.

No other changes have been made that may adversely influence the analysis.

6.5.1.2 Second analysis run

Running the analysis a second time resulted in the concept map shown in Figure 16. Each theme is represented by a circle. Each circle uses a different colour to differentiate between other themes. The brightness of the circle indicates how often it occurs within the document (University of Queensland 2010c). Warm colours such as red or orange indicate a high level of relevance, and cool colours such as blue indicate least amount of relevance (University of Queensland 2010c). The concept map with the 'Visible Concepts' was increased to 100% to show the concepts within each thematic circle.



Thematic Summary

Theme	Connectivity	Relevance
student	100%	
information	66%	
system	48%	
things	45%	
looking	39%	
induction	18%	
area	16%	
lost	10%	
suppose	06%	
course	06%	
place	05%	
office	04%	

THEME: student
(student)

student ***(Hits: 171)***
What about the ways you communicate with people, is there a chance that?
more...

THEME: information
(information)

information ***(Hits: 44)***
with
another information then that could be compromised.
more...

THEME: system
(system)

Figure 16: Leximancer concept map - Focus group two - visible concepts

6.5.1.2.1 Theme 'student'

The Leximancer concept map in Figure 16 shows the theme 'student' as a circle in the warm colour red. In Leximancer, colours are used to communicate whether a theme is least or most relevant. Warm colours such as red and orange, in Leximancer, are given to most relevant themes (University of Queensland 2010c). This theme is also positioned closed to the centre of the map, indicating importance. In addition to that, it has lines radiating from it to other themes, showing the connections between themes. The thematic summary, Table 5, shows 100% connectivity for theme 'students'; and the ranked concepts, Table 6, shows 100% relevance with a count of 171.

Table 5: Leximancer thematic summary - Focus group two

Theme	% of Connectivity
student	100
information	66
system	48
things	45
looking	39
induction	18
area	16
lost	10
suppose	6
course	6
place	5
office	4

Even though the ‘Edit emerging concept seeds’ option was implemented, lemmatisation by merging the concepts ‘people’, ‘person’, ‘somebody’, ‘someone’, ‘staff’, ‘student’ and ‘students’ into ‘people’, the theme ‘student’ has a strong presence on the concept map. The creation of the concept map was repeated to ensure that this result was not caused by human error.

Table 6: Leximancer ranked concepts - Focus group two

Concept	Count	Relevance percentage
student	171	100
information	44	26
access	43	25
things	39	23
university	29	17
looking	26	15
system	21	12
faculty	19	11
use	19	11
email	18	11
lost	18	11
different	17	10
area	15	9
time	14	8
working	13	8
induction	13	8
process	13	8
data	13	8
doing	12	7
security	11	6
suppose	11	6
place	11	6
certain	10	6
course	10	6
details	9	5
everything	9	5
office	7	4

Participants tended to use the word ‘students’ when discussing the sharing of ‘usernames’ and ‘passwords’.

> *I don’t see how a lot of things from the social engineering aspect. We see a little bit of that in the residential colleges where students are sharing usernames and passwords and those sorts of things.*

Participants used the word ‘people’ when discussing issues related to outsiders.

> *But the unknown to, there is an expectation all these people from an external contract point of view will actually send back all of the documentation. You know, quite often the system breaks down because only part of it comes back or it comes back slowly, or they haven't filled out there part properly.*

When discussing the loss of knowledge, participants were referring to a new staff member as 'person'.

> *And because we don't have dedicated people it's that loss of knowledge of what needs to be done. I mean it's very when everybody has a full PD of their own and then you say to them, oh by the way can you, we have a new person starting next week, you know, well who's responsibility is that?*

Participants used the word 'somebody' when discussing the issue of staff members leaving a computer unlocked when walking away, allowing it to be accessed by a stranger.

> *Realistically we would be very much reliant on somebody realising that somebody who wasn't meant to be there was sat there tapping away at the keyboard. So very much getting into the habit of if you leave it you lock it.*

Participants used the term 'someone' as they were discussing the issue of staff members leaving employment and it being up to the staff member's supervisor to determine when the account should be terminated.

> *So, as part of, if we significantly tightened up that aspect, HR can disable accounts now, that, after a period that someone leaves the issue is that it is entirely up to the supervisor of the person that is actually leaving. So the supervisor can request that particular condition and request a new cut off be instant.*

The participants used the word 'staff' when discussing 'honesty' and 'good will' rather than 'explanations' for new 'staff' and ongoing 'reminders' for continuing 'staff' who will be accessing personal information.

> *I think we just rely on people's honesty and good will without there being any real explanations to new staff or even regular ongoing reminders to continuing staff that we are dealing with personal information and we have certain responsibilities about dealing with that information correctly. I was actually talking to someone yesterday who works at centrelink, no her husband works at centrelink, and she was telling me every time her husband looks up a centrelink recipient it's recorded and there is even in fact he has a little device on his desk, I am not sure what it is exactly, but if he's been out of his database for a while and then wants to re-access it he has to actually get a new password.*

The participants also used the word 'student' to discuss matters about offshore students.

> *We regularly had you know, accounts from the res colleges being logged in and used even though the student was a resident of Malaysia, and they never set foot on campus. They were freely sharing it with friends and stuff.*

Participants used 'students' to discuss issues with sharing usernames and passwords.

> *I don't see how a lot of things from the social engineering aspect. We see a little bit of that in the residential colleges where students are sharing usernames and passwords and those sorts of things.*

In summary, the Leximancer concept map in Figure 16 shows the theme 'student' centrally on the concept map with other themes radiating from it. The thematic summary, Table 5 , shows 100% connectivity for theme 'students'; and the ranked concepts, Table 6, shows 100% relevance with a count of 171.

Participants used the word 'student' when discussing the sharing of usernames and passwords, 'people' when referring to an outsider, 'person' when referring to a new staff member, 'somebody' when discussing a staff member leaving computer unlocked, 'someone' when a staff member is leaving employment, 'staff' when considering explanations or ongoing reminders for staff members accessing personal information, 'student' when discussing issues related to offshore students sharing access, and 'students' when referring to sharing usernames and passwords.

6.5.1.2.2 Theme ‘information’

The Leximancer concept map in Figure 16 shows that the theme ‘information’ in light orange indicating more relevance, is connected to the theme ‘student’. The thematic summary, Table 5, shows 66% connectivity for the theme ‘information’; and the ranked concepts, Table 6, shows 26% relevance with a count of 44.

Participants discussed ‘information’ in regard to course work requiring setting up of groups on a system for the purpose of applying group work. This includes providing individual details to other students, however, the group members may not have agreed to share their details.

> *Very shortly yeh, another thing is I don’t know if it’s a huge problem or what you are after but, if you are talking about exposure of information group’s submission. Students are submitting their details to collectively they don’t necessarily, they’re not always friends they could be forming a group because a course examiner puts them in a group for their credit submission but their details are documented on the front page and so each member of that group gets that information so if you are talking about exposure of a student number which may then allow them to get so far*

Participants also discussed ‘information’ in regards to various compulsory online training materials not including aspects of handling ‘information’.

> *It always strikes me as odd, that every single year we get the email through with that mandatory online training for workplace health and safety, workplace harassment and that’s mandatory and you get chased up if you don’t do it but all of the professional development stuff on freedom of information and handling information they are all voluntary. Yet we all do it. So it’s one of those things that perhaps we need that sort of a training module, just to not necessarily, because we are expecting people to take a couple of hours out of their day and learn it all off by heart but if you got a yearly reminder that was mandated that was go through this, it will just refresh your memory a bit, then it shows that this is something the organisation takes seriously.*

Participants also discussed ‘information’ in regard to some of it still being processed manually, which exposed the possibility of old delivery mechanisms being open to comprise.

> *So there is all of these variables that, you know, allows the system to break down. It just seems like you get people employed here, we still go through a lot of hard copy documentation and yet we want them to operate in an online environment, you know, it just seems that from that end it seems to be a lot of information that floats around getting signatures, personal information and all that has to be done in hard copy, and then that has to be put through internal mail.*

Participants also discussed ‘information’ in regard to potential risk if a student’s birth date is known to others.

> *Because if a student rings with an enquiry, one method of verifying that you are talking to the person who you think you are talking to is to ask them, what their date of birth is. Well, you know, students who are working in a group may not be best friends but they may know when someone’s birthday is and so, you know there is a potential risk, that a student that has done some group work may know that about another student and may use that information to access information, that they shouldn’t have access to.*

Participants used the term ‘information’ when voicing their concern over ownership, confidentiality, and security when using Turnitin (an academic plagiarism detector).

> *The only thing that I would say as potential risk would be, with electronics, there is definitely a market for the sale of assignments or various assessments and I know even the discussion with the use of turn it in being an external database in America, where there’s debate over who owns the work particularly where it’s PhD, doctorate work where it’s been presented for the first time, once you run it through turn it. in then it is actually now on a database, and who owns that, and if that’s compromised at a later point by, we don’t facilitate that database so we are relying on turn it in to have security measures a lot of that work will encompass information from sources that you know they want it to remain confidential,*
> *it’s you know, it’s even generic assignments where if it’s project management it’s somebody basing that assignment on .*

Participants also used ‘information’ when explaining their information gathering processes being linked in with consultation with the legal office.

> *The second example is that we create online forms on the USQ website which collects data of maybe students, it can be different organisations, staff etc, and we work quite closely with the legal office, having the correct disclaimers attached to forma, and also looking into how long they will be keeping this information for, where is it stored, how are they storing it, who are they giving access to it.*

Participants discussed ‘information’ about organisations that students include in their assignments.

> *their company, the company will allow that specific information to go into that assessment but not for it to be published. So there’s security and debate over the validity of that.*

Participants also voiced their concerns about manual processes containing ‘information’.

> *So there is all of these variables that, you know, allows the system to break down. It just seems like you get people employed here, we still go through a lot of hard copy documentation and yet we want them to operate in an online environment, you know, it just seems that from that end it seems to be a lot of information that floats around getting signatures, personal information and all that has to be done in hard copy, and then that has to be put through internal mail.*

Participants also used ‘information’ when discussing human error in information erroneously being divulged.

> *I don’t know if this is what you are after, but I suppose, there’s always room for error with information going out, where you are directing it to a particular student, and you are entering their email address, in the email addresses there is a student number where you get pre, where you have used student email addresses in the past and if you are not careful and you get a pre empted address come up, you choose it., and then it’s not the right student that information, if theirs is confidential stuff that might go out inappropriately but.*

In summary, the Leximancer concept map in Figure 16 shows that the theme ‘information’, in light orange indicating more relevance, is connected to the theme 'student'. The thematic summary, Table 5, shows 66% connectivity for the theme 'information'; and the ranked concepts, Table 6, shows 26% relevance with a count of 44.

Participants used the word 'information' when discussing issues related to course group work exposing student data to team members, compulsory online training not including handling of information, manual processing information exposed to compromise, ownership, confidentiality, and security regards third party Turnitin, some university sections working closely with the legal office regarding their handling of information, inclusion of company information in student assignments, manual processing, and human error in accidentally divulging information.

6.5.1.2.3 Theme 'system'

The Leximancer concept map in Figure 16 shows the theme 'system' light orange, indicating stronger relevance, connected to the theme 'student'. The thematic summary, Table 5, shows 48% connectivity for the theme 'system'; and the ranked concepts, Table 6, shows 12% relevance with a count of 21.

Participants were using 'system' when discussing usability testing of the website and systems, referring implicitly to corporate systems.

> *We do usability testing of the website and systems, it only started this year and so we have lots of perspective students and current students and we actually film their comments about what they say about the systems that they find*

Participants also used the word 'system' to refer to manual paper processing.

> *With the paper system you get the assignment, you mark it, you enter the marks the assignment goes back so we don't have anything left.*

In discussing corporate applications participants used the term 'systems', including the generic 'systems' in the library.

> *Initially, most of this would come from our off campus students, because the system in place at the moment that we have for requesting documents, document x, relies on the data that we get from PeopleSoft and the problem is, is that in between semesters, especially over semester 3 if a student hasn't enrolled for semester 1 then they essentially drop off the system. Off of the library system.*

Participants also used 'system' to refer to a process that relates back to using corporate applications also referred to as 'system'.

> *And even when people within the organisation change roles, whether that is a permanent change or a temporary change there isn't a system whereby the various systems access is reviewed so I've moved from being the assessment manager into managing partnerships but my systems access hasn't reduced and it works fine for me, because it means that there is still a lot of issues that come up, that are raised by partners .that I can deal with myself, instead of having to refer them onto somebody else.*

Participants also used 'system' when discussing issues related to staff members who are processing examination and are also enrolled as students.

> *We have removed exams from the general processing system in order to allow for people who would otherwise have had access to those, not to have access so when I was doing the role that *** is currently doing, and we had *** and *** at one time studying with us instead of those exams being lodged the way the rest of the faculty lodged them they used to come directly to me*

In summary, the Leximancer concept map in Figure 16 shows that the theme 'system' is light orange, indicating stronger relevance, connected to the theme 'student'. The thematic summary, Table 5, shows 48% connectivity for the theme 'system'; and the ranked concepts, Table 6, shows 12% relevance with a count of 21.

Participants used the word 'system' when discussing usability testing of websites and corporate systems, manual paper processing, and corporate applications, and concerns about staff members who are also students processing examinations.

6.5.1.2.4 Theme 'looking'

The Leximancer concept map in Figure 16 shows that the theme 'looking', in light green indicating less relevance, is connected to the theme 'student'. The thematic summary, Table 5, shows 39% connectivity for the theme 'information'; and the ranked concepts, Table 6, shows 15% relevance with a count of 26.

Participants used the word 'looking' when discussing the alignment of procedures with new software to address risks.

> *From the university point of view when we are looking at software that are more, and more using now what procedures should there be to make people aware to go looking for situations with risks like that?*

Participants used 'look' to discuss the difference in priority processing by centralised systems.

> *It's not the case now, because the HR section has gone to centralisation, the computer section has gone to ICT. We have to now log a job to them, they just look at the jobs as they come in and wait your turn, you don't know how busy they are and they have got to service the whole university*

Participants used 'look' when discussing the issue of staff members also being students and having access to examination papers.

> *In relation to those, when it came to exam time remember those who were taking business exams that were working with us in the area, we had to block them from that access on that particular time, so they didn't get to see the question paper for the particular exams. It doesn't automatically block them, so we had to remember to, and rely on their honesty, to which mostly they did but you did rely on their honesty, and not to have a look in the back room*

Participants used 'looking' when discussing the topic of induction and its importance in preparing a new employee.

> *Just getting back to your question just now though ***, I'm not sure what could be done in that sort of scenario but I do believe that universities induction methods are lacking in regards to informing, well it's a bit difficult for me to say this because I have been at the university for 15 years but I know that when I came my induction which I didn't get until after I had been here for over a year and half, 2 years because I was on casual contracts, but it was very inadequate, and it's on my mind at the moment because we are currently looking at what we do in the faculty and I know there are freedom of information sessions and all that sort of thing, but I just think the whole ethical issues around the information that we have access to as staff members is not highlighted enough.*

In summary, the Leximancer concept map in Figure 16 shows that the theme 'looking', in light green indicating less relevance, is connected to the theme 'student'. The thematic summary, Table 5, shows 39% connectivity for the theme 'system'; and the ranked concepts, Table 6, shows 15% relevance with a count of 26.

Participants used the word 'looking' when discussing the alignment of procedures with new software to address risks, the difference in priority processing by centralised systems, the issue of staff members being students having access to examination papers, and the induction process and its importance in preparing a new employee for the workplace.

6.5.1.2.5 Theme 'induction'

The Leximancer concept map in Figure 16 shows that the theme 'induction', in light green indicating less relevance, is connected to the theme 'student'. The thematic summary, Table 5, shows 18% connectivity for the theme 'information'; and the ranked concepts, Table 6, shows 8% relevance with a count of 13.

Participants use 'induction' when discussing the value of a personal induction as opposed to completing it online.

> *If you are going into that type of role that you would have policies within that section that you would be sat down, as part of your induction. Okay this is what we expect when you're identifying your student on the phone or this is what we expect when you are sitting at the front desk you have got a student coming to see you, and you need to walk away from the computer you need to lock it.*

Participants also discussed their own 'induction' experience during a period when it was still run like a training session.

> *Actually it's funny, when I first came here about 15 odd years ago, the induction was really good, HR sat us down in a room basically for the day and went through all of the ethical concerns, security, and privacy and that sort of stuff in a huge amount of detail. None of that exists any more, back then it was the only way they could get to do it, they had to get you to sit down for the entire day.*

Participants discussed 'induction' created by professional staff being made available to academic staff to alleviate the gaps currently experienced.

> *So in our own induction is we have just got a working group going amongst the professional staff we are actually looking at overall induction not just for the professional staff but for any new academics so that we are trying to alleviate some of the problems with when new people come because when you lose your central person, well you know, she used to organise the access and she used to organise .this that and the other. The school admin officers are saying well we need to have a much more, the experience that a new academic coming into the school of law may be completely different to the experience of someone coming into the school of information simply based on the experience and the knowledge of a school admin officer, and if you have got new school admin officers in a new school, where there is no history, no.*

In summary, the Leximancer concept map in Figure 16 shows that the theme 'induction', in light green indicating less relevance, is connected to the theme 'student'. The thematic summary, Table 5, shows 18% connectivity for the theme 'information' and the ranked concepts, Table 6, shows 8% relevance with a count of 13.

Participants used the word 'induction' when discussing the value of person-to-person versus online induction, the effect when induction was run like a training session in the past, and how professional staff created an induction that can also be used for academic staff to overcome problems caused by gaps in the current induction process.

6.5.1.2.6 Summary

The Leximancer concept map in Figure 16 shows the theme 'student' centrally on the concept map with other themes radiating from it. The thematic summary, Table 5 , shows 100% connectivity for theme 'students'; and the ranked concepts, Table 6, shows 100% relevance with a count of 171.

Participants used the word 'student' when discussing issues related to sharing of usernames and passwords, 'people' when referring to outsiders, and 'person', 'somebody', 'someone', 'staff' when referring to staff members.

The Leximancer concept map in Figure 16 shows that the theme 'information', in light orange indicating more relevance, is connected to the theme 'student'. The thematic summary, Table 5, shows 66% connectivity for the theme 'information'; and the ranked concepts, Table 6, shows 26% relevance with a count of 44. Participants used the word 'information' when discussing issues related to course group work exposing student data to team members, compulsory online training not including handling of information, manual processing information exposed to compromise, ownership, confidentiality, and security regarding third party Turnitin, some university sections working closely with legal office in their handling of information, inclusion of company information in student assignments, manual processing, and human error in accidentally divulging information.

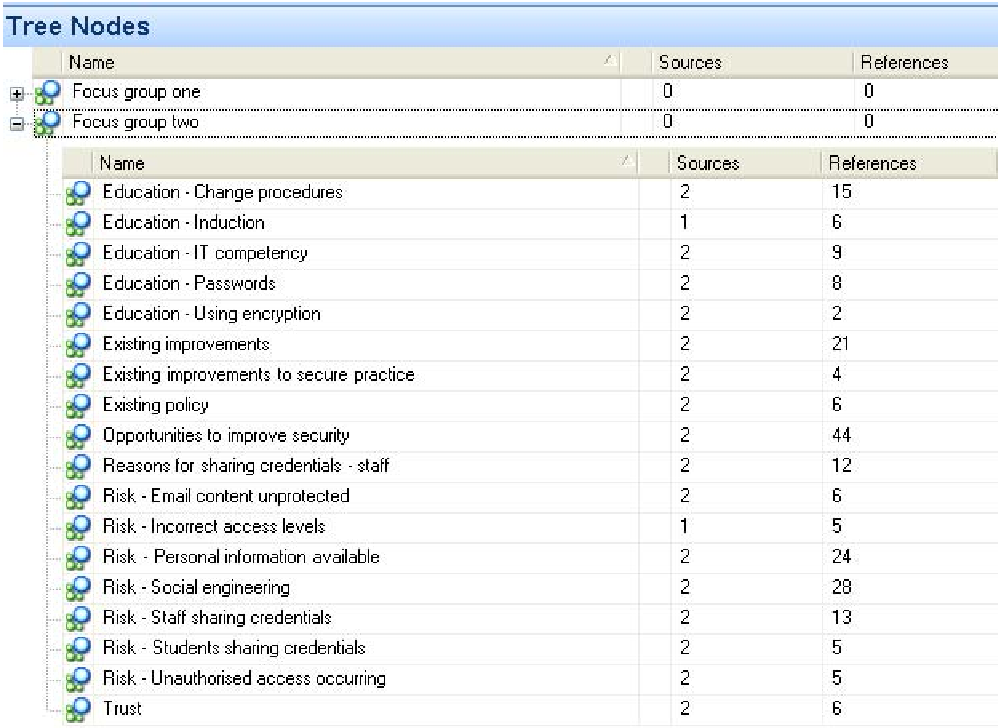
The Leximancer concept map in Figure 16 shows that the theme 'system' is light orange, indicating stronger relevance, connected to the theme 'student'. The thematic summary, Table 5, shows 48% connectivity for the theme 'system'; and the ranked concepts, Table 6, shows 12% relevance with a count of 21. Participants used the word 'system' when discussing usability testing of websites and corporate systems, manual paper processing, corporate applications, and concerns about staff members who are also students processing examinations.

The Leximancer concept map in Figure 16 shows that the theme 'looking', in light green indicating less relevance, is connected to the theme 'student'. The thematic summary, Table 5, shows 39% connectivity for the theme 'system'; and the ranked concepts, Table 6, shows 15% relevance with a count of 26. Participants used the word 'looking' when discussing the alignment of procedures with new software to address risks, the difference in priority processing by centralised systems, issue of staff members also being students and having access to examination papers, the topic of induction and its importance in preparing a new employee for the workplace.

The Leximancer concept map in Figure 16 shows that the theme ‘induction’, in light green indicating less relevance, is connected to the theme ‘student’. The thematic summary, Table 5, shows 18% connectivity for the theme ‘information’; and the ranked concepts, Table 6, shows 8% relevance with a count of 13. Participants used the word ‘induction’ to discuss the value of person-to-person versus online induction, the effect when it was run like a training session in the past and how professional staff created an induction that can also be used for academic staff to overcome problems caused by gaps in the current induction process.

6.5.2 NVivo 8

The next step was to create two tree nodes, one for each focus group. The free nodes were then copied under the corresponding focus group parent node. As the free nodes were used for both focus groups, it shows the areas that were discussed by both focus groups resulting in saturation.



Tree Nodes

Name	Sources	References
Focus group one	0	0
Focus group two	0	0

Name	Sources	References
Education - Change procedures	2	15
Education - Induction	1	6
Education - IT competency	2	9
Education - Passwords	2	8
Education - Using encryption	2	2
Existing improvements	2	21
Existing improvements to secure practice	2	4
Existing policy	2	6
Opportunities to improve security	2	44
Reasons for sharing credentials - staff	2	12
Risk - Email content unprotected	2	6
Risk - Incorrect access levels	1	5
Risk - Personal information available	2	24
Risk - Social engineering	2	28
Risk - Staff sharing credentials	2	13
Risk - Students sharing credentials	2	5
Risk - Unauthorised access occurring	2	5
Trust	2	6

Figure 17: NVivo tree nodes - Focus group two

Focus group two differentiated itself by focusing on induction and incorrect access levels. This focus group had a more managerial view of the same processes. However, saturation was achieved as all the other nodes are shared with the first focus group.

6.5.2.1 Education – Change procedures

Participants considered in more detail the implications of having ‘access’ to ‘all student records’, particularly where ‘staff members’ are also ‘students’.

> *I suppose in the faculty, from the faculty professional staff view point, we would mostly all have access to student records, and I suppose this is really an ethical issue as well isn’t it whether people access information about someone who is a student which they may not necessarily need to do their job but just for some personal interest, whether that’s a gain or whether it’s just you know, somebody thinks ‘Oh I wonder what they got in their exam’ if they happen to know that maybe another staff member is a student with us, that’s quite common isn’t it in our faculty anyway we have got a lot of staff that are also students and it would be possible for someone else in the faculty to access that information from just a desire to know not for any professional reasons. Is that the kind of thing you were thinking?*

Participants discussed being aware of the risks when ‘logged into at the beginning of a shift’ and best practice of, when walking away from the computer, ‘you leave it you lock it’, particularly as the login provides access to ‘borrower records’.

> *The second one is the fact that and this is something that come up in any library that I’ve worked with, is that we’ve got to be security conscious about our computers, because a library is public space. What that basically means is on the information desk where I will be logged into at the beginning of a shift on the information desk I’ll log into virtual which is our, which has got all of our borrower records on, so that’s everything from their home address to mailing address, email, telephone, date of birth the whole works, is all in that borrower data base, as well as logging onto other systems that we use. Now if, a student say was to come to the desk, and say, ‘listen I can’t find this it’s on the other side of the library’ I get up and I walk away, essentially from the information desk that generally can’t be seen from the other desk, from the loans desk. Realistically we would be very much reliant on somebody realising that somebody who wasn’t meant to be there was sat there tapping away at the keyboard. So very much getting into the habit of if you leave it you lock it. That’s pretty much the*

> *way that I would say most people would be operating now. It’s keeping in the back of your head. What could a student do if they sat down and I’m logged in with all of my access? The third is of course we have the licensing agreements for all of our data bases, which very strictly state that we can’t provide the information to anyone who is not a current USQ student or staff member~~.~~*

Participants discussed the situation of staff leaving after a contract period finished and, ‘3 months after’ they left, ‘email was still set up’ and ‘password’ and access still worked.

> *On the flip side of that, the experience that I had when I finished my first contract here, went back to my other job, and a job as a research assistant came up 3 months after I had actually left and I was contacted by the researchers and they said would you be interested in the job, yeh not a problem, and I came in to sign all of the paperwork, and they said we will have to get all of your access going and one of them said out of idol curiosity, log onto this computer here and just see if your old details are still on the system and I could get access to everything. I had been out of, my contract had expired 3 months prior to that my email was still set up, all my password still worked the whole works. There really wasn’t too much that I couldn’t get into and even when you look at some staff, and I have seen this happen very recently when some staff that I know throughout the university have moved onto jobs with other universities, they will say oh I’m leaving now, but my official leaving date is 6 weeks time and then 6 weeks after the fact you will get another email, which states, if you need to get in contact with me I’m now at where ever here is my new email address because as of this Friday my USQ details stop working. Whether or not that is a security breach for us to have staff moving on but they still have access to everything for the next 6 weeks.*

Participants discussed the situation, where staff members intend leaving employment, but first use up their ‘long service’, ‘annual leave’ or ‘rec leave’. In the meantime, they are still ‘officially a USQ staff member’.

> *They are still officially employed because if they leave they say they are going to use their long service, going to use my annual leave, or rec leave or whatever up so they are still officially a USQ staff member, however they may not actually be working here they may be already starting their job at a new institution.*

Participants discussed both the ‘induction process’ and ‘exit interviews’.

> *We were having a conversation about this in the faculty recently and I believe that there is some provision by the university to keep their email account current for about a month so that if, and this was particularly in the academic staff who may have some email from students or need to finalise something that after they’ve officially left even so is some level of continuation, I think a lot depends on whether, you know, as the induction process being perhaps less than adequate, we don’t really have a very rigid system in place for doing exit interviews, you know in the faculty we have a check list that we make sure we get back people’s keys, and any university phones or laptops or whatever they may have had, but you know, we know that sometimes, well we have an office upstairs for a staff member that is no longer employed by us but all of her personal effects are still there. I mean that is a bit of a special case but never the less she has still got her keys, and everything else.*
>
> *Does the exit side of things really focus on the physical objects that you have collected?*
>
> *Yes, I think so, I don’t think it goes, beyond the faculty to, you know, to systems cut off and that sort of thing.*

Participants said that while ‘HR can disable accounts now’ when ‘someone leaves’, the responsibility for that is ‘entirely up to the supervisor’, and that ‘there isn’t any real guidance’ ‘from HR’ about ‘how those things should be managed’.

> *So, as part of, if we significantly tightened up that aspect, HR can disable accounts now, that, after a period that someone leaves the issue is that it is entirely up to the supervisor of the person that is actually leaving. So the supervisor can request that particular condition and request a new cut off be instant. It happens, it's like an email extension request like after 6 months, but yeh, there is something in place basically limits exposure we do keep peoples account and data active like I said it could be *** or something like that, but the number of people changes between positions like have a month break here or there are a lot of data actually kept, apart from actually terminating your privileges which has changed just recently it's completely up to the supervisor and some supervisors are very rigid about that, and some supervisors just let it go,*
>
> *There isn't any real guidance that comes from HR on how those things should be managed. I mean we have this whole documented recruitment and selection process and you have to do the training and all that sort of stuff, but once you are here there really isn't very much in the way of guidance for staff. In fact we have just put in a request now to HR for our heads of school to get some guidance on how best to manage poor performance, because it's an issue in certain pockets. People aren't equipped to know how to really manage it.*

In regards to induction, participants discussed that 'online material' would allow people to 'skim it', because it only requires to be ticked, and new staff would miss out on the 'soft information' that people would pick up in conversations and that 'every single school' and 'every single faculty' 'is different' in the way things are done.

> *Yeh, I'm doing this online material because I have to, and if I tick all the boxes then they will let me get on with my job, and so you skim it, and move through it, and I think that an online course like that would fail to capture all of the soft information. Like if you were running a faculty induction you would have, sort of your break for coffee and during the coffee break you might say to someone, incidentally, we have a social club if you're interested come and see me later on. I'll get you some forms and that, the online and it doesn't contextualise to well either, because as you say, every single school, every single faculty is different in the way that they do things. How can you get a one size fits all electronic solution to that?*

> *I don't think it's meant to be one size fits all. I think there is almost two parts to inductions. There is a compliance issue and it is a compliance issue to have all the broad university perspective, but then I think it does come down to the individual section so one. I think that more of the responsibility has to put on the supervisor, or the new staff member that there should be a check list that you go through and they check them off, like there is a social club. I think there really is a two side, you get the compliance at the top and that is wheat HR I'm sur is going to point out to us all, but you have to have that personal responsibility of the supervisor, I don't think you could possibly blame HR for doing inductions and as you said each environment is very different. As I'm sure the faculty is really different from marketing services and we have our own little, supervisor sits down with them.*
>
> *Actually it's funny, when I first came here about 15 odd years ago, the induction was really good, HR sat us down in a room basically for the day and went through all of the ethical concerns, security, and privacy and that sort of stuff in a huge amount of detail. None of that exists any more, back then it was the only way they could get to do it, they had to get you to sit down for the entire day. It might be 17 years ago. It's a while ago. Yeh, it used to be very efficient.*

Participants are saying that they used to have 'a HR person within' their 'section' who would look after the 'sign ons', 'log ins', 'credentials', which now has 'gone to HR', and that this is 'the reason' that 'people use other credentials'.

> *you mentioned when you had a HR person within your section, that person would look after sign ons, log ins, credentials that's now gone to HR, do you see that as being the reason as such delay that people use other credentials?*
>
> *The delay is the reason why people will do, yes.*
>
> *And is that because you don't have the log on HR person did it?*
>
> *No*

Participants compared their experience of the induction process in a financial institution with that of their current position. Their concern was that for a 'student enquiry' they were not advised what they needed to 'identify' for 'privacy' reasons when dealing with a student enquiry.

> *I think a really good point about the whole induction, I think it's really depending on what role, so I actually came to the university from a bank, so having known how strict that is and actually going into a role where I was dealing with student enquiry and that sort of thing but not even being sort of sat down and saying okay for privacy you need to identify these persons in 3 different ways or something like that which was a complete different contrast to the bank and I found, that was very interesting I thought that would be a standard procedure. If you are going into that type of role that you would have policies within that section that you would be sat down, as part of your induction. Okay this is what we expect when you're identifying your student on the phone or this is what we expect when you are sitting at the front desk you have got a student coming to see you, and you need to walk away from the computer you need to lock it. Simple things like that, that were never discussed.*
>
> *Within our section, I don't think we are really told much confidential data.*

6.5.2.2 Education – Induction

Participants thought that 'universities' induction methods' were 'lacking' 'information', and their own induction was 'inadequate'. The re-evaluation of current induction processes within the faculty and the existing 'freedom of information sessions' and 'ethical issues' were not highlighted sufficiently in regard to their 'access'. In addition, they thought that 'freedom of information' and the 'handling of information' were voluntary training sessions, while 'workplace health and safety' as well as 'workplace harassment' were mandatory.

> *'m not sure what could be done in that sort of scenario but I do believe that universities induction methods are lacking in regards to informing, well it's a bit difficult for me to say this because I have been at the university for 15 years but I know that when I came my induction which I didn't get until after I had been here for over a year and half, 2 years because I was on casual contracts, but it was very inadequate, and it's on my mind at the moment because we are currently looking at what we do in the faculty and I know there are freedom of information sessions and all that sort of thing, but I just think the whole ethical issues around the information that we have access to as staff members is not highlighted enough. I think we just rely on people's honesty and good will without there being any real explanations to new staff or even regular ongoing reminders to continuing staff that we are dealing with personal information and we have certain responsibilities about dealing with that information correctly. I was*

actually talking to someone yesterday who works at centrelink, no her husband works at centrelink, and she was telling me every time her husband looks up a centrelink recipient it's recorded and there is even in fact he has a little device on his desk, I am not sure what it is exactly, but if he's been out of his database for a while and then wants to re-access it he has to actually get a new password and it sort of rolls over on a frequent basis, I don't know all the technical details, we were just having this conversation in the hallway and she was saying about how the systems at centrelink are much tighter, than anything we have got here, and possibly it is a different level of information you have got about people, but she said even her husband who works there, cannot look up the records of what payments have been made to his wife, because that is a breach of security. So it's a family thing, but you cannot look up information about someone else unless you prove that you are working on a case. Only the cases that you have got there, are the only people you are allowed to access, possibly that level of security may be a little over the top for us here, but it just highlights that we don't really have any clear guidelines and we don't as I said new staff come along who is responsible for giving staff those guidelines and I think it's one of those too hard things.

It always strikes me as odd, that every single year we get the email through with that mandatory online training <u>for workplace health and safety</u>, <u>workplace harassment</u> and that's mandatory and you get chased up if you don't do it but all of the professional development stuff on <u>freedom of information</u> and <u>handling information</u> they are all <u>voluntary</u>. Yet we all do it. So it's one of those things that perhaps we need that sort of a training module, just to not necessarily, because we are expecting people to take a couple of hours out of their day and learn it all off by heart but if you got a yearly reminder that was mandated that was go through this, it will just refresh your memory a bit, then it shows that this is something the organisation takes seriously. Rather that running something, and saying, well if you feel like coming along register here.

Participants were concerned with a 'new online induction', due to 'centralisation' of 'certain services' and having 'lost our HR person in the faculty' and 'central HR don't do everything', the 'residual amount of work that remains in the faculty' with 'no one there to do it' resulted in creating their own 'induction' and a 'working group' of 'professional staff' designing induction processes for professional and academics.

> *Well I think, I know that HR are currently about to release new online induction for all new USQ staff and it has been worked on for some time, but one of the problems with our OP and centralisation of certain services is that HR is one of those things that is being centralised so we lost our HR person in the faculty but the central HR don’t do everything. So there’s a residual amount of work that remains in the faculty but there is no one there to do it. So in our own induction is we have just got a working group going amongst the professional staff we are actually looking at overall induction not just for the professional staff but for any new academics so that we are trying to alleviate some of the problems with when new people come because when you lose your central person, well you know, she used to organise the access and she used to organise this that and the other. The school admin officers are saying well we need to have a much more, the experience that a new academic coming into the school of law may be completely different to the experience of someone coming into the school of information simply based on the experience and the knowledge of a school admin officer, and if you have got new school admin officers in a new school, where there is no history, no documented procedures it’s very much trial and error, and that can be incredibly frustrating for new staff, who 6 months after they got here they suddenly find, ‘Oh, I could have been in the faculty social club, I could have been doing this, or I could have support from here or there’ they just don’t know. So I think it will be interesting when we finally see the university’s induction. Personally, and this might be an age related thing. I know online interactive kind of things are less resource intensive in the long run, once the online induction has been or the training has been established, you know, it requires no further input, from anyone else, except the person. I don’t think that is a very welcoming or a very effective way of inducting someone into an organisation. That’s just my personal opinion and maybe age related.*

6.5.2.3 Education – IT competency

Participants discussed the situation of a ‘forged’ ‘transcript’, and how most participants had ‘never seen an official transcript’ to be able to identify it.

> *Well I really don’t know how the student would have, he must have obviously seen someone else’s official transcript, to have been able to produce*
>
> *Isn’t there watermarking in the copy*
>
> *Yes, but when I read at the bottom of the document that he forged there was a little sort of, and I don’t know, you see I’ve never seen an official transcript, you know, who*

> *signs it and the watermark that you speak of and things like that, I've never ever seen one. So I've got nothing to compare it with, but that's why I sent it to student management to check it out.*

Participants also discussed the issue of not knowing how to 'identify' a student for 'privacy' purposes, as well as guidelines on when to 'lock' the computer.

> *I think a really good point about the whole induction, I think it's really dependant on what role, so I actually came to the university from a bank, so having known how strict that is and actually going into a role where I was dealing with student enquiry and that sort of thing but not even being sort of sat down and saying okay for privacy you need to identify these persons in 3 different ways or something like that which was a complete different contrast to the bank and I found, that was very interesting I thought that would be a standard procedure. If you are going into that type of role that you would have policies within that section that you would be sat down, as part of your induction. Okay this is what we expect when you're identifying your student on the phone or this is what we expect when you are sitting at the front desk you have got a student coming to see you, and yo need to walk away from the computer you need to lock it. Simple things like that, that were never discussed.*
>
> *Within our section, I don't think we are really told much confidential data.*

6.5.2.4 Education – Passwords

Participants discussed issues regarding passwords, such as the possibility now exists for 'HR to disable accounts', but that it is still up to the 'supervisor' of the person leaving employment. Participants also stated that 'HR' has not provided any 'guidance' on how the supervisor should manage this aspect.

> *So, as part of, if we significantly tightened up that aspect, HR can disable accounts now, that, after a period that someone leaves the issue is that it is entirely up to the supervisor of the person that is actually leaving. So the supervisor can request that particular condition and request a new cut off be instant. It happens, it's like an email extension request like after *** months, but yeh, there is something in place basically limits exposure we do keep peoples account and data active like I said it could be *** days or something like that, but the number of people changes between positions like have a month break here or there are a lot of data actually kept, apart from actually terminating your privileges which has changed just recently it's completely up to the supervisor and some supervisors are very rigid about that, and some supervisors just let it go,*
>
> *There isn't any real guidance that comes from HR on how those things should be managed. I mean we have this whole documented recruitment and selection process and you have to do the training and all that sort of stuff, but once you are here there really isn't very much in the way of guidance for staff. In fact we have just put in a request now to HR for our heads of school to get some guidance on how best to manage poor performance, because it's an issue in certain pockets. People aren't equipped to know how to really manage it.*

Participants described that when a staff member leaves employment, they use 'long service', 'annual' or 'rec' 'leave' and are 'still officially employed', while not 'actually' 'working' at the university and may already be starting a new 'job'.

> *They are still officially employed because if they leave they say they are going to use their long service, going to use my annual leave, or rec leave or whatever up so they are still officially a USQ staff member, however they may not actually be working here they may be already starting their job at a new institution.*

6.5.2.5 Existing improvements

Participants discussed the previous procedure of extracting 'student data' from the 'database' to create 'reports' that would be 'emailed' to 'various marketers around the university'.   This process was stopped as the participants were concerned about 'what are they doing with it'. In addition, 'online forms' that collect 'student' 'data' now have 'the correct disclaimers attached', and considerations are given to 'how long' the participants will be 'keeping' these details, and 'how are they storing' this information.

> *Probably two things come to mind, in the area that we work. We often pull out perspective student data, from the database that we use, previously in the past we would actually sort of run reports and then these reports would maybe be in excel a spreadsheet format which would get emailed to various marketers around the university. So, we've actually sort of stopped doing that because we had concerns about okay, we've given them this data, what are they doing with it? So as an interim measure we upload them to our sharepoint site and that‘s where we stop ourselves from passing it on, and it's also limiting access to people who have access to that section within our sharepoint site. The second example is that we create online forms on the USQ website which collects data of maybe students, it can be different organisations, staff etc, and we work quite closely with the legal office, having the correct disclaimers attached to forma, and also looking into how long they will be keeping this information for, where is it stored, how are they storing it, who are they giving access to it.*

Participants are also working with the 'legal office' to determine 'what kind of information' they should 'capture online' to comply with 'privacy'.

> *We are kind of working with the legal office at the moment, because I think the privacy things they've just been talking to us about them. They are making changes to the privacy or something that they were interested on, what kind of information we capture online.*

Participants explained how they have 'consent forms' and work with 'legal office' to 'film current students' to obtain their 'comments about' the 'handbook' and 'student centre enrolment part'. They 'show this' and the 'videos' 'to the client that requested it'. In addition, they also ensure that they 'don't forward' these 'videos', and 'keep a log' of everybody 'who has seen it'.

> *So we actually have, consent forms and everything through the legal office then what we do is we often a client request this so if it's like the handbook or something like that or the student centre enrolment part, we film current students and their comments about it, and we often show this, obviously these videos, exert of these video's to the client that requested it. So we have to be careful that we don't forward on those presentations, and we keep a log of everybody who has seen it, because that could influence people decisions about that student.*

Participants revealed that they 'sought advice from the legal office' to obtain professional advice that they could put into place.

> *I think before we started we sought advice from the legal office. So we went and got professional advice and put into place what they suggested.*

6.5.2.6 Existing improvements to secure practice

In regard to security, participants mentioned that the 'paper system' marking the 'assignments' and sending them 'back' does not leave any information that needs securing.

> *With the paper system you get the assignment, you mark it, you enter the marks the assignment goes back so we don't have anything left.*

Participants discussed the changes in practice after seeking 'advice from the legal office'.

> *And the process that you put into place, I know you were talking earlier with the films and everything that you decided yourself, that it wasn't the appropriate way to do things, and you cut back on that, is that something that came from your own experience or from a supervisor or someone else?*
> *I think before we started we sought advice from the legal office. So we went and got professional advice and put into place what they suggested.*

6.5.2.7 Existing policy

Participants discussed how the 'legal office' is currently 'making changes to the privacy' policies.

> *We are kind of working with the legal office at the moment, because I think the privacy things they've just been talking to us about them. They are making changes to the privacy or something, that they were interested on, what kind of information we capture online.*

6.5.2.8 Opportunities to improve security

Participants outlined that a 'professional staff' member could 'have access to student records' and that the reason 'to access that information' may originate from a 'desire to know' rather than for 'professional reasons'.

> *I suppose in the faculty, from the faculty professional staff view point, we would mostly all have access to student records, and I suppose this is really an ethical issue as well isn't it whether people access information about someone who is a student which they may not necessarily need to do their job but just for some personal interest, whether that's a gain or whether it's just you know, somebody thinks 'Oh I wonder what they got in their exam' if they happen to know that maybe another staff member is a student with us, that's quite common isn't it in our faculty anyway we have got a lot of staff that are also students and it would be possible for someone else in the faculty to access that information from just a desire to know not for any professional reasons..*

Participants reflected on the situation where a staff member who is processing 'exams' was also a student, and had to be blocked from 'access' to 'the particular exams', as there currently is no way to 'automatically block them' from it. This required one staff member remembering to specify those relevant staff members and to 'rely on their honesty'.

> *In relation to those, when it came to exam time remember those who were taking *** exams that were working with us in the area, we had to block them from that access on that particular time, so they didn't get to see the question paper for the particular exams. It doesn't automatically block them, so we had to remember to, and rely on their honesty, to which mostly they did but you did rely on their honesty, and not to have a look in the back room.*

Participants discussed the issue of how an 'email trail' would allow students 'direct access to individuals', and how the participants are 'careful about looking back' to determine if they 'need that information going out to the student'.

> *Firstly because of the number of different areas, within the library, and the number of places that we liaise with often to deal with student enquiries, trying to be conscious of as said before and the email trail, that is generated you can often find that it would give students access or direct access to individuals within the university as far as there email address and things like that when admittingly if they did the staff search for example they would be able to find out that information anyway, but we always rather careful about looking back through that and say well okay cool, so we've spoken with, the assistant director or somebody, do we need that information going out to the student or can we crop that off.*

Participants voiced their concern about 'external database in America' such as 'Turnitin', where a 'debate' over who owns the 'PhD, doctorate work exists, particularly if the database is 'compromised', and reliance is on their 'security measures'.

> *The only thing that I would say as potential risk would be, with electronics, there is definitely a market for the sale of assignments or various assessments and I know even the discussion with the use of TurnitIn being an external database in America, where there's debate over who owns the work particularly where it's PhD, doctorate work where it's been presented for the first time, once you run it through turn it in then it is actually now on a database, and who owns that, and if that's compromised at a later point by, we don't facilitate that database so we are relying on Turnitin to have security measures a lot of that work will encompass information from sources that you know they want it to remain confidential, it's you know, it's even generic assignments where if it's project management it's somebody basing that assignment on their company, the company will allow that specific information to go into that assessment but not for it to be published. So there's security and debate over the validity of that.*

Participants discussed the varying 'different' ways 'of operating' in faculties and among professional staff. There are 'generic positions', but 'different departments operate' 'differently'. Roles and responsibilities' are not 'the same across' the university.

> *I think too that each faculty has a different way of operating, and it is the same with professional staff, I mean, whilst there are generic positions different departments operate those positions differently. Their roles and responsibilities aren't necessarily the same across the board so, certain people will have a greater degree of access to*

> *information in what is deemed a role and you go to the next faculty or department and they do something completely different. Or they don't have the same level of access, and so, you know, across the university there's a lot of flexibility to provide what each department needs themselves or each faculty needs themselves and it's the same with access you know, what we might want our partners or markers or tutors or academics to have access to doesn't fit what the next one does. So you get this overly broad spectrum of access and I suppose potentially that is where you get compromise.*

Participants also discussed the issue of staff members leaving employment who are 'still officially employed' while taking 'long service', 'annual leave', and 'rec leave'.

> *They are still officially employed because if they leave they say they are going to use their long service, going to use my annual leave, or rec leave or whatever up so they are still officially a USQ staff member, however they may not actually be working here they may be already starting their job at a new institution.*

Participants also pointed out that other organisations are 'told as part of the induction process', that when starting employment with a competitor 'you are leaving today; we will need your keys right now'.

> *And I suppose it depends, as well on how the university wants to deal with staff leaving for example my wife works for a bank and she's been told as part of the induction process, If she was to get a job at another bank and basically say to them, 'hey I'm moving onto somewhere else' they would actually say, well normally you would have your two weeks leave, we are terribly sorry but you are leaving today we will need your keys right now, and she said her log on and all of her electronic details would be locked out within the hour, and she would be told that she was on leave as of now. Because, they take the integrity of that information very seriously. Even when you look at the chain department stores, my father used to manage for Target for a long while and he has an assistant manager move onto Myer, and because they were a direct competitor it was a case of well we are really sorry to do this to you but keys now please, and he was sent home that morning. So, I know it's probably way over the top, with what you were saying about centrelink, for the university to say well you're going to know the university bank, we'll have your keys and lock you out now, but I think that we do need a process in place for managing the exit side of things.*

Participants voiced their concern over ‘hard copies’ that contain ‘personal details’ such as ‘certificates’ when ‘employing somebody’, and other ‘confidential information’ being posted to ‘HR’ through ‘pick up to delivery’ when it is known that ‘HR has lost a lot of forms or it got lost on the way’.

> *There could be concern there though to, when you are saying we only, you know, we want so many hard copies when employing somebody and then ask for the personal details and certificates and other things that would be private and confidential information and when we had it within the faculty it was kind of, I guess, you could say it was fairly secure because we knew it was all in that one area. But now if you’re putting it in the post to go to HR and we have known that HR has lost a lot of forms or it’s got lost on the way, from pick up to delivery. Then there is also the potential risk of confidential information getting into the wrong hands.*

Participants also discussed that material is ‘walked to HR and Finance’ as part of the process of ‘put it in the pick tray’ and have it ‘hand delivered’.

> *Well some of our stuff is walked to HR and Finance and stuff like that, but it doesn’t happen as a process. It just depends on who is sending it as to whether they stick it in the mailbag or put it in the pick tray to be picked up, and hand delivered.*

Participants discussed the issues with this kind of hand delivery, where one participant had ‘something come in the mail from the legal office and it took 3 days’, ‘a *** document’ that is ‘floating around the university somewhere’.

> *No, not all of the sensitive things, we have a collection point for materials to be walked to certain designated areas in the university. HR is one of those areas routinely but it depends on the person sending that information as to whether they use that or whether they chose to put in internal mail. I had something come in the mail from the legal office and it took 3 days to get here. You know, they told me they sent it, they put it in the internal mail on Monday last week and I didn't get it until Wednesday afternoon. In the meantime, it was a *** document, it was an *** so you know, it's floating around the university somewhere.*

Participants pointed out that 'most people in the faculty' probably know about this, and that it was intended for 'quick transfer' of 'student files'.

> *Well I think most people in the faculty probably know of it's existence and we don't want to make it you know, it isn't really, it was initially designed for the quick transfer of student files because they can't be sent in the mail, but, you know, sometimes when you broadcast that kind of service too widely you get people loading up the one person who has got to carry it all around the university unnecessarily. Because they are too busy, too lazy, to walk it there themselves, so you know, you have to be a little bit cautious about what you send.*

6.5.2.9 Reasons for sharing credentials – staff

Participants discussed the issues leading to the situation of credentials being shared so that people can do their work. Participants explained that in the past there was a 'local HR' and a 'local ICT' person in the faculty. Getting a new staff member 'onto a system' was possible to achieve 'in a day'. Through 'centralisation' the HR and ICT person has been moved to their corresponding departments. To add a staff member 'onto a system' now requires the relevant section 'to log a job'. Participants 'don't know how busy they are' as they have to 'service the whole university'. However, centralising the HR and ICT person resulted in 'loss of knowledge' in knowing 'what needs to be done' to add a new staff member 'onto a system'. One participant said that 'HR sent me over all these HR forms to keep in the faculty in case we needed them', even though these forms 'sit in someone's office' and 'it is not in their PD' to look after them.

> *We lost the local HR as well as the local ICT people. Which to get a person onto a system involves two or three different areas, one is the resources person that has the keys physically, and says yes we have got a room for you, and what have you. Yes we can organise a computer, then we had our ICT fellows who were there on the spot. I'm here '*** can you come and fix this for me?', *** would say ' *** we've got this new person starting Monday can you please set up the computer' Then we had our HR person that all had the details to say that the contract has been signed yes it's ready to go. And you could perhaps in a day have that computer up and running. It's not the case now, because the HR section has gone to centralisation, the computer section has gone to ICT. We have to now log a job to them, they just look at the jobs as they come in and wait your turn, you don't know how busy they are and they have got to service the whole university.*
>
> *And because we don't have dedicated people it's that loss of knowledge of what needs to be done. I mean it's very when everybody has a full PD of their own and then you say to them, oh by the way can you, we have a new person starting next week, you know, well who's responsibility is that? In fact I had quite recently had someone in HR send me over all these HR forms to keep in the faculty in case we needed them. I'm thinking well No, you know, because we don't have a HR to look after them. So it means the forms have to sit in someone's office, and it's not in their PD that they do HR but it's up to someone here to fill those forms in. Sorry, I don't mean that to sound so negative, but I think there is a loss of control that we might have had otherwise and the end to end the more holistic approach to someone's employment with us from when they arrive to when they leave.*

6.5.2.10 Risk – Email content unprotected

Participants supposed that it is possible for information to be sent in 'error' when selecting the wrong email address from a previous list of used emails.

> *I don’t know if this is what you are after, but I suppose, there’s always room for error with information going out, where you are directing it to a particular student, and you are entering their email address, in the email addresses there is a student number where you get pre, where you have used student email addresses in the past and if you are not careful and you get a pre empted address come up, you choose it, and then it’s not the right student that information, if theirs is confidential stuff that might go out inappropriately but.*

In addition, ‘forwarding’ emails that have ‘a long email trail’ that refers ‘to a number of different students within the email’ may ‘end up’ being accessed by one student if ‘that screening process’ was not applied.

> *And even forwarding emails if you, if there’s a long email trail and I know that this sort of can happen because people I know in central records tell me that when we send information to them recording on the student file they have to be quite careful, because sometimes you will get an inquiry particularly from a partner where they may refer to a number of different students within the email and then you can end up sending all that to a student record and with the student chooses to access that file, if that screening process hasn’t been done by someone there could be information on the students file about other students.*

Participants explained that ‘student records’ or ‘central records’ are required to remove references to ‘other student names, numbers’, which is ‘labour intensive’. In addition ‘a whole range of other people’ may be copied into the email.

> *Well people in student records or central records specifically have to go through and read the stuff that comes to them for filing on the students files. So if there is mention of other students other student names, numbers, you know, they either have to, I don’t know if they cut and paste, but I know that in some instances you’ll, when you recall a student’s file you’ll get certain information that’s been blacked out. So it is a labour intensive and just a question of someone sitting down and reviewing the contents of that email trail, and sometimes I’ve noticed particularly when dealing with our partners they will just send the same email backwards and forwards it could be ten times and often people will copy in a whole range of other people who don’t necessarily need to*

> *be involved. I think it's very easy to just copy in lots of people when it's not really relevant, and I guess to a certain extent that can be a danger at times too. There is a risk.*

Participants said that they are 'conscious' of the 'email trail' and in 'looking back' through the email to avoid access to individual's details.

> *Firstly because of the number of different areas, within the library, and the number of places that we liaise with often to deal with student enquiries, trying to be conscious of as said before and the email trail, that is generated you can often find that it would give students access or direct access to individuals within the university as far as there email address and things like that when admittingly if they did the staff search for example they would be able to find out that information anyway, but we always rather careful about looking back through that and say well okay cool, so we've spoken with, the assistant director or somebody, do we need that information going out to the student or can we crop that off.*

6.5.2.11 Risk – Incorrect access levels

Participants pointed out that 'education partners' require 'access' to the 'study desk'. When they have 'tutor access' they were assigned 'non edited teacher' which is currently under consideration as 'they have to have certain amount of access' to 'run the course'.

> *the partners, education partners are wanting access to do the study desk courses for the courses that they are running that particular semester. We are looking at even with the tutor access as to what access level that they should have, because it has been drawn to our attention, in previous, up to date now, tutors are given accesses as non edited teacher on, their respective courses, now from what I understand that gives them, obviously they have to have certain amount of access so that they can run the course.*

Participants describe the complexity of access requirements for the study desk. They highlighted the 'many different levels of access', which has become 'complex' with 'many layers' to cater for the 'course examiners', 'moderator', 'tutors', 'casual tutor' who is employed on a 'contract basis' or 'member of the teaching permanent staff', 'partner' tutors, and those who 'mark assessment'.

> *And I think with study desk there are so many different levels of access it's got so complex, that you know course examiners would require one level of access, then maybe the moderator and then they'll want another level of access for say any tutors they might have involved in the course that might be different between say a casual tutor who is not actually, who is only employed on a contract basis, but it could also be another member of the teaching permanent staff teaching team, so there are so many layers, that I think, even with the tutors we have got tutor access, tutors that only conduct tutorials with their partners which is another level again, and those who also mark assessment and everything seems to have just got so complex and I'm not really sure whether, there's a breakdown in communication I think. The flow of information between various sections of the university.*

Participants repeatedly expressed the view that 'each faculty has a different way of operating' and while 'there are generic positions different departments operate those positions differently'. However, 'there is a lot of flexibility to provide what each department needs' with an 'overly broad spectrum of access'.

> *I think too that each faculty has a different way of operating, and it is the same with professional staff, I mean, whilst there are generic positions different departments operate those positions differently. Their roles and responsibilities aren't necessarily the same across the board so, certain people will have a greater degree of access to information in what is deemed a role and you go to the next faculty or department and they do something completely different. Or they don't have the same level of access, and so, you know, across the university there's a lot of flexibility to provide what each department needs themselves or each faculty needs themselves and it's the same with access you know, what we might want our partners or markers or tutors or academics to have access to doesn't fit what the next one does. So you get this overly broad spectrum of access and I suppose potentially that is where you get compromise.*

Participants highlight that there 'isn't a system' where 'systems access is reviewed' and while moving into a new position and still having access to systems from the previous position allows the participant to perform their work more efficiently, this access may not be 'appropriate'.

> *And even when people within the organisation change roles, whether that is a permanent change or a temporary change there isn't a system whereby the various systems access is reviewed so I've moved from being the ***into *** but my systems access hasn't reduced and it works fine for me, because it means that there is still a lot of issues that come up, that are raised by partners that I can deal with myself, instead of having to refer them onto somebody else. So instead of me sending *** all of these inquiries I can look it up myself, and provide a response email straight away, but it isn't probably appropriate for me in my new role to still have that access.*

6.5.2.12 Risk – Personal information available

Participants voiced their concern regarding 'students' 'group' 'submission', where their submission shows 'their details' 'documented on the front page' allowing each member to see the other student's 'name' and 'student number', or where 'hardcopy' may contain the 'address' as well.

> *Very shortly yeh, another thing is I don't know if it's a huge problem or what you are after but, if you are talking about exposure of information group's submission. Students are submitting their details to collectively they don't necessarily, they're not always friends they could be forming a group because a course examiner puts them in a group for their credit submission but their details are documented on the front page and so each member of that group gets that information so if you are talking about exposure of a student number which may then allow them to get so far with another information then that could be compromised.*
>
> *Is there only the student number or name I suppose as well and?*
>
> *It's definitely the name and student number. On occasions it might be more information then that but it probably depends on the degree of submission. If it's hardcopy then you'll get a postal address generally for each student as well. If it's electronic submission then you won't get that but I suppose it does compromise.*

Participants explained how 'personal contractors' such as 'markers' are given 'restricted access'. However 'the degree' of 'detail' required for the 'paperwork' is considered as 'overkill', as they are 'mapped to those systems' and it is not expected that they could 'cause great harm'. In addition, hard copies with 'personal details' and 'certificates' containing 'private and confidential information' were deemed 'fairly secure' 'within the faculty' as it was confined 'all in that one area'. However, 'putting it in the post to go to HR' knowing that 'HR has lost a lot of forms' between 'pick up to delivery' with the potential to 'risk of confidentiality' and falling into the 'wrong hands' was a concern to participants.

> *Personally, I think getting personal contractors employed here like markers. I think, we are a little bit overkill to all intents they get restricted access they don't get grade book access they basically have been given access to the study desk, but I think the degree detail that you have to go through to get the paperwork finalised to get them access to systems to which, I don't see they are going to cause great harm. The way they are mapped to those systems allows them only certain access, so you are only going to have a problem if that mapping is wrong, but we're talking about you know, the study desk. It's nothing else, so.*
>
> *There could be concern there though to, when you are saying we only, you know, we want so many hard copies when employing somebody and then ask for the personal details and certificates and other things that would be private and confidential information and when we had it within the faculty it was kind of, I guess, you could say it was fairly secure because we knew it was all in that one area. But now if you're putting it in the post to go to HR and we have known that HR has lost a lot of forms or it's got lost on the way, from pick up to delivery. Then there is also the potential risk of confidential information getting into the wrong hands.*

6.5.2.13 Risk – Social engineering

There was an awareness among participants that in the situation of a 'student' 'enquiry', the process of 'verifying' has its own risks in that 'students who are working in a group' may know someone's 'birthday' and 'may use that knowledge' to 'access information'.

> *Because if a student rings with an enquiry, one method of verifying that you are talking to the person who you think you are talking to is to ask them, what their date of birth is. Well, you know, students who are working in a group may not be best friends but they may know when someone's birthday is and so, you know there is a potential risk, that a student that has done some group work may know that about another student and may use that information to access information, that they shouldn't have access to.*

Participants described the situation of 'a collection point for materials to be walked' to certain areas within the university. These materials can also be put into 'internal mail', however, their concern was that this process sometimes 'took 3 days'.

> *No, not all of the sensitive things, we have <u>a collection point for materials to be walked</u> to certain designated areas in the university. HR is one of those areas routinely but it depends on the person sending that information as to whether they use that or whether they chose to put in <u>internal mail</u>. I had something come in the mail from the legal office and it <u>took 3 days</u> to get here. You know, they told me they sent it, they put it in the internal mail on Monday last week and I didn't get it until Wednesday afternoon. In the meantime, it was a *** document, it was an *** so you know, it's floating around the university somewhere.*

Participants stipulated that a 'competitive' 'higher education market' resulted in 'unintentionally passing on information' to 'someone else at another institution' or to someone 'around the dinner table'.

> *Given the <u>competitive</u> nature of the <u>higher education market</u>, I mean working in your area of the university, you could be seen to be having access to information, say on the new brand for example or an upcoming campaign, there is with the amount of communication that goes on with sections in any universities, with other universities, there is some potential that there could be risks of either <u>unintentionally passing on information</u> to someone else you might know, even if it's not directly to <u>someone else at another institution</u>, but it could be, you know you have a conversation at home around the <u>dinner table</u> or someone else in your family might have a friend or relative or, you know who is chatting*
>
> *Who works for TV.*
>
> *Yeh, exactly, and you imagine that if we had something like, something that is quite unique to our institution whether you say that's fulfilling lives or whether you say that's a university for a real world. Well if they were conversations that were happening about a change and you are throwing ideas around that, don't know whether you do, but you could there is a potential there, isn't there for there to be, even though you're not dealing so much now necessarily with student information but that corporate and brand.*

Participants agreed that ‘a strategic campaign’ activity has the potential for ‘social’ engineering.

> *I would say a good example is we are about to release a new future students website, so we built it, and it’s locked down to the IP addresses in our area, so nobody could access it, but yeh you are right it is a strategic campaign activities*
>
> *Yeh, and very any section of the university, I think, in any organisation there would be some potential for that.*
>
> *And I wonder if it is the social, because I just recently came back from a conference with a lot of other university people and there were some web site people there. I wonder if it’s just like, I know also when we do the PeopleSoft upgrades and things like that we do share a lot of data*
>
> *Because you want to share the experience, don’t you*

Participants recognise that ‘a social environment of tertiary education in Australia’ may lead them to ‘share quite a lot’. While considering the exchange of information about what ‘other universities’ are ‘doing with their websites’ and ‘what software they are going to use’, it also provides a ‘glimpse into their new marketing campaigns’. However, participant conversations lead to the realisation that the tertiary environment is ‘starting to get more and more competitive’ because there is ‘not that many students around to share’.

> *wonder if it is a social environment of tertiary education in Australia, that we do share quite a lot. So when I was there they were talking about their right now upgrade and how did it go for them and we have been and visited other universities what they are doing with their websites, how they are going about it, and what software they are going to use, we get a glimpse into their new marketing campaigns and what they are going to do. Bring that back here and tell our marketers that. So I wonder if it’s just the nature of the tertiary environment here that we do share quite a bit of information, of what other universities are doing.*
>
> *Yeh, I suppose it’s different in the aspect that we’re not, whilst we are competing for students and income it’s a little bit different of industry when you are looking at profit, producing a product to sell to make a profit. Obviously we want to be able to*
>
> *If I know what the university of Sunshine Coast is doing with their website or QT is about to do with theirs.*
>
> *But this is a good point because I think universities are starting to get more and more competitive because there are not that many students around to share, so*

> *And with potential deregulation in 2012, that could potentially, well if it comes through, it will change the life of the place very, very severely.*
>
> *But like, not us personally, but I know some of the marketers that can tell okay, so QT their first round references are up by so much they get all of that data from QTAC. So it's also other agencies letting us know what other universities are doing.*
>
> *But also, we are not a private institution either, we are semi government. It would be very different if we were a private profitable institution, even just a private institution it would be different altogether.*

6.5.2.14 Risk – Staff sharing credentials

Participants discussed the case of a previous employee still having access after '3 months', and their 'password' still working.

> *On the flip side of that, the experience that I had when I finished my first contract here, went back to my other job, and a job as a research assistant came up 3 months after I had actually left and I was contacted by the researchers and they said would you be interested in the job, yeh not a problem, and I came in to sign all of the paperwork, and they said we will have to get all of your access going and one of them said out of idol curiosity, log onto this computer here and just see if your old details are still on the system and I could get access to everything. I had been out of, my contract had expired 3 months prior to that my email was still set up, all my password still worked the whole works. There really wasn't too much that I couldn't get into and even when you look at some staff, and I have seen this happen very recently when some staff that I know throughout the university have moved onto jobs with other universities, they will say oh I'm leaving now, but my official leaving date is 6 weeks time and then 6 weeks after the fact you will get another email, which states, if you need to get in contact with me I'm now at where ever here is my new email address because as of this Friday my USQ details stop working. Whether or not that is a security breach for us to have staff moving on but they still have access to everything for the next 6 weeks.*

6.5.2.15 Risk – Students sharing credentials

One aspect of 'social engineering' discussed by participants related to the 'sharing' of 'user names and passwords'. Participants believe that this practice is driven by the need for increased 'Internet quota'.

> *I don't see how a lot of things from the social engineering aspect. We see a little bit of that in the residential colleges where students are sharing usernames and passwords and those sorts of things. Do one student a favour, you know, logging in as him and checking something for him and then he can use the password indefinitely after that. We used to see a lot of that particularly when students were given Internet quota, that was a prized, if you could get someone else's username and password you could use their quota for them. We regularly had you know, accounts from the res colleges being logged in and used even though the student was a resident of ***, and they never set foot on campus. They were freely sharing it with friends and stuff. We do see other sort of aspects, social engineering access to information, I don't see a lot of it really.*

6.5.2.16 Risk – Unauthorised access occurring

Participants explained that, typically, while 'still officially employed', staff members leaving employment will use 'long service', 'annual' and 'rec leave', but are still regarded as a USQ staff member despite 'not actually working here' or already 'starting their job at a new institution'.

> *They are still officially employed because if they leave they say they are going to use their long service, going to use my annual leave, or rec leave or whatever up so they are still officially a USQ staff member, however they may not actually be working here they may be already starting their job at a new institution.*

Participants explained the exit policy, whereby 'academic staff'' keep their email account current' to complete correspondence with students after they have 'officially left'. The concern was raised that there is not a 'very rigid system in place for doing exit interviews' and it lacks a follow up mechanism.

> *We were having a conversation about this in the faculty recently and I believe that there is some provision by the university to keep their email account current for about a *** so that if, and this was particularly in the academic staff who may have some email from students or need to finalise something that after they've officially left even so is some level of continuation, I think a lot depends on whether, you know, as the induction process being perhaps less than adequate, we don't really have a very rigid system in place for doing exit interviews, you know in the faculty we have a check list that we make sure we get back people's keys, and any university phones or laptops or whatever they may have had, but you know, we know that sometimes, well we have an office upstairs for a staff member that is no longer employed by us but all of her personal effects are still there. I mean that is a bit of a special case but never the less she has still got her keys, and everything else.*
>
> *Does the exit side of things really focus on the physical objects that you have collected?*
>
> *Yes, I think so, I don't think it goes, beyond the faculty to, you know, to systems cut off and that sort of thing.*

6.5.2.17 Trust

Participants discussed implied trust when considering the situation where most 'professional staff' 'would mostly all have access to student records' and while there are a 'lot of staff that are also students' it would be possible for them to access personal data.

> *I suppose in the faculty, from the faculty professional staff view point, we would mostly all have access to student records, and I suppose this is really an ethical issue as well isn't it whether people access information about someone who is a student which they may not necessarily need to do their job but just for some personal interest, whether that's a gain or whether it's just you know, somebody thinks 'Oh I wonder what they got in their exam' if they happen to know that maybe another staff member is a student with us, that's quite common isn't it in our faculty anyway we have got a lot of staff that are also students and it would be possible for someone else in the faculty to access that information from just a desire to know not for any professional reasons. Is that the kind of thing you were thinking?*

Participants also discussed the scenario of staff members who are studying but working with 'exams' needing to be excluded from accessing examination information – which may ultimately rely on recall or personal honesty should this exclusion be overlooked.

> *In relation to those, when it came to exam time remember those who were taking business exams that were working with us in the area, we had to block them from that access on that particular time, so they didn't get to see the question paper for the particular exams. It doesn't automatically block them, so we had to remember to, and rely on their honesty, to which mostly they did but you did rely on their honesty, and not to have a look in the back room*
>
> *We have removed exams from the general processing system in order to allow for people who would otherwise have had access to those, not to have access so when I was doing the role that is currently doing, and we had *** and *** at one time studying with us instead of those exams being lodged the way the rest of the faculty lodged them they used to come directly to me*

6.5.2.18 Summary

'Education – Change procedures' highlighted the situation of having access to all student records, particularly where a staff member is also a student. Participants discussed their awareness of risk when logging in at the beginning of a shift, and then having to walk away from the computer and needing to develop the habit of locking the computer first. Participants discussed the situation of leaving work after a contract finished, where three months later email and password were still working. Other participants brought up the situation of staff members leaving employment, but first using up long service, annual or rec leave, while still officially being a staff member. Participants discussed the induction process as being less than adequate for exit interviews. Participants also discussed that while HR can disable accounts, the responsibility is with the supervisor. However, HR has not provided guidance on how this should be managed. Participants also mentioned that online induction training allows people to skim through the process and that it does not suit all sections as schools and faculties all have different ways of doing things. The participants stated that in the past a HR person in their section looked after signons, log ins and credentials, and they indicated that delays cause by changes in these procedures was the reason people shared credentials. Participant compared their own experience with the induction process in other institutions with their current position. Their concern was that they were not advised what they needed to identify for privacy reasons when dealing with a student enquiry.

‘Education – Induction’ highlighted that participants believed that university induction methods were lacking information, and were generally inadequate. Participants were concerned with a ‘new online induction’ due to ‘centralisation’ of ‘certain services’, having ‘lost our HR person in the faculty’ and ‘central HR don’t do everything’, the ‘residual amount of work that remains in the faculty’ with ‘no one there to do it’ resulted in sections creating their own ‘induction’ and a ‘working group’ of ‘professional staff’ designing the process for professional and academics.

‘Education – IT competency’ highlights the situation of a participant being unaware of what an official transcript provided by the university should look like to be able to identify a forged transcript. In addition, participants also mentioned not having been trained on the issue of privacy issues when identifying a student, or given guidelines on when to lock a computer.

‘Education – Passwords’ highlighted the ability of HR to disable accounts, even though it is still up to the supervisor to control this, without guidance from HR on how to manage this aspect. Participants also describe the situation where a staff member leaves employment, takes long service, annual or rec leave and, therefore, is still considered to be employed, despite not actually doing any work or possibility starting a new job.

‘Education – Using encryption’ highlighted issues of secure wireless and encryption as issues that could be resolved with education.

‘Existing improvements’ resulted in participants discussing the previous procedure of extracting ‘student data’ from the ‘database’ to create ‘reports’ that would be ‘emailed’ to ‘various marketers around the university’. This process was stopped as the participants were concerned about ‘what are they doing with it’. In addition, ‘online forms’ that collect ‘student’ ‘data’ now have ‘the correct disclaimers attached’, and considerations are given to ‘how long’ the participants will be ‘keeping’ these details, and ‘how are they storing’ this information. Participants are also working with the ‘legal office’ to determine ‘what kind of information’ should they ‘capture online’ to comply with ‘privacy’. Participants explained how they have ‘consent forms’ and work with ‘legal office’ to ‘film current students’ to obtain their ‘comments about’ the ‘handbook’ and ‘student centre enrolment part’. In addition, they also ensure that they ‘don’t forward’ these ‘videos’ and ‘keep a log’ of everybody ‘who has seen it’. Participants explained how they have ‘consent forms’ and work with the ‘legal office’ to ‘film current students’ to obtain their ‘comments about’ the ‘handbook’ and ‘student centre enrolment part’.

‘Existing improvements to secure practice’ highlighted that in regard to security, participants believe that the ‘paper system’ of marking ‘assignments’ and sending them ‘back’ does not leave any information that needs securing. Participants voiced their concern about ‘external database in America’ such as ‘Turnitin’, where a ‘debate’ over who owns the ‘PhD, doctorate work’, particularly if the database is ‘compromised’, thus we would be relying on their ‘security measures’. Participants discussed the varying ‘different’ ways ‘of operating’ in faculties and among professional staff. There are ‘generic positions’, but ‘different departments operate’ ‘differently’. Roles and responsibilities’ are not ‘the same across’ these areas. Participants also discussed the issue of staff members who are leaving employment being ‘still officially employed’ while taking ‘long service’, ‘annual leave’, and ‘rec leave’. Participants also pointed out that other organisations were ‘told as part of the induction process’, that when starting employment with a competitor ‘you are leaving today we will need your keys right now’. Participants voiced their concern over ‘hard copies’ that contain ‘personal details’ such as ‘certificates’ and when ‘employing somebody’, and other ‘confidential information’ being posted to ‘HR’ through ‘pick up to delivery’ when it is not uncommon that ‘HR has lost a lot of forms or it got lost on the way’. Participants also discussed that material is ‘walked to HR and Finance’ as part of the process of ‘put it in the pick tray’ and have it ‘hand delivered’. Participants discussed the issues with this kind of hand delivery, where ‘something coming in the mail from the legal office and it took 3 days’, ‘a legal document’ that is ‘floating around the university somewhere’.

‘Existing policy’ led participants to reveal that the ‘legal office’ is ‘making changes to the privacy’ policies.

‘Opportunities to improve security’ established that a ‘professional staff’ member could ‘have access to student records’ and that the reason ‘to access that information’ may originate from a ‘desire to know’ rather than for ‘professional reasons’. Participants pointed out the situation where a staff member involved in processing ‘exams’ was also a student, and had to be blocked from ‘access’ to ‘the particular exams’, as there currently is no way to ‘automatically block them’. This required one party to remember and to ‘rely on their honesty’. Participants discussed the issue of an ‘email trail’ allowing students ‘direct access to individuals’, and how the participants are ‘careful about looking back’ to determine if they ‘need that information going out to the student’. Participants pointed out that ‘most people in the faculty’ probably know about this, and that it was intended for ‘quick transfer’ of ‘student files’.

‘Reasons for sharing credentials – staff’ resulted in participants discussing the issues leading to the situation and their belief that credentials are shared so that people can do their work. Participants explained in the past there was a ‘local HR’ and a ‘local ICT’ person in the faculty. To get a new staff member ‘onto a system’ was possible to achieve ‘in a day’. Through ‘centralisation’ the HR and ICT person have been moved to their corresponding departments. To register a new staff member ‘onto a system’ now requires the appropriate staff member ‘to log a job’. Participants felt other staff ‘don’t know how busy they are’ as they have to ‘service the whole university’. However, centralising the HR and ICT functions resulted in ‘loss of knowledge’ in knowing ‘what needs to be done’ to register a new staff member ‘onto a system’. One participant said that ‘HR send me over all these HR forms to keep in the faculty in case we needed them’, even though these forms ‘sit in someone’s office’ and ‘it is not in their PD’ to store these records.

‘Risk – Email content unprotected’ resulted in participants discussing that it is possible for information to go out in ‘error’, by selecting the wrong email address from a previously list of used emails. In addition, ‘forwarding’ emails that have ‘a long email trail’ that refer ‘to a number of different students within the email’ may ‘end up’ being accessed by one student if ‘that screening process’ was not applied. Participants explained that ‘student records’ or ‘central records’ are required to remove references to ‘other student names, numbers’, which is a ‘labour intensive’ exercise. In addition, ‘a whole range of other people’ may be copied into the email. Participants said that they are ‘conscious’ of the ‘email trail’, thus they ensure ‘looking back’ through the email.

‘Risk – Incorrect access levels’ had participants point out that ‘education partners’ require ‘access’ to the ‘study desk’. When staff members have ‘tutor access’ they were given ‘non edited teacher’ status, which is currently under consideration as ‘they have to have certain amount of access’ to ‘run the course’. Participants describe the complexity of access requirements for the study desk. They highlight the ‘many different levels of access’, which has become ‘complex’ with ‘many layers’ to cater for ‘course examiners’, ‘moderator’, ‘tutors’, ‘casual tutor’ employed on a ‘contract basis’ or ‘member of the teaching permanent staff’, and ‘partner’ tutors, those who ‘mark assessment’. Participants continually pointed out that ‘each faculty has a different way of operating’, and that while ‘there are generic positions different departments operate those positions differently’. However, ‘there is a lot of flexibility to provide what each department needs’ with an ‘overly broad spectrum of access’. Participants highlight that there ‘isn’t a system’ where ‘systems access is reviewed’ and while moving into a new position and still having access to systems from the previous position allows the participant to perform their work more efficiently, it is assumed that this access may not be ‘appropriate’.

‘Risk – Personal information available’ had participants explain how ‘personal contractors’ such as ‘markers’ have ‘restricted access’. However ‘the degree’ of ‘detail’ required for the ‘paperwork’ is considered as ‘overkill’, as they are ‘mapped to those systems’ and it is not expected that they could ‘cause great harm’. In addition, hard copies with ‘personal details’ and ‘certificates’ containing ‘private and confidential information’ were deemed ‘fairly secure’ ‘within the faculty’ as it was ‘all in that one area’. However, ‘putting it in the post to go to HR’ knowing that ‘HR has lost a lot of forms’ between ‘pick up to delivery’ with the potential of ‘risk of confidentiality’ and falling into the ‘wrong hands’ was an issue of concern to participants.

‘Risk – Social engineering’ created awareness among participants that in a situation of a ‘student’ and ‘enquiry’ that the process of ‘verifying’ has its own risks, in that ‘students who are working in a group’ may know someone’s ‘birthday’ and ‘may use that’ to ‘access information’. Participants described the situation of ‘a collection point for materials to be walked’ to certain areas within the university. These materials can also be put into ‘internal mail’. Their concern was that sometimes it ‘took 3 days’ to receive materials. Participants stipulated that a ‘competitive’ ‘higher education market’ may result in ‘unintentionally passing on information’ to ‘someone else at another institution’ or ‘around the dinner table’. Participants were aware that ‘a strategic campaign’ activity could be affected in this way. Participants were also aware that the ‘social environment of tertiary education in Australia’ may lead them to ‘share quite a lot’. While considering the exchange of information about what ‘other universities’ are ‘doing with their websites’ and ‘what software they are going to use’, it also provides a ‘glimpse into their new marketing campaigns’. However, participants’ conversations lead to the realisation that this current environment is ‘starting to get more and more competitive’ because there are ‘not that many students around to share’.

‘Risk – Staff Sharing credentials’ had participants discuss the situation of a previous employee still having access after ‘3 months’, with their ‘password’ still working.

‘Risk – Students Sharing credentials’ had participants relate the ‘sharing’ of ‘usernames and passwords’ to ‘social engineering’, a practice they consider is driven by the need for increased ‘Internet quota’.

‘Risk – Unauthorised access occurring’ had participants explain that while ‘still officially employed’ staff members leaving employment will use ‘long service’, ‘annual’ and ‘rec leave’ yet remain ‘still officially a USQ staff member’ without ‘not actually working here’ or ‘starting their job at a new institution’. Participants explained the exit policy, where ‘academic staff’’ keep their email account current’ to complete correspondence with students after they have ‘officially left’. The concern was raised that there is not a ‘very rigid system in place for doing exit interviews’, and lacks a mechanism to make routine checks.

‘Trust’ had participants discuss implied trust when considering the situation where ‘professional staff’ ‘would mostly all have access to student records’ and since there are a ‘lot of staff who are also students’, it would be possible for them to access that information. Participants also discussed the issue of staff members who are studying and working and access by these people to ‘exams’ being blocked by either remembering to put procedures in place or relying on individual honesty.

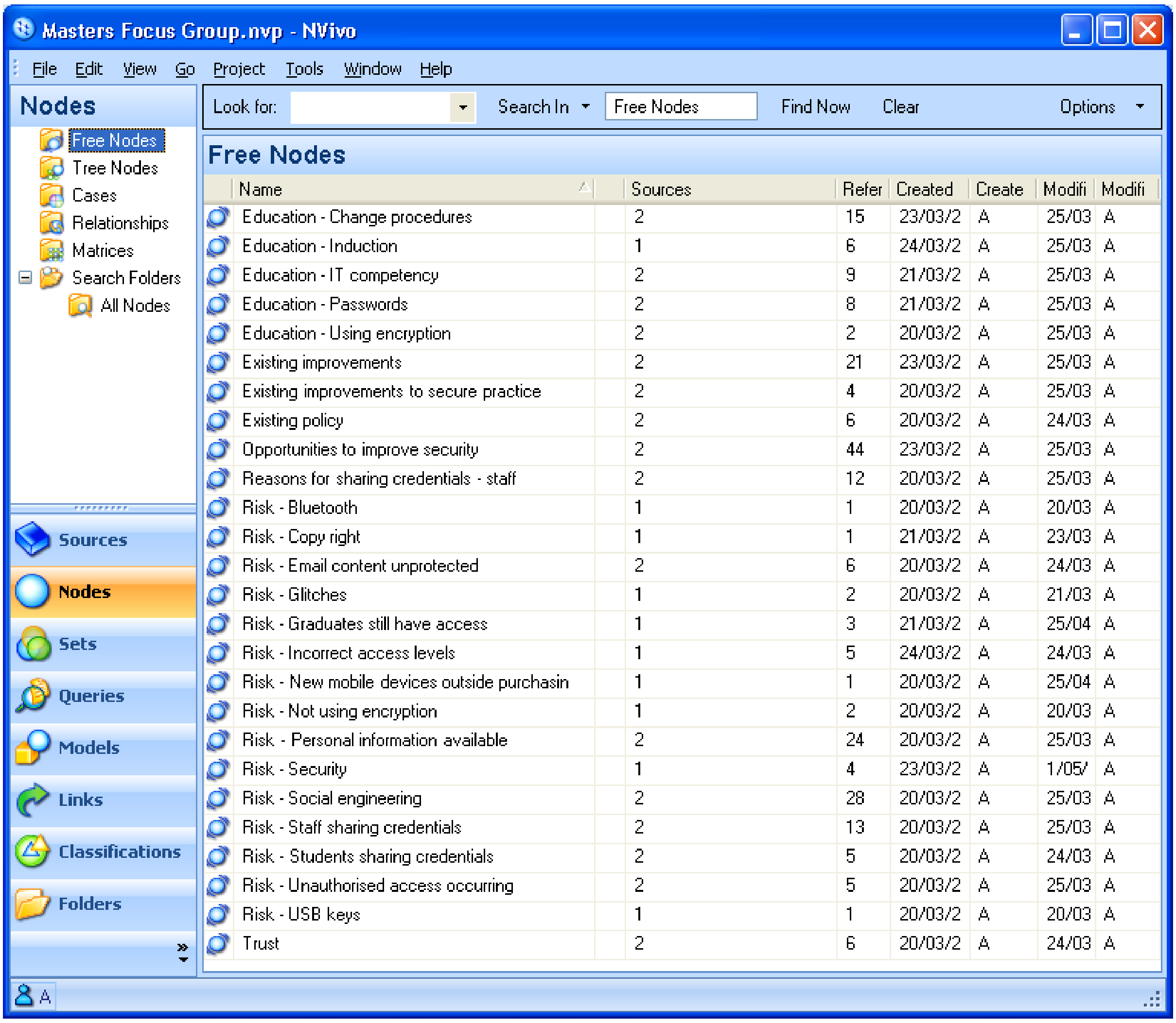
6.6 Combined analysis

The salient features of the Leximancer analysis for the first focus group are the theme ‘people’ , ‘credentials’, ‘password’ , ‘systems’, and ‘information’, while for the second focus group the themes are ‘student’, ‘information’, ‘system’, ‘looking’, and ‘induction’.

In focus group one the relationship between the themes have ‘people’ at its centre, with ‘credentials’ and ‘password’ overlapping either side (see Figure 14), and ‘system’ connected to ‘people’, while ‘information’ is further removed from ‘people’ with the concept ‘data’ at the furthest part of the circle away from ‘people’.

In focus group two the relationship between the themes show ‘student’ at its centre, with ‘information’ at some distance from ‘student’ and with ‘system’ overlapping with ‘student’. While ‘looking’ is connected to ‘information’, the theme ‘induction’ is a small distance off ‘student’.

The salient features of the NVivo coding process for both focus groups are 44 references to ‘Opportunities to improve security’; 28 references to ‘Risk – Social engineering’; 24 references to Risk – Personal information available’; 21 references to ‘Existing Improvements’; and, lastly, 15 references to ‘Education – Change procedures’.



Free Nodes

Name	Sources	Refer	Created	Create	Modifi	Modifi
Education - Change procedures	2	15	23/03/2	A	25/03	A
Education - Induction	1	6	24/03/2	A	25/03	A
Education - IT competency	2	9	21/03/2	A	25/03	A
Education - Passwords	2	8	21/03/2	A	25/03	A
Education - Using encryption	2	2	20/03/2	A	25/03	A
Existing improvements	2	21	23/03/2	A	25/03	A
Existing improvements to secure practice	2	4	20/03/2	A	25/03	A
Existing policy	2	6	20/03/2	A	24/03	A
Opportunities to improve security	2	44	23/03/2	A	25/03	A
Reasons for sharing credentials - staff	2	12	20/03/2	A	25/03	A
Risk - Bluetooth	1	1	20/03/2	A	20/03	A
Risk - Copy right	1	1	21/03/2	A	23/03	A
Risk - Email content unprotected	2	6	20/03/2	A	24/03	A
Risk - Glitches	1	2	20/03/2	A	21/03	A
Risk - Graduates still have access	1	3	21/03/2	A	25/04	A
Risk - Incorrect access levels	1	5	24/03/2	A	24/03	A
Risk - New mobile devices outside purchasin	1	1	20/03/2	A	25/04	A
Risk - Not using encryption	1	2	20/03/2	A	20/03	A
Risk - Personal information available	2	24	20/03/2	A	25/03	A
Risk - Security	1	4	23/03/2	A	1/05/	A
Risk - Social engineering	2	28	20/03/2	A	25/03	A
Risk - Staff sharing credentials	2	13	20/03/2	A	25/03	A
Risk - Students sharing credentials	2	5	20/03/2	A	24/03	A
Risk - Unauthorised access occurring	2	5	20/03/2	A	25/03	A
Risk - USB keys	1	1	20/03/2	A	20/03	A
Trust	2	6	20/03/2	A	24/03	A

Figure 18: NVivo - Free nodes for both focus groups

As Table 7 shows, the concept ‘information’ is covered in all focus groups and detected by analysis using Leximancer and NVivo. The concepts ‘credentials’ and ‘password’ came through strongly from the first focus group in Leximancer, and were confirmed by NVivo for both focus groups. In comparison, for the second focus group, Leximancer and NVivo show the concepts ‘student’ and ‘induction’ to be predominant.

Table 7: Combined concepts

Concept	Literature	Research question and propositions	Leximancer 3.5		NVivo 8	
			FG1	FG2	FG1	FG2
people			✓			
credentials			✓		✓	✓
password			✓		✓	✓
information			✓	✓	✓	✓
data			✓			
student				✓		✓
induction				✓		✓
system				✓		
looking				✓		
security awareness	✓	✓				
unauthorised access	✓	✓			✓	✓
policies and procedures	✓				✓	✓
education	✓	✓			✓	
social engineering	✓	✓			✓	✓

It is noted that during the data analysis, the computer of the researcher crashed. The consequence of this crash was that all software had to be reimaged on this computer. Following the reimaging, some of the software used for this dissertation generated errors that could not be explained or reproduced.

6.7 Chapter Summary

This chapter described the data analysis adopted for this research. It commenced with outlining the validity affecting this qualitative research during the data analysis process. It lists the concepts as they relate to the literature, and recaptures the research question and its propositions in preparation for the data analysis. For each focus group, Leximancer 3.5 was used first to obtain an unbiased result. This was followed up by the researcher using NVivo 8 to manually code the transcription. The combined analysis shows the concepts that were covered by the focus groups. The next chapter will discuss the findings of this data analysis.

7 Discussion, limitations, future research and conclusion

This chapter will discuss the results of the qualitative data analysis, followed by an outline of the limitations of this research. A list of opportunities for future research is provided and the chapter closes with the conclusion.

7.1 Discussion

The chapters leading up to this discussion have provided an insight into the literature that is the foundation of this research. This has led to the research question and model for this study which addresses some of the questions posited by previous research. This research aims to address the research question through qualitative data analysis. While the data provides a rich source, this discussion highlights the most relevant factors in answer to the research question. It is also noted that the researcher has excluded certain material from being discussed to prevent sensitive information from the focus groups being published.

Table 8 shows the concepts derived from the literature that lead to the research question, as well as the findings of the data analysis using Leximancer 3.5 and NVivo 8. The discussion of the concepts from Table 8 will be guided by the literature concepts. In regard to security awareness, the data analysis shows that the major concern expressed by all participants in relation to social engineering was the sharing of 'credentials' by staff and students. Previous studies by Choi et al. (2008), Manjak (2006) and Workman (2008) highlighted security awareness as an important aspect in the process of changing employees' habits and organisational procedures. The data analysis also highlighted a disconnection between access to a system and access to data. Participants seemed to focus on concerns about credentials being shared, but there was no clear link in their discussion about subsequent access to the data and the impact of this unauthorised access.

Table 8: Refined combined concepts

Literature concepts	**Research question and propositions**	**Leximancer 3.5**		**NVivo 8**	
		FG1	**FG2**	**FG1**	**FG2**
security awareness	✓	credentials		Existing improvements	✓
				Existing improvements to secure practice	✓
				Risk – Unauthorised access occurring	✓
unauthorised access	✓	people	student	Risk - Copyright	
		credentials		Risk – Unauthorised access occurring	✓
		password		Risk – Staff sharing credentials	
				Risk – Students sharing credentials	
policies and procedures		credentials		Existing policy	✓
		systems		Opportunities to improve security	✓
				Reasons for sharing credentials - staff	✓
education	✓	credentials	induction	Education – Change procedures	✓
		password			Education – Induction
		systems		Education – IT competency	✓
		Information and data		Education – Passwords	✓
				Education – Using encryption	✓
social engineering	✓	credentials		Risk – Bluetooth	
		password		Risk – Email content unprotected	✓
				Risk – Glitches	
				Risk – Graduates still have access	
					Risk – Incorrect access levels
				Risk – New mobile devices outside purchasing cycle	
				Risk – Not using encryption	
				Risk – Personal information available	
				Risk – Security	
				Risk – Social engineering	✓
				Risk – Staff sharing credentials	✓
				Risk – Students sharing credentials	✓
				Risk – Unauthorised access occurring	✓
				Risk – USB keys	
				Trust	✓

However, some of the participants were proactive in finding more secure ways to handle sensitive information. In addition, some corporate applications provide a platform of communication that is protective of staff details. Additionally, the staff search facility of the university's web site has been changed to further secure staff details. In other sections, participants have proactively created a database to resolve some of the issues encountered in an attempt to reduce sharing credentials to be able to do the work required of them. These proactive steps taken by employees are not driven by current management policies and procedures. Rather, they are initiated by staff in an attempt to improve practice and, already, these initiatives are starting to impact on subsequent policy and procedure. This is somewhat contrary to the research literature reviewed in this study. There appears to be little attention to this important aspect in existing literature, and therefore this could be regarded as a new contribution to the literature.

In regard to unauthorised access, credentials are the key to gaining access to an information system, which then allows access to the data. However, the data analysis highlighted that sharing credentials or passwords is seen a way to gain access to the Internet – by students – and being able to do one's job – by staff. Previous research by Nasheri (2003), Smith and Rupp (2002), and Walden (2005) highlighted that unauthorised access occurs when someone gains access to a computer system without having been given permission to do so. The data analysis shows a number of potential situations for sharing credentials. One concern was in regard to providing credentials to IT staff when a computer is refreshed. The implication of this is that staff members are not provided with a resetting password procedure when they receive their refreshed computer back. The data analysis also highlights that some of the processes do not include secure practices. One example of this is where sensitive hard copies are making their way through the manual internal delivery process. Another is where personal student details are visible to other students when groups are set up for course requirements. In general, the participants seem to focus more on security, access to systems, and credentials, rather than security of data or access to data. Social engineering is all concerned with disclosing information in a social environment (Mitnick & Simon 2002). It appears from the data that there is a disconnection between access to systems and access to data. Very little awareness about social engineering techniques in relation to a hacker came through in the group discussions, even though the participants discussed issues that create potential situations for social engineering.

In regard to policies and procedures, the data analysis highlighted that existing policies are currently causing staff to share credentials. This is supported by Emanavin (2004) who discussed the need to support policies and procedures on security measures as an ongoing requirement. This is reinforced by Choi et al. (2008), positing that it is essential to increase management's security awareness by keeping them informed about the consequences of security breaches. The increased security awareness may then result in change in procedures and policies. This change also has the potential to affect human behaviour as employees adopt the new practices (Choi et al. 2008).

In regard to education, the data analysis shows that participants believe a better induction process, as well as improved IT competency training, would address the issue of sharing credentials. This became particularly clear when participants noted that the induction and other training courses, currently conducted online, may create a weakness in understanding the norm of the USQ, as well as missing other vital communication by other staff completing these training sessions. This is supported by Barrett (2003) and Mitnick and Simon (2002), who identified education and training as strategies to reduce the success rate of social engineering.

In regard to social engineering the data analysis has highlighted a number of issues. These include the situation of contractors gaining physical access without being challenged, the lack of understanding of compromises and breaches occurring to overcome bureaucracy and slow processing, as well as perceived trust by staff and students when sharing credentials. Previous research has shown that these are social engineering situations used by hackers to obtain information or access (Mitnick & Simon 2002; Workman 2007, 2008).

In summary, to answer the research question, this research has shown that there are a number of situation that create potential security risks of unauthorised access. While there is some security awareness among the participants of the focus groups, their responses and elaborations highlight the fragmentation of work flowing through the organisation that is creating potential security risks. All staff members would benefit from security awareness education to address the current lack of policies and procedures that are currently causing these scenarios.

7.2 Limitations

One of the limitations of this research is that the data collection occurred only at the USQ. The study aimed to establish an understanding of one university first and then research could be expanded to other universities, and, ideally, to any organisation.

Furthermore, the study is also limited in that no prior screening of participants occurred. This screening could have identified a participant's level of security awareness. Also, there was no selection process for ICT participants as they were directly nominated by the CTO. This nomination limited the pool of ICT participants, and may have impacted on the focus group discussions.

In addition, this research focuses purely on qualitative research methods. This means that the result of the data analysis cannot be generalised. It also limits the outcome of the research to be subjective. This also means that this research does not provide quantitative analysis results.

Another limitation relates to timing. The USQ is undergoing the final stages of restructuring. Many of the current issues highlighted by the participants are in relation to the changes that occurred due to the restructuring process. At any other time, potentially, participants may have focused on other issues related to social engineering.

7.3 Future research

The data analysis highlighted an activity which the literature currently appears to have paid little attention to, in that participants who are currently working with sensitive data are proactively applying increased security into their processing and are also proactively seeking advice on legal and privacy issues. These are employees on the operational level and, without being guided by policies and procedures, they have a certain level of security awareness which they have addressed. Some of them are already in the process of changing policies and procedures where they can. This could lead into research comparing the security awareness levels in operational staff compared to security awareness levels in management. Additionally, this would also provide an opportunity to test the model - shown in chapter 3 – and its flexibility in regard to the cycle of updating procedures and policies from both management and operational viewpoints. This research opportunity could then further address the potential reduction in unauthorised access through social engineering.

Future research could also address the issue of focus group participants being screened before participating, in accordance to their understanding of social engineering. This would provide a better understanding in regard to their responses, and may provide more detailed insights about their security awareness. This could be followed up with quantitative research focusing on analysis of the more detailed qualitative findings.

In addition, future research could target the focus groups specifically at operational and management levels to determine if there are any differences in security awareness. This may lead to a better understanding of how security awareness could be increased in management to produce enhanced policies and procedures needed at the operational level.

As this study has focused only on some sections of the university, future research could address all areas of the university. This could have the potential to provide other universities and organisations with a method to determine their organisations security awareness and allow Human Resources to apply more flexible security awareness training sessions.

The combination of these recommendations may also result in Human Resources providing targeted training. In addition to existing training, Human Resources could then create very specific short sessions targeting a specific problem. For example, IT competency in employees varies according to their prior experience. Currently, it is assumed by employees that security is implemented by the experts, and the experts' expectation is that employees have secure practices. However, some of that knowledge may not have been communicated clearly in the past. Addressing very specific issues with short training sessions could have the potential to eliminate weak areas and increase overall security.

Future research could also consider clarifying what employees understand as the difference between accessing the information systems, the Internet, and corporate applications compared to accessing data.

Future research may also have the potential to produce different results. The USQ has recently undergone restructuring, and some of the issues discussed by participants are the result of this restructure. The results may vary sometime in the future as the passage of time would allow processes to be adjusted and provide a different set of issues for the participants to discuss.

Future research could consider targeting qualitative data collection towards different methods of grouping participants. For example, some of the focus groups could consist purely of academic and professional staff, with a mixed group as a control group. Academic staff members deal with different processes and have different work requirements.

Furthermore, considering the model developed for this research, opportunities exists to research the expectancy theory, to determine the combined impact of expectancy theory and social engineering, and to determine the potential of the procedures manual.

Lastly, this research has shown that there is potential for enhanced practices to increase security awareness at the operational level as well as management level, which is in line with the intention of the model.

7.4 Conclusion

The issues highlighted in this research provide some insight for the university to improve certain procedures and policies in light of increased security requirements. A number of issues highlighted in this research could be addressed by additional training. Human Resources could provide spot-training that would allow them to address a particular issue, without having to run a full training session on security or IT competency. Some of these issues could also feed into existing training to provide more depth. The research may also assist in reconsidering existing online training programs to determine how they could be enriched. This spot-training would allow Human Resources to target new and existing staff members alike. Particularly, there is a call for better induction training for staff.

The university would also benefit from a re-engineering process, whereby existing processes are analysed and improved to fit into the current structure. This has the potential to address some of the issues where knowledge has been lost when people moved to other sections. It would also provide a better understanding of the business requirements of different sections of the university. Reengineering has the potential to make existing processes more effective and result in faster response times. Increasing the understanding of other employees' work requirements also has the potential to create a better working community, as reengineering tends to draw in people from different sections to assist in the analysis.

7.5 Summary

This chapter has provided a discussion of the data analysis, which addressed the more relevant issues in relation to social engineering. Limitations on the scope on this research have been fully detailed and include the fact that this study has focused solely on the USQ staff members and students. It is also limited to qualitative analysis without the richness that quantitative analysis provides. Future recommendations for research provide a wide variety of issues to investigate.

8 References

Alanazi, HO, Noor, RM, Zaidan, BB & Zaidan, AA 2010, 'Intrusion Detection System: Overview', *Journal of Computing*, vol. 2, no. 2, pp. 130-3.

Anastasi, A & Urbina, S 1997, *Psychological Testing*, 7th edn, Prentice Hall, New Jersey.

Anonymous 2001, *Maximum Security*, 3rd edn, SAMS, Indianapolis, Indiana.

Barrett, N 2003, 'Penetration testing and social engineering: hacking the weakest link', *Information Security Technical Report*, vol. 8, no. 4, pp. 56-64.

Basit, TN 2003, 'Manual or electronic? The role of coding in qualitative data analysis', *Educational Research*, vol. 45, no. 2, pp. 143-54.

Baskerville 2003, 'A Possibility Theory Framework for Security Evaluation in National Infrastructure Protection', *Journal of Database Management*, vol. 14, no. 2, pp. 1-13.

Beattie, V, McInnes, W & Fernley, S 2004, 'A methodology for analysing and evaluating narratives in annual reports: a comprehensive descriptive profile and metrics for disclosure quality attributes', *Accounting Forum*, vol. 28, no. 3, pp. 205-36.

Beebe, NL & Rao, VS 2005, 'Using Situational Crime Prevention Theory to Explain the Effectiveness of Information Systems Security', paper presented to 2005 SoftWars Conference, San Antonio.

Blackburn, R 1993, *The Psychology of Criminal Conduct: Theory, Research and Practice*, John Wiley & Sons, Chichester.

Blake, T 2008, 'Leximancer Concept Miner', viewed 18 March 2011, <https://www.leximancer.com/site-media/lm/science/leximancer-concept-miner.pdf>.

Botha, M & von Solms, R 2001, 'The utilization of trend analysis in the effective monitoring of information security. Part 1: the concept', *Information Management & Computer Security*, vol. 9, no. 5, pp. 237-42.

Botta, D, Werlinter, R, Gagné, A, Iverson, L, Fels, S & Fisher, B 2007, 'Towards understanding IT security professionals and their tools', paper presented to Proceedings of the 3rd symposium on Usable privacy and security, Pittsburgh, Pennsylvania.

Breen, RL 2006, 'A Practical Guide to Focus-Group Research', *Journal of Geography in Higher Education*, vol. 30, no. 3, pp. 463 - 75, viewed August 06, 2010.

Çakanyildirim, M & Yue, WT 2007, 'Intrusion Prevention in Information Systems: Reactive and Proactive Responses', *Journal of Management Information Systems*, vol. 24, no. 1, pp. 329-53.

Çakanyildirim, M, Yue, WT & Ryu, YU 2009, 'The management of intrusion detection: Configuration, inspection, and investment', *European Journal of Operational Research*, vol. 195, no. 1, pp. 186-204.

Chantler, N 1995, 'The Profile of the computer hacker', Curtin University of Technology.

Choi, N, Kim, JD & Goo, J 2006, *Managerial Information Security Awareness' Impact on an Organization's Information Security Performance*, Association for Information Systems AIS Electronic Library (AISeL).

Choi, N, Kim, D, Goo, J & Whitmore, A 2008, 'Knowing is doing: An empirical validation of the relationship between managerial information security awareness and action', *Journal of Information Management & Computer Security*, vol. 16, no. 5, pp. 484-501.

Clark, JD & Themudo, NS 2006, 'Linking the Web and the Street: Internet-Based "Dotcauses" and the "Anti-Globalization" Movement', *World Development*, vol. 34, no. 1, pp. 50-74.

Creswell, JW 2009, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*, 3rd edn, SAGE, Los Angeles.

Denning, DE 2011, Cyber Conflict as an emergent social phenomenon, *IGI Global*, pp.170-171.

Doctor, B 2004, 'Intrusion Detection vs. Intrusion Prevention: The difference and what you need to know', *StillSecure*.

Dolan, A 2004, 'Social Engineering', *SANS Reading Room*, viewed 30 October 2009, <http://www.sans.org/reading_room/whitepapers/engineering/social-engineering_1365>.

Drennan, P 2007, 'Ethnography of Play in a Massively Multi-Player Online Role Playing Game: Marketplaces, Team Work and Free Play', University of Southern Queensland.

Dubé, L & Paré, G 2003, 'Rigor in Information Systems Positivist Case Research: Current Practices, Trends, and Recommendations', *MIS Quarterly*, vol. 27, no. 4, pp. 597-635.

Elson, D 2004, 'Engendering Government Budgets in the Context of Globalization(s)', *International Feminist Journal of Politics*, vol. 6, no. 4, pp. 623-42.

Emanavin, CC 2004, 'Testing Lessig: Applying User Acceptance Theory to Internet Use and Behavior for Privacy and Security Applications', Georgetown University.

Eysenbach, G & Köhler, C 2002, 'How do consumers search and appraise health information on the world wide web? Qualitative study using focus groups, usability tests, and in-depth interviews', *BMJ*, vol. 324.

Farid, DM & Rahman, MZ 2010, 'Anomaly Network Intrusion Detection Based on Improved Self Adaptive Bayesian Algorithm', *Journal of Computers*, vol. 5, no. 1, pp. 23-31.

Fitzgerald, J & Dennis, A 2009, *Business Data Communications and Networks*, 10 edn, John Wiley & Sons, Inc, Chennai, India.

Fötinger, CS & Ziegler, W 2004, 'Understanding a hacker's mind - A psychological insight into the hijacking of identities', viewed 10 April 2009, <http://www.donau-uni.ac.at/>.

George, JF, Biros, DP, Burgoon, JK & Nunamaker, JF 2003, 'Training Professionals to Detect Deception', *Springer-Verlag Berlin*, pp. 366-70.

Gibbs, J, Kraemer, KL & Dedrick, J 2003, 'Environment and Policy Factors Shaping Global E-Commerce Diffusion: A Cross-Country Comparison', *Information Society*, vol. 19, no. 1, p. 5.

Gurd, B & Palmer, P 2010, 'Exploring Accountability Relationships in the NFP Sector', paper presented to APIRA 2010 - Asia Pacific Interdisciplinary Research in Accounting, Sydney.

Hannes, K, Lockwood, C & Pearson, A 2010, 'A Comparative Analysis of Three Online Appraisal Instruments' Ability to Assess Validity in Qualitative Research', *Qualitative Health Research*, vol. 20, no. 12, pp. 1736-43.

Harris, S, Harper, A, Eagle, C, Ness, J & Lester, M 2005, *Gray Hat Hacking*, McGraw-Hill/Osborne, New York.

Hesse-Biber, SN & Leavy, P 2006, *Emergent Methods in Social Research*, SAGE Publishers, Thousand Oaks.

Hevner, AR, March, ST, Park, J & Ram, S 2004, 'Design Science in Information Systems Research', *Management Information Systems Quarterly*.

Indulska, M & Recker, J 2008, '13. Design science in IS research: a literature analysis', in *Information Systems Foundations: The Role of Design Science*, Internet WWW page, at URL: <http://epress.anu.edu.au/apps/bookworm/view/Information+Systems+Foundations%3A+The+Role+of+Design+Science/2271/upfront.xhtml>.

Jacobsson, A 2008, 'Privacy and Security in Internet-based Information Systems', Blekinge Institute of Technology.

Keeney, M, Kowalski, E, Cappelli, D, Moore, A, Shimeall, T & Rogers, S 2005, 'Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors', *United States Secret Service*.

Keneey, M, Kowalski, E, Cappelli, D, Moore, A, Shimeall, T & Rogers, S 2005, 'Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors', *United States Secret Service*.

Kerr, OS 2003, 'Cybercrime's Scope: Interpreting "Access" and "Authorization" in computer misuse statutes', *New York University Law Review*, vol. 78, no. 5, pp. 1596-668.

Kjaerland, M 2005, 'A classification of computer security incidents based on reported attack data', *Journal of Investigative Psychology and Offender Profiling*, vol. 2, no. 2, pp. 105-20.

Kleen, LJ 2001, 'Malicious hackers: a framework for analysis and case study.', Operations Research thesis, Air Force Institute of Technology.

Kollmann, T, Kuckertz, A & Breugst, N 2009, 'Organizational Readiness and the Adoption of Electronic Business - The Moderating Role of National Culture in 29 European Countries', *The DATA BASE for Advances in Information Systems*, vol. 40, no. 4, pp. 117-31.

Krueger, RA & Casey, MA 2000, *Focus groups a practical guide for applied research*, 3rd edn, Thousand Oaks Sage Publications.

Kumagai, F 2001, 'Possibilities for Using the Internet in Japanese Education in the Information Age Society', *International Journal of Japanese Sociology*, vol. 10, no. 1, pp. 29-44.

Kvedar, D, Nettis, M & Fulton, SP 2010, *The use of formal social engineering techniques to identify weaknesses during a computer vulnerability competition*, Rocky Mountains.

Kwai-Sang, C, Guijiang, D & Xiaoqing, T 2006, 'A computer-integrated framework for global quality chain management', *International Journal of Advanced Manufacturing Technology*, vol. 27, no. 5/6, pp. 547-60.

Lawlor, B & Vu, L, *A Survey of Techniques for Security Architecture Analysis,* 2003, ISL Information Networks Division, DSTO Information Sciences Laboratory.

Lee, AS & Baskerville, RL 2003, 'Generalizing Generalizability in Information Systems Research', *Information Systems Research*, vol. 14, no. 3, pp. 221-43.

Leedy, PD & Ormrod, JE 2005, *Practical research planning and design*, 8th edn, Pearson Merrill Prentice Hall, New Jersey.

Leeson, PT & Coyne, CJ 2006, 'The Economics of Computer Hacking', *Journal of Law, Economics and Policy*.

Levy, M & Powell, P 2000, 'Information systems strategy for small and medium sized enterprises: an organisational perspective', *Journal of Strategic Information Systems*, vol. 2000, no. 9, pp. 63-84.

Leximancer 2005, 'Leximancer Manual Version 2.2', viewed 18 March 2011, <https://www.leximancer.com/wiki/images/7/77/Leximancer_V2_Manual.pdf>.

Loveland, G & Lobel, M 2009, *Trial by Fire*, PriceWaterhouseCoopers LLP.

Manjak, M 2006, 'Social Engineering Your Employees to Information Security', *SANS Institute Reading Room*.

Mann, I 2008, *Hacking the Human*, Gower House, Hampshire.

Martin, NJ & Rice, JL 2007, 'Profiling Enterprise Risks in Large Computer Companies Using the Leximancer Software Tool', *Risk Management*, vol. 2007, no. 9, pp. 188-206.

Mauch, JE & Park, N 2003, *Guide to the Successful Thesis and Dissertation - A Handbook for Students and Faculty*, 5th edn, Marcel Dekker, Inc., New York.

Maurushat, A & Yu, R 2009, 'When Internet protocols and legal provisions collide: Unauthorised access and Sierra v. Ritz', *Computer Law & Security Review*, vol. 2009, no. 25, pp. 185-8.

Mitnick, KD & Simon, WL 2002, *The Art of Deception: Controlling the Human Element of Security*, Wiley & Sons, Indianapolis.

---- 2006, *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers*, Wiley Publishing.

Morgan, DL 1988, *Focus groups as qualitative research*, vol. 16, Portland State University Portland.

Nasheri, H 2003, 'The Intersection of Technology Crimes and Cyberspace in Europe: The Case of Hungary', *Information & Communications Technology Law*, vol. 12, no. 1, pp. 25-48.

Oates, B 2001, 'Cyber Crime: How Technology Makes it Easy and What to Do About It', *Journal of Law, Investigations, and Ethics*, pp. 45-50.

Palmer, CC 2001, 'Ethical Hacking', *IBM Systems Journal*, vol. 40, no. 3, pp. 769-80.
Parker, DB 2007, Risks of Risk-Based Security, Communications of the AC, vol. 50, no. 3, pp. 119-120.

Pearce, R 2006, 'Globalization and development: an international business strategy approach', *TGransnational Corporations*, vol. 15, no. 1.

Pleskonjic, D, Milutinovic, V, Macek, N, Djordjevic, B & Caric, M 2006, 'Psychological Profile of Network Intruder', paper presented to IPSI, Amalfi, Italy, 23-26 March 2006.

Potter, C & Beard, A 2010, *Information Security Breaches Survey 2010*, infosecurity Europe and PriceWaterhouseCoopers, .

Punch, KF 2006, *Developing effective research proposals*, 2nd edn, SAGE Publications, London.

Ragsdale, DJ, Carver, CA, Humphries, JW & Pooch, UW 'Adaption Techniques for Intrusion Detection and Intrusion Response Systems', *IEEE*.

Raju, RN 2005, 'State-of-the-art Intrusion Detection: Technologies, Challenges, and Evaluation', Linkoping University.

Redoli, J, Mompo´, R, Garcı´a-Dı´ez, J & Lo´ pez-Coronado, M 2008, 'A model for the assessment and development of Internet-based information and communication services in small and medium enterprises', *Technovation*, vol. 2008, no. 28, pp. 424-3.

Roberts, P & Webber, J 2002, 'Virtuous Hackers: developing ethical sensitivity in a community of practice', *Australasian Journal of Information Systems*, vol. 9, no. 2, pp. 172-7.

Rodrigues, VS, Piecyk, M, Potter, A, McKinnon, A, Naim, M & Edwards, J 2010, 'Assessing the application of focus groups as a method for collecting data in logistics', *International Journal of Logistics Research and Applications: A Leading Journal of Supply Chain Management*, vol. 13, no. 1, pp. 75 - 94, viewed August 06, 2010.

Rogers, MK 1999, 'Psychology of hackers: Steps toward a new taxonomy'.

---- 2000, *Theories of Crime and Hacking*, Center for Education and Research In Information Assurance and Security (CERIAS) Psychology and Computer Crime, Purdue University, <http://www.cerias.purdue.edu/>.

---- 2006, 'A two-dimensional circumplex approach to the development of a hacker taxonomy', *Digital Investigation*, vol. 3, no. 2, pp. 97-102, viewed 26 March 2009.

Rogers, MK, Seigfried, K & Tidke, K 2006, 'Self-reported computer criminal behaviour: A psychological analysis', *Journal of Digital Investigation*, pp. 116-20.

Ruane, JM 2008, *Essentials of Research Methods - A Guide to Social Science Research*, Blackwell Publishing, Oxford.

Sassen, S 2003, 'Globalization or denationalization?', *Review of International Political Economy*, vol. 10, no. 1, pp. 1 - 22, viewed September 27, 2008.

Scarfone, K & Mell, P, *Guide to Intrusion Detection and Prevention Systems (IDPS),* 2007, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg.

Silverman, D 2005, *Doing Qualitative Research*, 2nd edn, SAGE Publications, London.

Sirkemaa, S 2006, 'Information technology in developing a meta-learning environment', *European Journal of Open, Distance and E-Learning*, viewed 31 March 2011.

Smith, AD 2004a, 'Cybercriminal impacts on online business and consumer confidence', *Online Information Review*, vol. 28, no. 3, pp. 224-34.

---- 2004b, 'E-security issues and policy development in an information-sharing and networked environment', *Aslib Proceedings*, vol. 56, no. 5, pp. 272-85.

Smith, AD & Rupp, WT 2002, 'Issues in cybersecurity: understanding the potential risks associated with hackers/crackers', *Information Management & Computer Security*, vol. 10, no. 4, pp. 178-83.

Stanković, S & Simić, D 2010, 'A Holistic Approach to Securing Web Applications', *Journal of Computing*, vol. 2, no. 1, pp. 16-20.

Statistics Solutions 2011a, *The Focus Group*, viewed 29 March 2011, <www.statisticssolutions.com/dissertaton-resources/conducting-qualitative-research/the-focus-group>.

---- 2011b, *Validity in Qualitative Research*, viewed 29 March 2011, <www.statisticssolutions.com/dissertaton-resources/conducting-qualitative-research/validity-in-qualitative-research>.

Stoneburner, G, Goguen, A & Feringa, A, 2002.

Tashakkori, A & Teddlie, C 2003, *Handbook of Mixed Methods in Social & Beharioral Research*, SAGE Publications, Thousand Oaks.

Thonnard, O & Dacier, M 2008, 'A framework for attack patterns' discovery in honeynet data', *Journal of Digital Investigation*, vol. 2008, no. 5, pp. 128-39.

Tiller, JS 2005, *The Ethical Hack: A Framework for Business Value Penetration Testing*, Auserback Publications.

Trim, PRJ 2005, 'Managing computer security issues: preventing and limiting future threats and disasters', *Disaster Prevention and Management*, vol. 14, no. 4, pp. 493-505.

Trochim, WMK 2006, *The Research Methods Knowledge Base*, 2nd edn, Internet WWW page, at URL: <http://www.socialresearchmethods.net/kb/> (version current as of October 20, 2006).

Tryfonas, T, Kiountouzis, E & Poulymenakou, A 2001, 'Embedding security practices in contemporary information systems development approaches', *Journal of Information Management & Computer Security*, vol. 9, no. 4, pp. 183-97.

University of Queensland *What is Leximancer?*, viewed 4 January 2011, <http://www.leximancer.com>.

---- *About Leximancer*, viewed 4 January 2011, <https://www.leximancer.com/company/>.

---- 2005, 'Leximancer Manual Version 2.2', <https://www.leximancer.com/wiki/images/7/77/Leximancer_V2_Manual.pdf>.

---- 2010a, 'Leximancer White Paper', <https://www.leximancer.com/lmedia/Leximancer_White_Paper_2010.pdf>.

---- 2010b, *ARC Key Centre for Human Factors and Applied Cognitive Psychology*, <http://www.humanfactors.uq.edu.au>.

---- 2010c, *Leximancer Manual v3*, viewed 13 December 2010, <https://www.leximancer.com/ >.

University of Texas, A 2010, *Instructional Assessment Resources*, viewed 12 January 2011, <http://www.utexas.edu/academic/ctl/assessment/iar/glossary.php>.

Vadera, S, Potter, C & Beard, A 2008, *2008 Information Security Breaches Survey*, Department for Business Enterprise & Regulatory Reform.

Van Beveren, J 2001, 'A conceptual model of hacker development and motivations', *Journal of E-Business*, vol. 1, no. 2, pp. 1-9.

Vandenwauver, M, Claessens, J, Moreay, W, Vaduva, C & Maier, R 1999, *Why Enterprises Need More than Firewalls and Intrusion Detection Systems*, IEEE, Stanford, California.

Volonino, L & Robinson, SR 2004, *Principles and Practice of Information Security: Protecting Computers from Hackers and Lawyers*, Pearson Prentice Hall, New Jersey.

Walden, I 2005, 'Crime and Security in Cyberspace', *Cambridge Review of Internal Affairs*, vol. 18, no. 1, pp. 51-68.

Warren, MJ 2002, 'Security Practice: survey evidence from three countries', *Logistics Information Management*, vol. 15, no. 5/6, pp. 347-51.

Warren, M & Leitch, S 2009, ‘Hacker taggers: a new type of hackers’, *Information systems frontiers*, Online First, pp. 1-7.

Watson, M, Smith, A & Watter, S 2005, 'Leximancer Concept Mapping of Patient Case Studies', in R Khosla, RJ Howlett & LC Jain (eds), *Knowledge-Based Intelligent Information and Engineering Systems*, Springer Berlin / Heidelberg, vol. 3683, pp. 1232-8.

Weber, R 2004, 'The Rhetoric of Positivism Versus Interpretivism: A Personal View', *MIS Quarterly*, vol. 28, no. 1, pp. iii-xii.

Weber, RP 1990, *Quantitative Applications in the Social Sciences*, Basic Content Analysis, Sage, Newbury Park, California. viewed 12 January 2011, <http://www.netlibrary.com.ezproxy.usq.edu.au/Details.asp>.

Werlinger, R, Hawkey, K, Muldner, K, Jaferian, P & Beznosov, K 2008, 'The Challenges of Using an Intrusion Detection System: Is It Worth the Effort?', paper presented to Symposium On Usable Privacy and Security (SOUPS), Pittsburgh, Pennsylvania, 23-25 July 2008.

Whitman, ME & Mattord, HJ 2008, *Management of Information Security*, 2nd edn, Course Technology Cengage Learning, Boston.

Wikipedia *Positivism*, viewed 13 July 2010, <http://en.wikipedia.org/wiki/Positivism>.

Wilson, Z 2001, *Hacking: The Basics*, SANS, viewed 19 April 2009, <http://www.sans.org/reading_room>.

Wong, L 2008, 'Data Analysis in Qualitative research: A brief guide to using NVivo', *Malaysian Family Physician*, vol. 3, no. 14-20.

Workman, M 2007, 'Gaining Access with Social Engineering: An Empirical Study of the Threat', *Information Security Journal: A Global Perspective*, vol. 16, no. 6, pp. 315-31.

---- 2008, 'A test of interventions for security threats from social engineering', *Information Management & Computer Security*, vol. 16, no. 5, pp. 463-83.

Workman, M & Gathegi, J 2006, 'Punishment and ethics deterrents: A study of insider security contravention', *Journal of the American Society for Information Science and Technology*, vol. 58, no. 2, pp. 212-22, item: .

---- 2007, 'Punishment and ethics deterrents: A study of insider security contravention', *Journal of the American Society for Information Science and Technology*, vol. 58, no. 2, pp. 212-22.

Workman, M, Bommer, WH & Straub, D 2008, 'Security lapses and the omission of information security measures: A threat control model and empirical test', *Computers in Human Behavior*, vol. 24, no. 6, pp. 2799-816.

Yu, J, Reddy, YVR, Selliah, S, Reddy, S, Bharadwaj, V & Kankanahalli, S 2005, 'TRINETR: An architecture for collaborative intrusion detection and knowledge-based alert evaluation', *Journal of Advanced Engineering Informatics*, vol. 2005, no. 19, pp. 93-101.

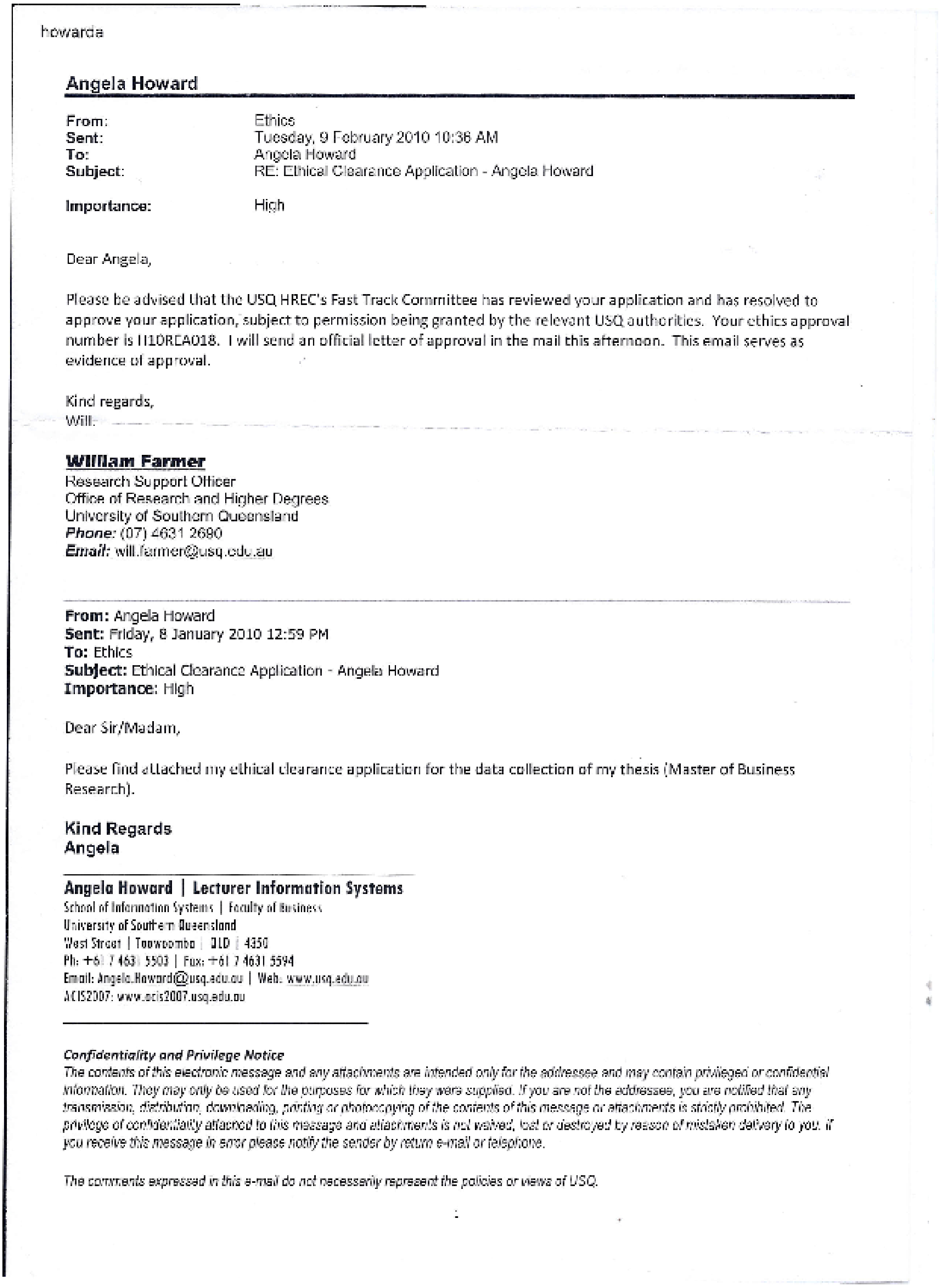
Yue, WT & Çakanyildirim, M 2007, 'Intrusion Prevention in Information Systems: Reactive and Proactive Responses', *Journal of Management Information Systems*, vol. 24, no. 1, pp. 329-53.

Zhou, CV, Leckie, C & Karunasekera, S 2009, 'A survey of coordinated attacks and collaborative intrusion detection', *Computers & Security*, vol. 29, no. 1, pp. 124-40.

Zikmund, WG 2000, *Business Research Methods*, 6th edn, Dryden Press, Fort Worth.

Zuccato, A 2007, 'Holistic security management framework applied in electronic commerce', *Computers & Security*, vol. 26, no. 3, pp. 256-65.

Appendix A - Ethical Clearance



howarda

Angela Howard

From: Ethics
Sent: Tuesday, 9 February 2010 10:36 AM
To: Angela Howard
Subject: RE: Ethical Clearance Application - Angela Howard

Importance: High

Dear Angela,

Please be advised that the USQ HREC's Fast Track Committee has reviewed your application and has resolved to approve your application, subject to permission being granted by the relevant USQ authorities. Your ethics approval number is H10REA018. I will send an official letter of approval in the mail this afternoon. This email serves as evidence of approval.

Kind regards,
Will.

William Farmer
Research Support Officer
Office of Research and Higher Degrees
University of Southern Queensland
Phone: (07) 4631 2690
Email: will.farmer@usq.edu.au

From: Angela Howard
Sent: Friday, 8 January 2010 12:59 PM
To: Ethics
Subject: Ethical Clearance Application - Angela Howard
Importance: High

Dear Sir/Madam,

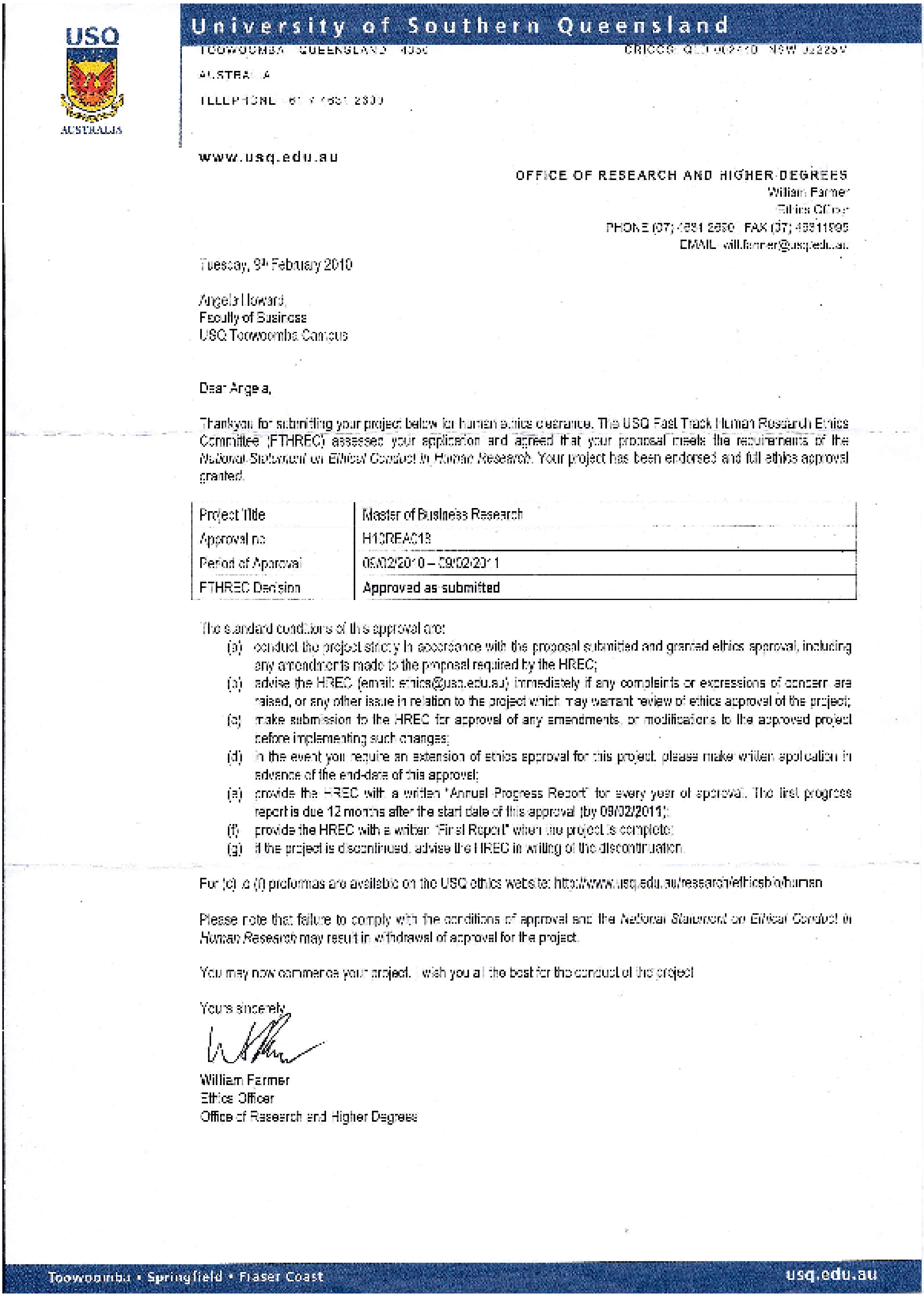
Please find attached my ethical clearance application for the data collection of my thesis (Master of Business Research).

Kind Regards
Angela

Angela Howard | Lecturer Information Systems
School of Information Systems | Faculty of Business
University of Southern Queensland
West Street | Toowoomba | QLD | 4350
Ph: +61 7 4631 5503 | Fax: +61 7 4631 5594
Email: Angela.Howard@usq.edu.au | Web: www.usq.edu.au
ACIS2007: www.acis2007.usq.edu.au

Confidentiality and Privilege Notice
The contents of this electronic message and any attachments are intended only for the addressee and may contain privileged or confidential information. They may only be used for the purposes for which they were supplied. If you are not the addressee, you are notified that any transmission, distribution, downloading, printing or photocopying of the contents of this message or attachments is strictly prohibited. The privilege of confidentiality attached to this message and attachments is not waived, lost or destroyed by reason of mistaken delivery to you. If you receive this message in error please notify the sender by return e-mail or telephone.

The comments expressed in this e-mail do not necessarily represent the policies or views of USQ.



USQ
AUSTRALIA

University of Southern Queensland

TOOWOOMBA QUEENSLAND 4350 CRICOS: QLD 00244B NSW 02225M
AUSTRALIA
TELEPHONE +61 7 4631 2100

www.usq.edu.au

OFFICE OF RESEARCH AND HIGHER DEGREES
William Farmer
Ethics Officer
PHONE (07) 4631 2690 FAX (07) 46311995
EMAIL will.farmer@usq.edu.au

Tuesday, 9th February 2010

Angela Howard,
Faculty of Business
USQ Toowoomba Campus

Dear Angela,

Thankyou for submitting your project below for human ethics clearance. The USQ Fast Track Human Research Ethics Committee (FTHREC) assessed your application and agreed that your proposal meets the requirements of the *National Statement on Ethical Conduct in Human Research*. Your project has been endorsed and full ethics approval granted.

Project Title	Master of Business Research
Approval no	H10REA018
Period of Approval	09/02/2010 – 09/02/2011
FTHREC Decision	Approved as submitted

The standard conditions of this approval are:

(a) conduct the project strictly in accordance with the proposal submitted and granted ethics approval, including any amendments made to the proposal required by the HREC;
(b) advise the HREC (email: ethics@usq.edu.au) immediately if any complaints or expressions of concern are raised, or any other issue in relation to the project which may warrant review of ethics approval of the project;
(c) make submission to the HREC for approval of any amendments, or modifications to the approved project before implementing such changes;
(d) in the event you require an extension of ethics approval for this project, please make written application in advance of the end-date of this approval;
(e) provide the HREC with a written "Annual Progress Report" for every year of approval. The first progress report is due 12 months after the start date of this approval (by 09/02/2011);
(f) provide the HREC with a written "Final Report" when the project is complete;
(g) if the project is discontinued, advise the HREC in writing of the discontinuation.

For (c) to (f) proformas are available on the USQ ethics website: http://www.usq.edu.au/research/ethicsbio/human

Please note that failure to comply with the conditions of approval and the *National Statement on Ethical Conduct in Human Research* may result in withdrawal of approval for the project.

You may now commence your project. I wish you all the best for the conduct of the project.

Yours sincerely,

William Farmer
Ethics Officer
Office of Research and Higher Degrees

Toowoomba • Springfield • Fraser Coast usq.edu.au

Appendix B – Invitation document and consent form

Angela Howard
Department of Information Systems
Faculty of Business
University of Southern Queensland
Toowoomba QLD 4350

Psychological Theories and their Applicability in Resolving Issues with Unauthorised Computer Access

I am a member of the School of Information Systems at the University of Southern Queensland and am currently undertaking a Masters of Business Research. As part of my degree I am conducting a study into psychological theories and their applicability in resolving issues with unauthorised computer access.

In regards to our conversation, I would like to thank you for your participation. Your consent to participate in my focus group on Tuesday, 31 August 2010, at 12:00 noon, in T356, is greatly appreciated.

Your participation in the focus group will provide guidelines about security awareness to ICT management. Light refreshments/lunch will be provided.

It is anticipated that the time to complete the focus group would be 60-90 minutes. This study is exploratory and aims to understand how people solicit information through unauthorised devious ways.

Participants can withdraw their consent and participation at any time. All information given during the focus group is confidential and no names or other information that might identify you will be used in any publications arising from this research. I am able to confirm that the participation in the focus group has no bearing on your current employment conditions.

I am happy to discuss with you any concerns that you may have on this study. If you have any concerns regarding the implementation of the project, you should contact The Secretary, Human Research Ethics Committee USQ. Ethical clearance, approval number H10REA018, for this study.

Would you please complete the attached consent form, as I am obliged to comply with USQ ethical requirements. Should you have any questions about this project please feel free to contact me on (07) 46 31 5503 or Angela.Howard@usq.edu.au.

Please print and sign the consent below, and forward to Angela Howard through internal mail or scan in and email to Angela.Howard@usq.edu.au.

Kind regards
Angela Howard

Consent Form

I, ……………………………. (the participant) have read the information above. Any questions I asked have been answered to my satisfaction. I agree to take part in this focus group, however, I know that I may change my mind and stop my participation at any time. I understand that all information provided is treated as confidential and will not be released by the investigator unless required to do so by law.

If I am participating in the focus group session, I agree for the focus group to be recorded. I agree that research data gathered for this study may be published provided my name or other information which might identify me is not used.

Participant's Name: ……………………………………………….

Participant's signature: ………………………………………….

Date signed: ……………………………………………………….