INFORMATION SECURITY MANAGEMENT IN AUSTRALIAN UNIVERSITIES – AN EXPLORATORY ANALYSIS

By

Tim Lane
AssocDipIT, BMangt&ProfStudies.

Thesis submitted for the degree of Master of Information Technology (Research)

QUT Faculty of Information Technology
School of Software Engineering and Data Communications
January 2007
Key Words

Information Security, Management, Culture of Compliance,
The work contained in this thesis has not been previously submitted to meet requirements for an award at this or any other higher education institution. To the best of my knowledge and belief, the thesis contains no material previously published or written by another person except where due reference is made.

Signature:

Date:
Acknowledgements

This study has been made possible with advice, support and cooperation from a number of people. In acknowledgement of the assistance and encouragement and support that I have received, I wish to express formally my sincere appreciation to the following:

1. My wife Jan for her unending support, encouragement and patience, and my two children Coen and Sophie for their understanding and patience with sacrificed family time.

2. My parents, Peter Lane for encouraging study through my life and Alice Lane for encouraging language skills.

3. My principle supervisor Dr. Lauren May, Senior Lecturer at Faculty of Information Technology Queensland University of Technology, for her support, continual encouragement and positive feedback.

4. My associate supervisors Dr. Kavoos Mohannak, Lecturer at the School of Management and Dr. Neville Meyers, Senior Lecturer at the School of Information Systems Queensland University of Technology for positive feedback, guidance and encouragement during the study.

5. Luke Walford, Infrastructure Manager in IT&TS Southern Cross University, for support and encouragement in undertaking and completing the study.
Table of Contents

1 Introduction to Research
   1.1 Abstract
   1.2 Overview of Research Problem
   1.3 Research Contributions
   1.4 Method Overview
   1.5 Background to Research
   1.6 Security Practitioner’s Management Model
   1.7 Limitations to Research

2 Literature Review
   2.1 Introduction
   2.2 Security Management Approaches
   2.3 Security Policy
   2.4 Awareness of Information Security
   2.5 Compliance with Security
   2.6 Conclusion on Literature Review

3 Methods
   3.1 Research Design
   3.2 Data Generation
   3.3 Data Analysis

4 Key Findings
   4.1 Introduction
   4.2 Summary Coding Results
   4.3 Coding Results for Senior Management Involvement
   4.4 Coding Results for Security Management Approach
   4.5 Coding Results for Security Policy
   4.6 Coding Results for Security Awareness
   4.7 Coding Results for Security Compliance
5 Discussion........................................................................................................................................... 166
5.1 Discussion on Senior Management Involvement ........................................................................ 166
5.2 Discussion on Security Management Approach ........................................................................ 171
5.3 Discussion on Security Policy .................................................................................................. 178
5.4 Discussion on Security Awareness ......................................................................................... 191
5.5 Discussion on Security Compliance ....................................................................................... 195
5.6 CAUDIT ...................................................................................................................................... 209
5.7 Security Practitioner’s Management Model ........................................................................... 210

6 Conclusion....................................................................................................................................... 237
6.1 Summary of Research Outcomes and Recommendations ...................................................... 237
6.2 Research Learning Outcomes .................................................................................................. 241
6.3 Suggestion for Further Study .................................................................................................... 242

7 Appendix A – Survey Instrument .................................................................................................. 243

8 References ....................................................................................................................................... 253
List of Tables

Table 1 Common Australian Based Security Related Standards.........................................41
Table 2 Characteristics of Qualitative Research and Applicability to Project......................70
Table 3 Matrix Showing Research Question and Data Gathering........................................84
Table 4 Super Code Summary - Assigned Codes and Density.............................................97
Table 5 Coding Summary for Senior Management Involvement........................................99
Table 6 Coding Summary for Security Management Approach.........................................109
Table 7 Coding Summary for Security Policy.........................................................................118
Table 8 Coding Summary for Security Awareness..............................................................131
Table 9 Coding Summary for Security Compliance..............................................................143
Table 10 Coding Summary for CAUDIT Involvement..........................................................161
Table 11 International Standards’ Recommendations for Security Policy.........................187
Table 12 International Standards’ Essential Elements of Security Policy..........................189
Table 13 Layers within the Security Practitioner’s Management Model..............................222
Table 14 Detert, Schroder and Mauriel’s Dimensions of Culture........................................229

List of Figures

Figure 1 Security Practitioner’s Management Model for Information Security.................29
Figure 2 AusCERT 2004 Survey - Common Information Security Related Standards.....42
Figure 3 AusCERT Survey 2004 Challenged Computer Security Management Issues....60
Figure 4 Research Methodology Framework.........................................................................67
Figure 5 Assigned Codes for Security Practitioner’s Management Model........................98
Figure 6 Assigned Codes for Senior Management and Information Security..................100
Figure 7 Participants Who Regularly Provide Reports to Senior Management...............101
Figure 8 Participants’ Perception of Senior Management Support.................................102
Figure 9 Senior Management Understanding of the Importance of Security..................104
Figure 10 Assigned Codes for Security Management Approach.......................................110
Figure 11 Approach Adopted for Managing Information Security.................................112
Figure 12 Participants Who Considered Existing Security Management Effective .....113
Figure 13 Changes Required to Improve the Security Management Approach ...........114
Figure 14 Assigned Codes for Security Policy ..............................................................119
Figure 15 Technical Stakeholder are Involved and Supportive of Policy Process ........120
Figure 16 Management is Involved and Supportive of Policy Process .......................123
Figure 17 Participants Who Considered the Policy Process to be Effective ..............124
Figure 18 Participants Who Considered Policy was Complied With .......................126
Figure 19 Assigned Codes for Security Awareness ....................................................132
Figure 20 Participants Who Had a Structured Awareness Program in Place ..............134
Figure 21 Participants Who Considered Raising Awareness an Important Priority ....134
Figure 22 Participants Who Considered Raising Awareness Activities Adequate .......137
Figure 23 Factors that have Increased Awareness ....................................................137
Figure 24 Barriers to Improving Awareness ..............................................................140
Figure 25 Assigned Codes for Security Compliance ..................................................144
Figure 26 Participants Who Measure Security Against Benchmarks .......................146
Figure 27 Participants Whose Organisation Had a Culture of Compliance ...............147
Figure 28 Participants Positioned to Detect and Defend Against Incidents ..............149
Figure 29 Causes of Security Incidents .................................................................151
Figure 30 Top Three Security Threat Concerns ......................................................152
Figure 31 Security Spend Measured Against Central IT Budget ...............................155
Figure 32 Barriers to Improving Compliance ..........................................................156
Figure 33 Areas for Improved Compliance ...............................................................158
Figure 34 Top Three Critical Success Factors .........................................................159
Figure 35 Assigned Codes for CAUDIT Involvement ...............................................162
Figure 36 International Standards’ Recommendations for Security Policy .............188
Figure 37 Edgar Schein’s Model of Layered Organisational Culture and Behaviour ..205
Figure 38 Security Practitioner’s Management Model .............................................211
Figure 39 The Belis and Kiountouzis Structural Model of Security Knowledge ......216
Figure 40 Self Determination Continuum Showing Types of Motivation ...............234
Thesis Structure

This thesis has been structured into the following eight sections:

**Section One** – Section One provides an overview of the research problem, and an explanation of what was undertaken and why. A background context to the research is discussed, including the requirement for information security management to protect the information that modern organisations rely on for continuity of operations. The reliance on information by universities is specifically discussed, together with the university environment and how this presents challenges to the management of information security.

As an outcome of the research, a security practitioner’s management model for information security in the Australian university sector is introduced. The research and its significance to the Australian university sector are described.

**Section Two** – in Section Two a review of the literature is provided. This includes the topical areas that have been reviewed, the main findings from the literature and identification of gaps. These gaps lend support to the research itself by highlighting the issues relevant to information security management.

**Section Three** – the methodology used in the research project is described in Section Three, including the research design and purpose, the data generation method and the data analysis method.

**Section Four** - a statement of the results and the findings are provided in Section Four.

**Section Five** - an interpretation and discussion of the findings is provided in Section Five, outlining the current status of security management, the issues uncovered and how improvements can be made to security management in Australian universities.
An explanation of how the findings and analysis of results supports the proposed security practitioner’s management model is given. Specific as well as general implications and applications are discussed, and recommendations for improvements in security management in the Australian university sector are proposed.

**Section Six** - the final section provides a conclusion and recommendations from the study as well as discussing contributions from the research. Learning outcomes and potential future research are also identified.

**Section Seven** – a copy of the survey instrument is provided.

**Section Eight** – references used in the research are provided.
1 Introduction to Research

1.1 Abstract

Australian Universities increasingly rely on Information Technology (IT) systems for essential business operations, including administration, teaching, learning and research. Applying information security to university IT systems is strategically important to maintaining overall business continuity in universities. However, the process of effectively implementing information security management in the university sector is challenging for security practitioners. University environments consist of a cultural mix of academic freedoms, student needs and compliance mandates. Consequently, unique and divergent demands are placed on securing and accessing university IT systems.

This research undertook a qualitative based exploratory analysis of information security management in Australian universities. The aims and objectives of the research (represented as the research questions) were to determine:

1) What is the current status of information security management practices in the Australian university sector?

2) What are the key issues and influencing factors surrounding the effectiveness of information security management practices?

3) How could improvements in information security management be achieved?

The findings from the research led to a comprehensive and insightful examination of the current status, issues and challenges facing information security practitioners in Australian universities. The research findings culminated in the development of a Security Practitioner’s Management Model. An essential aim of the model is to assist security practitioners to successfully implement and progress information security in the Australian university environment. The research improves current understanding of information security issues and reinforces the pertinence of information security management as a strategically important business function for Australian universities.
1.2 Overview of Research Problem

The Security Practitioner’s Challenge

Although information security in universities is a function that is recognised as necessary, the actual priority allocated to security is not always commensurate with its importance. Further, there is often conflict with exactly how specific implementation of security practices should occur and how to manage the associated impact on work practices. This conundrum leads to difficulties in how security should be managed. Often an overall lack of a coordinated security approach can exacerbate this situation, highlighting the problem of gaining acceptance of security in a diversified and priority-competitive environment.

From the security practitioner’s perspective, working in the university environment means dealing with complexity, both in terms of people and systems. An approach is required that provides a meaningful structure for progressing information security in what is a highly challenged environment, where competing priorities exist. Therefore determining how the process of information security management could be improved within the university environment has been a key focus of this study.

There has been limited published academic literature to date that specifically focuses on information security management in Australian universities. At the same time, the profile of security is increasing due to the recognition of its important role in protecting information. Many Australian universities are coming to terms with establishing effective governance over information security. Understanding the placement of security in both the corporate and academic context is a difficult balancing act.

The effective management of security risks ultimately requires appropriate implementation of information security management. Security management is more effective when it is applied in context to business requirements and balanced against the university’s adopted risk posture.
The Australian University Environment

The context for information security in Australian universities is complex and tends to be obfuscated by university culture and operating environments. The practical implementation of information security practices and activities in universities requires a solid foundation from which to operate. Yet despite the importance of information security to Australian universities, existing approaches, standards and guidelines for security are not necessarily integrated. They do not provide a single point of understanding for how the process of information security should be managed. There is certainly no overall governance for how information security should be managed within the higher education sector or sector specific recommendations.

In determining how information security management could be improved in Australian universities, an analysis of the factors and issues that facilitate or impede information security in Australian universities was required. An analysis of these factors through this research has lead to a management model to assist security practitioners in universities to achieve a more effective approach in managing information security.

1.3 Research Contributions

Context and Significance

The relevance of this research work is of significant value to the university sector, as it represents the first comprehensive published study into contemporary and relevant issues facing Australian universities from the security practitioner’s perspective. The research provides an insightful examination of the current status of play, highlights issues and deficiencies, and provides an explanation of how improvements can be made.

The timing of the research reflects an early attempt to begin to ‘baseline’ knowledge on security management in Australian universities. This importantly brings us a step further in placing security at a level where all Australian universities have participated in an improved understanding and awareness of security as an increasingly prominent theme in operations. From this perspective the research effort sets a precedent in
involving all Australian universities in a security research project, which in itself establishes an initial benchmark.

**Theoretical and Applied Contributions**

The benefits of this research include both theoretical and applied contributions. On a *theoretical* level, the research contributions include:

- The study provides an integrated theoretical framework that can be used by Information Security Practitioners to effectively structure the process of applying information security within the organization. This model is an aid for security practitioners to conceptualise the task, aimed at a ‘how to think’ instead of a ‘what to do’ approach, and provides a way for practitioners to focus on transitioning the knowledge they and others possess into security implementation.

- The Security Practitioner’s model can be adapted to other relevant small and large organisations, not just Australian universities. Investigation of the model's suitability to other organisations is a topic for future research.

- The research has contributed to the existing literature through a journal paper to the Journal of Theoretical and Applied Electronic Commerce Research (May and Lane, 2006), and two conference papers APIEMS 2004 (Lane and May, 2004) and RNSA 2006 (May and Lane, 2006).

- The study also highlighted the potential for benchmarking security in Australian universities as a future research project.
On a practical level, the research contributions include:

- Providing practical guidance via a detailed articulation of the current status of security management in specific key areas. The main issues, barriers and influencing factors that impact the actual implementation of security in Australian universities are identified, with recommendations for addressing those areas.

- The research demonstrated how the application of the theoretical framework can assist the security practitioner in the process of security management in Australian universities by leveraging from previous research and incorporating contemporary requirements. This includes relating the various disparate objectives of existing security management guidelines, standards and policy to the theoretical framework.

- The establishment of an Australian higher education specific security email forum through AARNet (Australian Advanced Research Network) dedicated and used by university security practitioners and other interested practitioners in Australia. This forum is constantly gaining momentum in use, and has extended to other related institutions providing a collaborative forum for sharing and discussing security related ideas, problems and solutions.

- The submission of a key findings report to CAUDIT (Council of Australian University Directors of IT).

- Lastly, this research has promoted on a wide scale to all involved that security in universities is a growing imperative and needs to be elevated to an appropriate corporate governance level.

**Benefits of Research - Theoretical**

It is of interest that to date, research focusing specifically on information security management in the Australian university environment has had limited academic involvement. The general research that does exist on information security management
often focuses predominantly on context specific models for management or specific behavioural aspects of managing security – not both. Management models tend to concentrate on specific approaches for aspects of security (for example risk management), whereas behavioural aspects often focus on areas such as policy and awareness. What is lacking in the literature is a systemic approach to the management of security in Australian universities, which integrates and shows the relationship between both the organisational context and behavioural aspects.

**Benefits of Research - Practical**

The security practitioner’s model has been adopted at Southern Cross University in Lismore, NSW. The model provides a holistic structure which has substantially improved the credibility of the information security management program. The model structure is fully compatible with, and complementary to, the concurrent phasing-in of enterprise-wide IT architectures.

Effectiveness of the model is measured most noticeably at both management and staff levels. Management at the university recognise and accept the ‘knowledge gathering’ role of the information security manager’s position, and now not only support the role, but expect security based research. General awareness of university staff has also increased with a particular emphasis on individuals’ active participation in relevant areas of the security process.

**1.4 Method Overview**

An introduction to the method used for the research is provided in this section, with full details provided in Section Three – Methods. The research involved an exploratory method using a survey instrument applied to universities as well as observation in field work. The primary data generation method involved applying a survey instrument containing 35 open and closed questions to every Australian Vice Chancellor (AVCC) University in Australia. This represented a 100% response rate as all 38 Universities participated in the survey. The survey was conducted via telephone interview with
either the university Director IT and/or Security Manager equivalents. The interviews averaged approximately 30 minutes each and were digitally recorded, then transcribed verbatim to a word processor. This produced over 70,000 words of text, providing a very rich data set for analysis. Qualitative data analysis was then rigorously applied in order to identify themes, patterns and relationships. Theoretical constructs were then generated from the gathered data, with validation from the literature.

The secondary data gathering method involved the researcher as an instrument through the role of Information Security Manager at Southern Cross University. This provided an opportunity for observation in the field as well as review and analysis of written material.

**Research Purpose**

The purpose of the research was to undertake an exploratory analysis of information security management in Australian universities in order to understand the current status, and identify issues, barriers and enablers to security management in universities. Understanding these issues is necessary in order to determine and develop strategies for improving the existing management of security in the higher education sector. The focus of this research project therefore became one of an exploratory analysis, involving understanding the current situation, identifying key issues, and developing strategies for improvement in security management.

**Research Justification and Rationale**

As previously noted, research focusing specifically on information security management in Australian universities has received little academic focus. This is despite growing reliance on information and the importance of protecting information through security practices. The associated difficulties in the university environment with managing information security are a key aspect of this study. As this work is relatively new in the Australian university context, an exploratory process was required in order to identify issues and develop improvements in current information security management practices.
The justification and rationale for the study are further grounded by linking the importance of information security management in Australian universities to wider social implications. Universities constitute an important aspect in protecting both their own information as well as critical infrastructure in society. Looked at from a social perspective, universities host a large number of diverse systems from both a business and academic viewpoint. The sector also characterises a fertile breeding ground for IT exploration and research as well as reflecting and promoting good community standards through their practices, customs and processes.

In order to improve security process there is a need for an increased understanding of complex interactions, tacit processes, and often hidden beliefs and values (Marshall and Rossman, 1999). This demonstrates the need for the study to gain a behind-the-scenes view and improve on current practices. Improvement on practices can be achieved through the identification and interpretation of commonly held perceptions, norms and customs and the often hidden, tacit aspects that impact the effectiveness of information security management practices.

A systematic approach and methodology was implemented to ensure an improved understanding of the phenomena, so that improvements in security management practices could be realised. This research proposes a conceptual model (the security practitioner’s management model). This model is designed to facilitate the process of knowledge transition into implementation, towards an overall culture of compliance towards information security in the university sector. The linking of this conceptual framework to larger theoretical domains ensures that this work is of wider significance to the Australian university security community. Strong, detailed conclusions and recommendations also ensure that this research provides a significant contribution back to Australian universities.

In studying the phenomenon and linking the specific research questions to larger theoretical constructs, the particulars of the study serve to illuminate larger issues and therefore hold potential significance. The nature of the research being exploratory
provides the potential for identifying important variables for subsequent explanatory or predictive research in the relevant area (Marshall and Rossman, 1999). On this basis a significant outcome of the study for subsequent research is highlighted as the need to focus on benchmarking information security management within the university sector. Results from the study indicate that, whilst it can be argued that universities act somewhat in competition, cooperation between universities also forms part of the culture. Universities are extremely interested in peer activities and are curious to benchmark their own efforts and direction against peer institutions.

**Ethical Issues in Research**

The researcher completed the standard Queensland University of Technology ethical clearance application. Following ethical clearance and approval, an information package was developed to complement the survey instrument, and distributed to participants. The information package included a statement advising ethical clearance, as well as confirmation of the confidentiality and privacy of collected information.

**Research Questions**

In order to identify and understand the phenomena and to improve on the current approach that universities adopt for information security management, three key research questions were generated that evaluated the research problem by acting as boundaries around the study without unduly constraining it. The questions essentially focus on current status, interactions and processes. This provides a linkage to the key research problem and to research literature and theory, while at the same time being importantly founded in everyday realities (Marshall and Rossman, 1999).
The following research questions were used to form the basis for an exploratory analysis of information security management in the Australian university sector:

1) *What is the current status of information security management practices in the Australian university sector?*

2) *What are the key issues and influencing factors surrounding the effectiveness of information security management practices?*

3) *How could improvements in information security management be achieved?*

Initially, to find out how information security is currently being managed in the university sector, an interview using a survey instrument was conducted with all 38 Australian Vice Chancellor Committee (AVCC) listed universities. The interviews were aimed at answering each of the above questions. The first question was concerned with identifying and describing the current status of information security management in Australian universities. The second question aimed at identifying and understanding the associated information security management issues and deficiencies. The third question was aimed at identifying strategies for improving the future status of information security management.

The information gathered from the interviews was analysed. The findings provided a description of the current status of information security management. Based on an analysis of the findings, identification of key issues and suggested strategies for improvement were proposed. Further analysis of the survey results gave rise to a conceptual model (the security practitioner’s management model – Figure 1). This model is designed specifically for university information security professionals whose role encompasses not only an awareness of relevant security issues, but a responsibility for transforming their knowledge and understanding into applicable processes and techniques suitable for implementation at the practical operational level. The model aims to facilitate security management in the Australian university sector, by linking theories and findings from the study to an improved process for security management. The model provides a theoretical reference for facilitating the management process of
security transition from knowledge into implementation, towards an overall culture of compliance.

A detailed explanation of the model is provided in Section Five - Discussion. The model essentially acts as a reference for security practitioners to understand how the process of security knowledge should be transitioned into implementation. This is achieved by mapping knowledge against a layered management structure, where other existing security guidelines, standards and frameworks are able to be referenced against organisational requirements. Through the use of a structured process and supported by communication and awareness, a university’s culture of compliance is focused on. The intended outcome is to facilitate normalisation of behaviour towards information security compliance. This effectively constitutes the organisation’s security posture, norms of behaviour and resultant compliance with security.

The model incorporates influences on organisation culture resulting from both internal and external factors, including outputs from the layered structure. The end culture of compliance is continuously referenced back to the overall body of security knowledge through a ‘Plan, Do, Check, Act’ process (ISO/IEC 27001:2005), for further channelling through the layered management framework. In this way, a quality process is established where a continual momentum of knowledge applied through a structured framework affects the desired culture of compliance. The framework is premised on the notion that developing and maintaining a culture of compliance is a fundamental goal to information security management.

1.5 Background to Research

The background to the research expands on the concept of modern organisations’ growing dependence on information. The constantly evolving risks that preservation of information faces are exacerbated by the increasing frequency and sophistication of threats. Effectively managing threats to information in the university environment
involves the process of applying information security to ensure that risks, costs and efforts are balanced.

Universities are amongst the growing number of institutions that increasingly acknowledge the importance of protecting information which is relied upon for business purposes. Protecting information in universities involves a range of controls applied appropriately and guided through information security practices. As information and its use evolve, attention is being paid to the need to apply information security practices in accordance with the dynamic business environment in which universities operate. The environment itself is therefore recognised as an important contextual factor in the overall management of information security.

The Information Age and Continuity

The growing importance of information in modern societies is no doubt a defining feature of our present-day world. The prominence of information in today’s society has led various scholars and leaders to claim that we now live in a new information society, a society where information dominates new modes of social organisation (Pyati, 2005). As our information society evolves, organisations increasingly store, use and distribute information. Information used by organisations is now highly valued and has become an important strategic asset.

Social order in contemporary society is highly dependent on accurate and predictable information structures. Internationally, boundaries in cyberspace necessitate an integral relationship between organisational structures and their information foundations. Reliance on the underlying information structures and technologies demands a responsible approach to the technological structures themselves, as well as to the management of those structures. Understandably, focus on the reliability and resilience of information structures becomes an important component of maintaining order within organisations.
A connection exists in society between the growing reliance on electronic systems and associated information. A requirement exists for effective information security management to protect information systems from an escalating number of threats and risks. This is necessary in order to avoid major disruptions to services, as well as to protect organisations from loss, damage or modification of important data.

The dichotomy of social reliance on information is reflected in the fact that some components of society either inadvertently fail to stabilise, or in fact deliberately increase efforts to destabilise, the very information upon which we depend. This can occur through system user errors or malicious action taken by hackers and cyber criminals. As a result, one or more key characteristics of the confidentiality, availability or integrity of information can be compromised. Consequently, maintaining continuity in modern organisations ultimately relies on the preservation of information achieved through the process of applied information security.

**Universities’ Reliance on Information**

Universities today are highly reliant on information to support their core activities and business operations. There is a dependence on activities associated with creating, using and sharing information for universities’ core teaching, learning and research functions. Add to this the extensive amount of intellectual property generated by universities, and the importance of information to universities is evident.

Universities have, along with other organisations, adopted and embraced information systems and technologies in order to survive in a competitive environment. In today’s environment effective operational control and strategic direction are linked to the effective management of high-quality information. The ubiquitous nature of information means that universities are directly impacted by their reliance on, and use of, information technology resources, systems and information.
Information Security in Universities

As with other organisations in society, universities are increasingly acknowledging the importance of information security to protect business and research information. This acknowledgement is underpinned by recognition of information as a valuable asset and a strategic resource. Valuable assets understandably require appropriate protection. Having appropriate and effective information security control mechanisms in place to ensure the availability, confidentiality and integrity of information is therefore critical to the process of security management (Fulford and Doherty, 2003).

While this concept is simple to state, the practical implementation of activities associated with information security processes in universities is not necessarily straightforward. Wood (1999) suggests that few authors have recognised the fact that individual organisations have not only disparate security requirements, but that the dynamic business environments in which they operate are important factors that need to be taken into account. Hence the culture of organisations including universities is an important factor to consider for security management.

The function of information security management in universities tends to operate with corporate mandates associated with the business of providing education on one side, and the cultural and pedagogical pursuit of academic teaching, learning and research on the other side. Security becomes somewhat of an art form in this environment, requiring navigation through the various complexities of university culture and challenges.

The University Cultural Environment

Universities represent an eclectic environment involving an interesting challenge of culture and technologies. By their very nature universities are dynamic and operate in increasingly complex environments, typically reflecting large, complex and diverse information systems. These systems are used by different stakeholders with varying requirements. The complexities and challenges that exist involve diverse requirements, changing and disparate technologies, openness to the Internet, explorative students and
research bases, and business goals and objectives that are not always understood or accepted by all constituents.

There is a need to ensure academia is not impeded while balancing corporate and business requirements, including a transient and at times explorative student base. Add to the equation a student residential base, various research environments, and broad core values. Further, a complex technology base consisting of multiple high bandwidth links to the Internet, and frequently a disparate mix of technologies, systems, operating systems and requirements, forms the basis of university computer environments.

The research environments in universities often have values including tolerance, individual autonomy and experimentation. These are values which, although contribute ultimately to developments in security, paradoxically do not necessarily go hand in hand with fostering a culture of maintaining operational security. University members understandably differ in opinion on the application of specific practices. Constituents are therefore challenged with the right balance between adopting effective security measures and maintaining the fundamental principles of academia (Luker and Petersen, 2003).

The relatively open access environment in higher education institutions from an information security perspective needs to take into account contributing factors such as the size of the organisations, the decentralization of Information Technology services and the associated standards, policies and procedures. The real cost of impeding ‘academic freedom’ through stringent security rules and requirements, and the fact that higher education sectors are a gateway to the Internet with potentially thousands of members (staff and students) as system users are also issues. The cross-section of interest groups and various stakeholders with conflicting interests is another factor. Higher education sectors in particular are unique in their semi-privatised quasi-government mode. This suggests that establishment and implementation of stringent controls, which would normally provide adequate protection of information can in fact prove politically and technically difficult to implement or uphold.
In relying on the quality of their information, universities are currently facing a growing number of threats that have increased in the level of sophistication and severity of impact. The increased risks and threats have led to an increased awareness amongst managers of the needs for careful and organized management for information security.

**Security Management Challenges in Universities**

Due to the augmented awareness amongst managers of the need for information security, the associated appointment of Information Security Officers, Coordinators or Program Managers is now commonplace. In some cases the appointment of the information security function defaults to an existing staff member. In either case there is evidence to suggest that while recognition is occurring for the need for information security, the level of funding is not commensurate with the acknowledged need for security (Ernst and Young 2003).

This ultimately culminates in a downward shift of information security responsibility within the organisation and can result in a number of difficulties (Kwok and Longley 1999). This can include a lack of senior management commitment, a lack of authoritative source of guidance and problems with understanding and therefore knowing exactly how much security is required. Further, risk analysis may not uncover all necessary information, and demonstrating security compliance with internal and external auditors may be difficult without a proper representation of information security.

The challenges for universities extend well beyond mere technical diversity. There also exists a requirement for effective information security to coexist and balance with the more traditional university cultural values, such as academic freedom and work practices, and to merge seamlessly with modern universities’ business goals. The traditional embracement of this cultural value has fostered an acceptance of freedom of exploration, experimentation and generally pushing boundaries. Kotulic et al., (2004) accurately typify these types of challenges by noting a need to not only attend to the complexities of the various components of IT systems, but also to successfully integrate
the IT components with the organisation’s business strategies. The essential goals of information security extend therefore, to enabling business functions in universities.

Effective information security ensures a high ‘quality of service’ of information infrastructures and technologies, which support and complement the business goals of the organisation. As such, the discipline of information security has evolved to demand that its practitioners integrate an understanding of the business issues, use sound interpersonal skills, and adapt a solid understanding of the role of information technology itself in the process of ensuring security. The management of information security necessitates an approach that is suited to the organisation. This also necessitates an understanding of how information security ‘fits’, based on the structure and culture of the organisation. This is where the requirements for information security in universities differ from other types of institutions.

Information security is progressively being seen as an important business function requiring management from a business perspective. Although technology itself is a major control applied to mitigate security risks, it is the management of security as a business function that determines ultimate success. The application of technology is most effective when aligned with the business goals. Therefore, effective security depends on effective management.

The need for effective information security management is therefore evidenced by a combination of factors. These include an increase in the reliance on electronic information, an increase in the events and activities that threaten the information that is relied upon, and the corresponding need for the application of controls to mitigate risks.
1.6 Security Practitioner’s Management Model

The study improves current understanding of information security management in Australian universities by synthesising the findings of the study to a theoretical framework presented in this thesis as a Security Practitioner’s Management Model (Figure 1). The model aims to facilitate the transition of expert security practitioner knowledge into implementation. This is achieved through channelling knowledge through the model’s abstracted security framework and focusing on cultural compliance towards security.

The security practitioner’s model provides a mechanism for addressing some of the complexity in university environments for security practitioners. The model begins with the concept that security practitioners possess and have access to, specific expertise and knowledge related to information security. Security practitioners are aware of current and emerging threats and know what should occur to mitigate threats, but at times experience difficulty in obtaining appropriate compliance with security. By applying the model, knowledge retained by the practitioner is referenced through a structured, layered security management framework. This knowledge may be a combination of personal and professional understanding and knowledge, peer knowledge, broader organisational knowledge, information technology expertise, management ability, best practice frameworks, and previous experiences of the individual practitioner.
Figure 1 Security Practitioner’s Management Model for Information Security
For knowledge to be implemented, an information security management framework is used to interface with a layered structure across the organisation. In summary, ensuring that the adopted information security management framework can be applied through a layered model across the enterprise is fundamental to ensuring a structured, coordinated and comprehensive approach to security. The various layers of the model are briefly described, with a more detailed description of each layer provided in Table 13, page 212.

**Contextual Layer** – the contextual layer takes into account the business context of the organisation, to incorporate the core business and organisational environment, and includes the prevalent culture of the organisation. This layer ensures that information security management has an understanding of the objectives of the business and is therefore an enabler of the business.

**Conceptual Layer** – the conceptual layer represents the security posture of the organisation, reflected through risk management and supporting policy. The concepts of information security management are applied in this layer, providing the framework for security in lower layers.

**Logical Layer** – the construct layer symbolizes the virtual constructs of security, the logical application of security achieved through design and architecture and domains.

**Physical Layer** – the physical layer denotes the actual physical security including infrastructure, devices, hardware and software. This is the application of security policy, architecture and design through physical means.

**Operational Layer** – the operational layer involves people applying technologies, processes and procedures, in support of the security function.

This layered structure begins at the business strategic level, represented as the contextual level, and is abstracted across the organisation to the daily operational layer. Across this layered structure, the process of communication and awareness facilitates the end goal of a culture of compliance. The central goal of the model is the required organisational
level of a culture of compliance with the depicted external and internal influences viewed as inter- and intra-organisational factors. Both inter and intra organisational factors have varying degrees of impact on cultural outcomes. The resultant level of organisational compliance towards security is then assessed, with necessary adjustments taken by the security manager to continuously improve the security process. This lifecycle approach represents the continuous transition of knowledge towards an effective security management process and improved cultural compliance.

An important attribute of this model is that best practices are extremely important and have a significant role to play in the management of security. A range of best practices is applicable to information security management, including the growing maturity and consequential acceptance of well-regarded frameworks such as AS/NZS ISO 17799, CobiT, ITIL, COSO, ISO9002, Capability Maturity Model (CMM®), Project in Controlled Environments (PRINCE), Managing Successful Programmes (MSP), Management of Risk (M_o_R®), and Project Management Body of Knowledge (PMBOK®), (ITGI, 2005).

Although selection of various elements of disparate best practices can be aligned to suit the organisation, invariably the use of best practices needs to be applied in context to organisational needs. The implementation of best practices tends to be costly and unfocused if treated as purely technical guidance. The most effective approach is to apply best practices starting at the business context. Implementation of best practices should therefore be consistent with the organisation’s business risk management and control framework (ITGI, 2005).
1.7 Limitations to Research

The research questions and the conceptual framework establish boundaries and limitations. The research is specific to the management of information security within the Australian university context. The study is from the information security practitioner’s perspective and is further limited to an exploratory analysis of the current status of implementation, identification of the key factors and issues impacting effectiveness, and identification of strategies for improvement.

In terms of limitations and unresolved issues, the study found that security is a moving target and therefore the survey was a ‘snapshot in time’. The insights gained from this study are therefore likely to change over time. However, it is hoped that changes will be positive and that increased sophistication in security governance adopted by universities will continue. The study focused very much on issues and influencing factors, and therefore an examination of the technical side of security was outside the scope of this research. It is the firm belief of the researcher nonetheless, that technology must ultimately be accompanied by an appropriate behavioural response towards security to facilitate effective security management across the enterprise.
2 Literature Review

2.1 Introduction

The approach to the literature review involved an initial in-depth study of available literature through a variety of sources. These sources included library books, journal articles, magazines, research from Australian Digital Thesis (ADT) online, online books, information security whitepapers, conference proceedings and presentations, and a wide variety of other information security sources available from the Internet. During the course of the research project, a consistent and continuous refreshing and updating of information as well as seeking out further information in the field of information security management occurred. This served several main functions as recommended by Marshall and Rossman (1999). Primarily, the review helped to:

- support the relevance of the study by confirming the importance of the area and highlighting the challenges associated with effective information security management
- locate knowledge through an initial broad overview, followed by an ongoing and continuous update of information security literature
- review and critique previous work undertaken by researchers and authors
- identify and demonstrate the research paradigm being studied
- place the research problem in context by identifying both assumptions and gaps that needed to be solved within larger empirical traditions
- play an important role in both the data gathering and data analysis phases by illuminating propositions, guiding theoretical constructs and linking relationships between abstract concepts.

The primary objectives of the literature review were to provide a relationship between current knowledge on the key areas of the research and to highlight the research gaps that exist in relation to their application to Australian universities. It was found that the literature strongly advocates managing information security through a framework or
what is more commonly described as an ‘Information Security Management Programme’ (ISMP) or ‘Information Security Management System’ (ISMS). The international standards for the development of an ISMS recommend that, as the first step towards developing an ISMS, policy is defined.

Similarly, a major end goal of information security policy is compliance so as to minimise risks; yet awareness, which is a most challenging area, is most integrally connected with gaining increases in compliance. Therefore the literature review focused around these areas, which linked to the research questions and objectives. The literature review found gaps relevant to the project, namely that a framework for management of information security specifically in Australian universities is required. Following from this is that policy and ultimate compliance is an area of importance difficult to progress - the university environment poses its own unique challenges in this area.

2.2 Security Management Approaches

Gaining an accepted taxonomy of the components of information security is a difficult task. It is however useful to categorise and describe the elements, components or aspects of information security in an effort to conceptualise the problems facing those responsible for security. Information security is a wide area, covers a large variety of both technology and governance issues, and as a function has changed substantially over the past fifty or so years.

An Historical Perspective to Information Security Management

It is helpful to understand exactly what and where information security is today, by applying an historical perspective. Von Solms (2000) provides such a perspective by offering a view of the development of information security as having undergone three distinct generational ‘waves’. Von Solms proposes that the first generation, the ‘first wave’, which he calls the ‘technical wave’, existed up to the early eighties and was distinguished by a very technical approach to information security. Recall the days of mainframe terminals and batch Electronic Data Processing (EDP).
Even during this stage however, the technical administrators realised they would need to obtain further management involvement. The ‘second wave’, which ranged from the early eighties to the mid nineties, is labelled as the ‘management wave’. This wave is characterised by an increasing interest and involvement by management in information security. This wave supplemented the technical wave and increased the importance of information security.

However, while this improved things somewhat, after a while it became apparent that a greater understanding was needed – specifically, understanding the value and effectiveness of information security. This necessitated being able to measure and compare information security against a baseline, as well as measure and compare against other institutions. This saw the development of the ‘third wave’, called the ‘institutional wave’. This is the existing wave today. This third wave is represented by the recognition of and interest in, international standards, codes of practice, security certification, cultivating a corporate security culture, and dynamic and continuous security measurement. While this analogy helps in providing an historical perspective in information security, it reveals little regarding what is involved in information security.

Besides these generational waves, information security has also been described from a very high conceptual level as broadly involving both 'technical controls' and 'leadership'. Therefore, besides technology, the actual leadership of security approaches, involving overall governance and management, is a major facet of security. Other definitions have attempted to explain information security in more detail, by including the interrelationships between the areas of information security in a more holistic manner.

The CIA Model of Information Security Management

Whitson (2003) suggests that the major facets of security management are guaranteeing the confidentiality, integrity and availability of information (referred to as the ‘CIA’ model of security). The confidentiality, integrity and availability of security is a relatively commonly accepted ‘model’, whereby security can be viewed as involving a process to provide information with the CIA principles. Until recently, the CIA model
has been considered the ‘cornerstone’ of security. However, increasingly it is considered deficient in taking into account many of the other important aspects of security. Despite the relatively wide embracement and overall acceptance of the CIA model as a security model, research suggests that this model is now too simple to describe more than the basic elements of security. For example, elements that the CIA model does not represent include accountability and responsibility.

This is explained perhaps by the fact that the CIA model was developed in the era of computing, when electronic data processing (EDP) operations were representative of most computing environments, and information security was seen mostly as basically a technical function. The IT environment is now substantially different to the early data processing days and hence the comprehensiveness of the CIA model is in question. The CIA model reflects early approaches that were very technically oriented. Lacking in the CIA model is the new requirement to have a business focus incorporated by an accountability and responsibility orientation; i.e. information security should be driven from a business objective approach not just a technical approach. Moving information security out of the IT domain is necessary to include a wider business perspective, and more human related activities.

Whitson (2003) contends that security is primarily achieved through risk analysis, security policies, procedures and documentation, providing training and awareness and preparing for disaster avoidance and recovery. Comparatively, Andersen (2001) and Von Solms (1999) include in their definition substantial organisational involvement of stakeholders and the application of recognised security standards. It is obvious at this point that even if the CIA model were uniformly accepted, it is too basic now to properly represent security. Additionally, it does little to guide the way in which security should primarily be achieved, including the activities and functions involved, and as such would probably result in a lack of agreement on this.

Having an historical perspective therefore may help understand where information security is up to. However, to date, despite the emergence of CIA and other standards,
models and frameworks, there lacks a commonly held view and practical implementation of a standard approach to the management of information security. It is almost as if organisations are caught somewhere between a technical CIA view of information security at one end, and true integration within corporate governance at the other end.

Applying the lack of consensus to the development of a practical conceptual framework for information security management thus becomes even more difficult, perhaps due in part to the evolving uniqueness of requirements for different organisations. So while some authors agree loosely on the functions within security management (Siponen and Kajava, 1998; Andersen, 2001; Von Solms, 1999), actually applying information security functions effectively within the organisational context of the higher education sector is still a complex issue.

**An Information Security Management Framework**

A range of standards and frameworks has been developed in recent years that has helped shift the focus away from the previously narrow view of security (represented by the CIA model) to a wider framework. This type of framework is one that takes into account a business perspective, including not only a range of measures but also a focus on organisational structure, policy, and the capacity for measurement and certification. An emerging concept leading from the development of these frameworks, and related to the application of management to information security, is the use of an ‘Information Security Management System’ (ISMS) based on recognised standards. An ISMS provides a management framework which the organisation can reference, and is designed to meet the needs of the individual organisation. Information Security Management Systems are in effect, an organisational framework for the operation of information security.

The primary purpose of an ISMS is concerned with the way, process or method in which information security is managed from an organisational perspective. From this perspective ISMSs are considered to be a helpful reference to the process of managing
information security. The use of an ISMS for the management of information security is recognised through research as being important and is recommended by various authors (Eloff and Eloff, 2003; Von Solms 1998c, Longley, 1999).

**Information Security Management and Organisational Culture**

An ISMS should reference all the necessary required areas of governance for information security and include the use of an appropriate mix of policies, standards, guidelines, codes of practice and technical controls. It should also reflect organisational cultural values and consider relevant legal and obligatory requirements. Ideally, an ISMS should be holistic in approach. However, a significant issue exists in developing an ISMS in attempting to cover the applicability of various perspectives including managerial, technical, legal, strategic and human related aspects. Issues in this area include the extensive human resourcing required to cover all areas, and the lack of understanding regarding the effectiveness of doing this. It also includes a tendency by some organisations to push IT systems and solutions out with little quality assurance (i.e. security).

Universities are often one of the early adopters of initiatives such as collaborative networking and instant communication. University structures mean that individuals who use information in a highly collaborative manner are characterising a strategic focus on the value and protection of information systems, whether intentional or not. These type of initiatives are likely to increase as work practices evolve. However, despite this collaboration, pressures of cost containment and external competition exert an influence.

This results in the adoption of security often being secondary to the adoption of the actual IT systems that provide the support for collaboration. Therefore there is scope to understand the relationship of an ISMS to organisational collaboration, structure and context, particularly when new systems are introduced. A reasonable premise is that the development, implementation and use of an ISMS have the potential to provide an effective integrative conceptual framework to assist in the function of information security within universities, if applied and maintained appropriately.
It follows that a key issue in relation to an ISMS is understanding the organisational requirements. The organisational requirements for Australian universities are complex and unique due to the challenges that were previously highlighted. Due to the nature of technology, organisational structures and processes as well as collaborative requirements in universities, a flexible or dynamic solution is often required in an ISMS. Information security for universities in the future will therefore need to take into account organisational operations and context (Dhillon and Backhouse, 2000; Siponen and Kajava, 1998; Anderson, 2003). An examination and understanding of the relevance of ISMSs within universities, including the extent to which they are used and how effective they are, is useful information to help understand this problem.

**Measurement of Security Management**

The process of managing security needs a reference to ensure that all the necessary areas are being covered, and requires quantification to determine the level of security that is being implemented, identification of what is lacking and to track effectiveness of control measures (Martins and Eloff, 2001). A problem with not applying some type of management system to security is that it’s likely to result in either too many controls or not enough controls being applied to areas within the organisation. An ad-hoc approach to information security from a management standpoint, therefore, has the potential to be ineffective, and measurement becomes difficult. Measurement of the effectiveness of security is an important yet difficult process. In order to gain commitment from senior management, not only is it necessary to align security with business goals, but also to demonstrate that the application of security is effective to those goals, therefore having benefits that can be evaluated and measured.

The difficulty in evaluating the benefits of information security is considered one of the reasons for reluctance by senior management to invest in information security (Kankanhalli et al., 2003). May (2003) advocates that meeting the principles contained in standards can help measure and improve existing security processes and procedures. Obviously this would be accompanied by performing risk assessments and internal reviews. While measurement of security through models such as checklists based on
17799 standards or the ‘Capability Maturity Model’ exist, the challenges associated with measuring security are outside the scope of this project.

It is, however, worth mentioning that the challenges of measurement have an impact on the capacity to evaluate the benefits of information security, and therefore influence the likely commitment to information security. In the opinion of the researcher, information security can only be truly properly managed if an international certification scheme is provided, a security culture of compliance is ubiquitous, and measurement is possible and is undertaken.

**The Use of Standards within Information Security Management Systems**

Standards are an important aspect of developing an ISMS. Having an ISMS based on international standards such as ISO/IEC 17799 means that an organisation has a reference framework, leading to greater confidence that its practices are based on standards that are internationally accepted as being relevant and important (Von Solms, 1999).

Previous research undertaken by authors (most notably Von Solms, Longley, Siponen and Baskerville) stress the importance of applying an effective model of management to information security, including the application of various recognised security standards (Siponen and Kajava, 1998; Kwok and Longley, 1999; Von Solms, 1998b and 1999). Research by Von Solms (1999) indicates that standards themselves such as 7799 should play a major role in information security management, and May (2003) argues that standards are one of the best methods for organisations to develop effective strategies.

Table 1 provides a summary of common standards applicable to information security management. It is likely that some universities will be using or moving towards using one or more of these standards for information security management. Because the use of standards can assist an ISMS, part of this research will be to assess the use of various information security standards in terms of the extent of their use and their applicability.
<table>
<thead>
<tr>
<th>Code</th>
<th>Name</th>
<th>Overview</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACSI 33</td>
<td>Australian Government Information Technology Security Manual</td>
<td>Developed by the Defence Signals Directorate (DSD) to provide policies and guidance to Australian Government agencies on how to protect their IT systems.</td>
</tr>
<tr>
<td>HB171:2003</td>
<td>Guidelines for the Management of IT Evidence</td>
<td>Aims to provide guidance on the management of electronic records that may be used as evidence in judicial or administrative proceedings.</td>
</tr>
<tr>
<td>RFC 2196</td>
<td>Site Security Handbook</td>
<td>A guide to developing computer security policies and procedures for sites that have systems on the Internet. It essentially takes a risk management approach.</td>
</tr>
<tr>
<td>AS/NZ 4360:1999</td>
<td>Risk Management</td>
<td>Provides a generic guide for the establishment of a risk management process not necessarily IT related.</td>
</tr>
<tr>
<td>IS18</td>
<td>Information Standard 18: Information Security.</td>
<td>This Queensland standard covers similar areas as 17799 and enunciates the mandatory requirements for agencies when establishing, implementing and maintaining information security within their organisation.</td>
</tr>
<tr>
<td>AS13335 -2003</td>
<td>Information Technology – Guidelines for the Management of Information Security</td>
<td>Contains five parts which give guidance on the implementation and management of information security.</td>
</tr>
</tbody>
</table>
Figure 2 AusCERT 2004 Survey - Common Information Security Related Standards
Standards such as 17799 (as shown above in Figure 2) are merely a series of checklist controls. Considering the emergence of more recent standards such as AS13335, a review of the existing use and applicability of 17799 is appropriate. An evaluation of standards needs also to consider the ways in which they are being used, to what effect, and an evaluation of the overall benefit of them in an ISMS. It will be relevant within the proposed research to look at ISMSs and to identify whether they have been developed with a standards based approach, and to identify the relationship between the management system and the use of standards within information security overall. Figure 2 provides results of a survey conducted by AusCERT indicating the most commonly used standards in Australia.

**Conclusion on Information Security Management Approaches**

The literature strongly supports the use of a structured framework or model as being beneficial to the process of information security management. An ISMS which allows all the appropriate aspects of information security to be conceptualised for management purposes is recognised as being an effective instrument for the functional operation of information security in organisations. An ISMS based on standards is accepted as supportive of the process of information security management and provides a way to ensure that all required security areas receive coverage.

There is little research, however, to suggest the existence of the widespread use of structured ISMSs based on commonly accepted standards, despite recognition of their benefits. In the cases where standards are used, Australian surveys indicate that ISMSs are based on a few main standards. However, no information is available on the use of ISMSs or the use of standards in Australian universities.

Additionally, the literature advocates that ISMSs should be operated by linking closely to an appropriate organisational context and be supported by appropriate policy. A complexity of the standards however is that while they provide a framework for operation, it is not evidently clear how these standards should be converted to policy and practical operations, and further whether attempts to do this have been effective within universities. It is important to understand that for an information security management
system to be effective, it still requires the ability to make effective management
decisions about organisational activities (Cohen, 1999). This means that even if an ISMS
is developed that reflects best practice, is based on internationally accepted standards
such as 17799, and is properly resourced, it will only be effective if it is supported by
other organisational processes.

It can be concluded that ISMSs need to be researched to understand the extent of their
use in universities, whether their application is successful, and if they are not being used,
the alternate management approach in use. The evidence of any use of standards for
ISMS operation should be included. It would be possible to determine the uptake in
these two areas and gauge the effectiveness of their use so as to develop improvement
strategies.

2.3 Security Policy

Security policy is supported in the literature as being extremely important and
fundamental to information security. Yet policy is an area that faces several challenges,
including a lack of understanding about what security policy actually is and how it
should best be used. An organisational security policy is described by Olson and
Abrams and Bailey (2001) as the ‘...set of laws, rules and practices that regulate how an
organisation manages, protects and distributes resources to achieve specified security
policy objectives….to be meaningful these laws, rules and practices must provide
individuals (with a) reasonable ability to determine whether their actions violate or
comply with the policy’.

Security policy therefore plays a strategic role in defining high level organisational
direction, as well as being specific to the practical operations for users. So policy needs
to address high level direction as well as end user guidance. One of the main goals of
information security policy, according to Hone and Eloff (2002b), is to define the rights
and responsibilities of information resource users.
Policy as a Foundation to Security Management

Higgins (1999) suggests that information security policy is a prerequisite to security management. Security policy is considered as being the foundation for applying information security within the organisation. There is a high degree of consensus overall that effective information security management is dependent on the existence and practical application of security policy (Fulford and Doherty, 2003). Implementation of security policy is noted widely in literature as having a highly significant correlation to successful information security. The relationship between effective information security policy and an effective ISMS is also established within the literature (ECAR, 2003).

According to Wood (2002) security policies are pivotal to enabling processes within the organisation. Information security policy is increasingly critical to the continued operation of information systems and, as with other aspects of strategic importance, policy needs to be addressed and driven at a high level within the organisation. The open literature evidences a growing acknowledgement and emphasis on information security within organisations (Ernst and Young 2003, AusCERT 2003). Correspondingly there has been an associated increase in the uptake of security implementation measures, including development and deployment of security policies.

Studies on security policy within universities have been rare; however studies in other large organisations have indicated several factors that provide gaps which apply to universities. Firstly, a study by Fulford and Doherty (2003) looked at the application of information security policies in large UK based organisations. They received over 208 responses after sending nearly 3000 questionnaires to senior ranking IT professionals in large UK based organisations. The research looked specifically into security policy in terms of the security policy dissemination, the coverage of information security policy and factors affecting the success of the policy. While the results indicated a high rate of policy existence (76%), it was noted that most organisations usually relied on a single mode of dissemination only. The authors suggested that a single mode of dissemination
had the potential to result in a lower level of compliance due to the fact that the information in the policies may not reach all people concerned.

The research by Fulford and Doherty noted that a general lack of academic research had been conducted into the adoption of specific areas of security policy or the impact on the organisation of those areas. Again other research including surveys conducted by Ernst and Young (2003), FBI, EDUCAUSE and the Anderson report generally concentrate on the adoption rates of security policy rather than the specifics of the areas covered (although the AusCERT survey which was originally structured on the FBI report is an exception to this). These surveys do not, however, report on the organisational impact of policy.

**Development Issues with Information Security Policy**

The issue of how organisations develop policy, whether these policies are effective and what factors are used to determine if they are successful, are areas that have had relatively little research. Maynard and Ruighaver (2002) suggest that research on security policy tends to be normative and does not indicate what is actually happening in organisations. Therefore it can be concluded that there exists a lack of extensive research on the development and successful use of security policy itself, as well as whether the security policy itself is based on particular standards or models for information security.

The development processes for policy are numerous. One development process highly focused on policy formulation is the process proposed by Bayuk (1996) which examines assets to be secured, moves to prototype documents and finally results in the drafting of policy. Another is the model put forward by Control Data (2000) which uses a ‘policy’, ‘enforcement’ and ‘assurance’ model. Both these models provide information on the process but do not necessarily provide information on how policy should be structured.

Dhillon (2001) puts forward a model for policies offering a classification as ‘individual’, ‘modular’ and ‘comprehensive’, with a description and comment on each approach.
‘Individual’ was described as being specific to individual technologies, ‘modular’ as being fairly broad but grouping technologies, and ‘comprehensive’ as being principles based and applying to all technologies as well as covering processes and people. Dhillon looks at the requirement for organisations to address security through effective security policy, and suggests that policy adoption is very low, requiring more effective approaches (this somewhat contradicts studies by Ernst and Young who suggest that adoption of policy is increasing).

The author raises a key point saying that governance over systems through security policy is a major part of security that is often left uncovered because it is not necessarily 'tangible' or 'visible', whereas aspects such as access control, authentication and accounting are. Whether policies in organisations are becoming more common or not, the literature indicates that success in the development, implementation and compliance with policies is still lacking.

Baskerville and Siponen (2002) argue that an increasing trend towards 'emergent' organisations (those organisations experiencing significant structural and IT related change) has resulted in often federated and emergent policy with little guidance on how policies should actually be developed. The authors suggest that organisational emergence recognises a theory of social organisation in which stable structures cannot be relied upon. Literature supports this by demonstrating that a large component of research on security policy has been dedicated to content as opposed to security policy development. Consequently there exists a need for research on not only the coverage of policy but also an examination of the development processes within universities.

It is worth examining models for policy development in relation to advocates of ‘meta-policy’ development and ‘abstraction and refinement’ models for policy development such as those put forward by Baskerville and Siponen (2002) and Abrams and Bailey (2001). Meta-policy is effectively a ‘policy on policies’, and provides an important framework for security policy development, as it provides guidance on traditionally difficult areas of development (i.e. structure, content, format and process). The
abstraction and refinement model effectively looks at ‘abstracting’ and ‘refining’ policy at the level that is most effective and relevant to the end user. This approach generally avoids the development of excessively long policies that are never read, and instead extracts components of policies and shapes them to a more dynamic and usable context.

Although meta-policy has been adopted by some universities, the extent of meta-policy (templates for policy) adoption and compliance levels within universities is unknown. Further, the overall applicability including the usefulness of meta-policy and its strengths and weaknesses is worthy of examination. This research project looks at the use of meta-policy in universities and examines its take-up and effectiveness. Similarly, policy is considered from the abstraction and refinement models to determine if improvements can be made.

**Implementation Issues with Information Security Policy**

Security policy plays an important function in communicating a vision of the organisation’s direction and position on information security, as well as guiding end users in their daily work. The actual implementation of security policy to users on the ground can be extremely difficult according to Hone and Eloff (2002b). Reasons for this may include the fact that the policy may not be well-communicated and promulgated to the users; it can be too long or technical, and the relationship between the security policy and users’ tasks is often not understood or is seen as needing a ‘workaround’ due to a perception of its obstructive nature. A basic assumption in information security is that policies will be referenced by users during their daily work. However, according to Wood (2000) this assumption is flawed and needs to be met by ‘dispersed information security policies’ which effectively link procedural tasks to policy statements through some means.

Although the literature strongly supports the importance and significance of policy, ineffective or incorrect application of policy is likely to dilute the process of information security and may result in information security being seen as unnecessary and unhelpful, even obstructive, and at the least not well-managed. From a management perspective it
can be easy to mistake security as the end goal; however security should be seen as an enabler of the organisation’s priorities (Luker and Petersen, 2003) rather than as the goal itself, particularly considering the general lack of awareness and less understood aspects of information security.

Information security should be provided as a service to enable the organisation’s priorities. As a service, however, it can be adversely affected by inappropriate application of security policy. This indicates that an effective development and implementation process is necessary. An effectively implemented security policy should not only indicate the required behaviour from users but should also reflect the objectives of the organisation so that users do not see it as a necessary evil (Hone and Eloff, 2002b). It should be done in a way that is relevant to the end users, be enforceable and appropriately reflect the direction of the organisation.

Security policy therefore plays a key role in providing direction for the organisation on information security. Policy needs to be linked to an associated high level management commitment which, when combined with user awareness, gives an appropriate organisational context for the implementation of, and compliance with, information security.

Although policies tend to specify how the organisation should operate, they are only relevant if they are implemented within supportive operational structures and actually complied with. To be meaningful, policies must provide individuals with an understanding of their responsibilities. Compliance completes the process.

For these reasons security policy can be a difficult process. Policy must not only reflect security objectives but a number of other factors as well which are critical to the relevance, usefulness and applicability of the policy. These include relating policy objectives to wider organisational objectives, having an appropriate development process for policy including content and structure, and encouraging compliance as well as providing mechanisms for enforcing policy. Processes for breaches of policy are also
required, for when compliance is lacking. The correct operational structure and organisational context to support the policy is therefore essential.

The overall responsibility for security policy development all too often defaults to technical administrators or security officers with insufficient authority or knowledge of the organisation’s higher objectives. This is often due to information security being seen as ‘IT Security’, instead of ‘Information Security’, a seemingly slight difference but one that differentiates between a perception of ‘it’s an IT problem’ and ‘it’s a business problem’. Policy developed under these circumstances tends to lack ownership and stakeholder collaboration, and can result in important objectives not being considered properly: particularly business goals.

Even reviews of policy by senior management can be conducted without a strong sense of ownership by the managers themselves if they are dissatisfied with the content or process used, or if they don’t see it as part of their responsibility. This situation can result in policy being developed by people not necessarily aware of, or having an understanding of, high level objectives. Yet these people are required to engage many people in the organisation to eventually implement an effective policy. Therefore what is already an arduous task is even more difficult and ineffective - and consequently, often avoided.

The traditional model for information security consists of the CIA theme (confidentiality, integrity and availability) (Rees, Bandyopadhyay and Spafford, 2002). Considering the complexity of most IT environments, however, the interpretation and applicability of this model is somewhat limited without clear instructions in the form of security policy on how CIA relates to, and impacts on, the organisation. Additionally, the use of standards in an ISMS is relatively meaningless unless compliance with these standards is facilitated by practically applicable security policy statements.

In summary, the actual writing, implementation and ultimate compliance with policy are major areas requiring further research and careful consideration for effective security
management. Accordingly, this research focuses on what areas universities are covering with policy, the process used for continued development and implementation of that policy, and the methods applied for awareness of, and compliance with the contents of that policy.

**Conclusion on Security Policy**

Fulford and Doherty (2003) in their investigation on the application of information security policies in large organisations, noted the paucity of research on security policy aside from content focused research. Nonetheless, several common themes have emerged in relation to security policy. Firstly, although the prevalence of instances of security policy appears to be increasing each year, a lack of a consistent approach to policy development and requirements definition is apparent. While processes vary, the research problem becomes one of relating a process that suits the higher education sector, including the relevance, applicability and current status of, meta-policy. Additionally, a lack of consistency in content, uptake and dissemination methods is apparent. The uptake of policy in terms of gaining top level management support and attaining compliance at all levels to policy is another major problem.

A structured process (meta-policy) may be useful to ensure requirements are met and that the ultimate content will be relevant and useful in meeting higher education organisational requirements, easily understood by end users. The need for appropriate abstraction of policy based on organisational requirements (Gaskell, 2000; Baskerville and Siponen 2002) and a corresponding lack of clear distinction between policies, procedures, standards and guidelines is also an issue that suggests meta-policy may be helpful. A relevant gap in academic research that this project includes, therefore, is in the examination of universities’ policies in the areas of coverage including existing policy content, ‘in-development’ coverage (policies currently in development), and proposed future coverage areas. The development process and dissemination methods will be examined along with apparent issues with these processes. Additionally, the impact to the organisation and the uptake of policies will be discussed.
2.4 Awareness of Information Security

Information security awareness is a state brought about primarily through initiatives resulting in activities by the organisation aimed at ensuring that both management and end users are aware of and committed to, security risk mitigation as well as policies and guidelines. By way of practical example, information security compliance is where security management wants end users to be aware of, understand and follow security policy and processes (prescriptive commitment). This is in contrast to being aware (or unaware) of policy and then failing to comply with guidelines (Siponen 2000). Siponen (2000) and Straub (1997) argue that information security awareness is considered important because information security techniques or procedures in relation to information systems can be misused, inadvertently applied incorrectly or not used at all, rendering security guidelines as less useful and effective.

There are many challenges, however, to improving information security through awareness activities. One such challenge is that firstly, awareness of the requirements for behaviour is necessary and secondly, the set of factors that interact with the user’s willingness to comply needs to be understood. This leads to a level of overall security awareness and therefore compliance that can vary substantially and, in general, is indicated by the literature as being highly challenging. It follows that compliance is difficult to obtain if awareness levels are low.

Another frustrating aspect of awareness is that its effectiveness depends on the interest of the person receiving it. Awareness activities are not particularly effective when done in the absence of an actual interest in information security (Cohen, 1999). Cohen proposes that the relevance and effectiveness of steps taken towards improving security awareness should be influenced by the receiver’s predisposition towards information security. The difficulty of awareness is supported by Figure 3, taken from AusCERT research, which indicates that changing users’ behaviour is one of the most challenging aspects of security.
Adoption Rates of Awareness Programs

Literature research indicates that effective information security awareness, either in some basic measurable fashion or as a fully developed structured program, is far from being widely implemented in organisations. A survey conducted by the ‘Educause Centre for Applied Research’ (ECAR, 2003) found that only one third of the 435 higher education institutions surveyed had a formal security awareness program. Additionally the Ernst and Young (2003) Global Information Security Survey found that only 35% of organisations surveyed had a formal information security awareness program in place, and that funding for awareness and training ranked as a low priority. In another global information survey conducted in 2002 of midsize and large firms, less than 50% of the 459 CIOs and IT Directors advised that they had a security awareness and training program in place (Kankanhalli et al., 2003).

While the survey results vary, they indicate that awareness programs are invariably low compared with the recognised need for information security. The survey results contradict the recognised need to undertake awareness activities. An ECAR report titled the ‘Fourth Annual EDUCAUSE Survey Identifies Current IT Issues’, (Caruso, 2003) and (Crawford et al., 2003), placed the need for further training and awareness activities for end users in the ‘top ten’ issues list. The results of the AusCERT 2004 survey indicate that changing users' attitudes and behaviours regarding computer security ranked as the aspects of computer security management that organisations found most challenging in 2002, 2003 and 2004. Leach (2003) cites a recent study by the ‘ISF’ (‘Information Security Culture’, The Information Security Forum, 2000) that suggests up to 80% of critical security failures are the result of end user behaviour as opposed to inadequate security technical solutions, and suggests that a well-targeted security program has the potential to reduce that figure.

The literature evidences that security awareness is an important function, yet it is under-funded, under-represented and generally applied in an ad hoc process and in a reactive manner. Security awareness is therefore highly unstructured in most organisations and can be seen as operating on a spectrum ranging from either ignoring it, or developing
and communicating basic security guidelines, all the way to administering a well-developed and highly structured information security education program.

When examining the available models for awareness, categorisation of information security awareness models has generally been associated with framework and content based systems, according to Siponen (2000). In his article, Siponen references framework based systems as being measurable by quantitative methods, and as containing ‘engineering disciplines’ such as standards, guidelines and principles of operation. Content based systems are described as being more qualitative in nature and relate to more ‘non engineering’ areas, including tacit knowledge, behavioural and motivational theories and end user persuasion theories. In either case, a substantial focus on security awareness is at the end user level.

This inherently suggests the assumption that other levels of security awareness (i.e. for system owners, high level management, system designers etc) is already at an acceptable level, however this may not necessarily be the case. To address security awareness requires developing a security culture through an effective security strategy that targets all necessary levels within the university. This necessitates targeting from students and end users, to staff and general management, academics, senior management and executive, to council, in order to address security awareness at the required layers. To effectively target this range requires understanding and addressing human factors in gaining awareness and compliance with information security policy and processes (Siponen 2000, Thomson and Von Solms 1998).

Motivational theories in relation to awareness and compliance for the use of information security systems are widely recognised by authors including Adams and Sasse (1999), Baskerville (1989), Straub et al., (1997) and Thomson and Von Solms (1998a). The recognition, however, of motivational theories to a large degree has been on a relatively abstract level and has not been used to consider the effectiveness of approaches to security awareness and compliance. Motivation is an important aspect of understanding how effective information security awareness activities are towards compliance. An
interesting study conducted by Adams and Sasse (1999) on the compromises of security in relation to password management identified a number of contributing factors. Importantly, these included insufficient communication from security sections in organisations to users, which caused users to construct their own models of reality on possible security threats and the importance of security. The study indicated the model of reality constructed by the user could be wildly inaccurate due to insufficient knowledge.

Developing a culture of compliance depends to a degree on having everyone in the organisation motivated to be compliant. Understanding how to motivate people requires understanding their current abstraction of reality, which is often constructed based on their knowledge of the area. In terms of the user being motivated, the study noted the requirement to align security information and mechanisms with work practices and noted that user motivation increased in association with an increase in their knowledge of the rationale for security behaviours. An interesting aspect of this study was the conclusion that because security originated from a military perspective, an authoritative ‘need to know’ principle still existed in relation to users. This, in turn, discouraged security people from informing users, and ultimately led users to construct their own reality. This caused security people to view users as inherently insecure, and users to view security people as obstructionist in mechanisms deployed, creating a vicious cycle. Therefore, understanding people’s motivation and deconstructing any false sense of realities towards information security is a useful exercise when undertaking awareness activities.

The focus within this research is to identify the activities that are being undertaken for awareness development, and to identify at what levels within the organisation these are being undertaken. The issues that exist with this process are examined as well as recommendations for improving awareness throughout the university community.
Conclusions on Security Awareness

It can be concluded from the research that information security awareness is considered an important mechanism for improving information security management. Surveys indicate that security awareness programs, despite their acknowledged significance, are generally instituted in less than 35% of organisations. Unfortunately, focus and prioritisation on awareness activities tends to be ignored and under-funded, despite the links between increased awareness and compliance.

In undertaking awareness as an activity, various constructs exist for models of awareness programs, and it is worth examining the human element in the design and application of any model. Because IT serves as a tool for people it is therefore people’s motivation that affects the use of those tools. Understanding basic human motivation is likely to increase the chances that the application of an awareness program may lead to improved compliance. Motivation in universities can vary greatly due to the variety of situations that exist. An important aspect is looking at what is working and what is not in universities, and identifying the problem areas so as to understand solutions.

Aspiring to instil a ‘culture of compliance’ in universities that embodies a balance between prescriptive and descriptive behaviours is seen as desirable. Although a link exists between awareness and compliance, it is not well-understood how awareness is being achieved in universities, including the awareness activities undertaken, nor how compliance levels are achieved or affected by awareness programs.

The relevant areas of research include identifying the universities that have awareness programs, the approach taken, how successful they are, and understanding the influencing factors relevant in both developing and implementing an awareness program.
2.5 Compliance with Security

A theme relating to awareness involves the concept of instilling into the organisation a ‘culture of compliance’ towards information security (Furnell et al., 2000). The idea behind this is that the culture of the organisation, which includes its values and norms of behaviour, including descriptive and prescriptive behaviour, its overarching policies, and higher level management support, results in a ‘culture of compliance’. An organisation with this type of culture has a level of compliance that is not only demonstrated from ‘the top’, but includes norms for security guidelines and practices that are invariably followed by all in the organisation.

A culture of compliance in this case, would include an awareness of, followed by compliance with, information security policies, processes and guidelines, as part of its norms, values and culture. Compliance in this research is based on the relationship between the university’s security posture and, consequently, the policy security requirements and levels of compliance reflected at all levels of the university community through a ‘culture of compliance’.

Research by Gartner and AMR (Haldar and Forsyth, 2004) conclude that many enterprises remain inadequately protected from security threats because of the perceived high cost of an effective security strategy that suits the organisation’s culture. The lack of focus on security strategy has led to an emphasis on products and technologies instead of a security strategy that incorporates security awareness, training, and policy and standards in an effort to develop a ‘culture of compliance’ towards information security. An effective commitment to security requires that a process be in place that suits the culture of the organisation (Spurling, 1995; Leach 2003). When looking at the culture of an organisation, it is understanding the problem of gaining compliance with security as opposed to determining practical examples of increasing awareness that would appear to be least understood in terms of applicable research.

Understanding the factors that add to compliance within this environment is multifaceted. The university environment contains a mix of corporate culture and
traditional academic freedoms. It is not uncommon for information security to be seen by individuals or groups within the university environment as disabling rather than enabling. Usually the negative aspects held by users in relation to information security should decrease as awareness increases, but this is not always the case.

According to Dickie (1996) security tends to be a transparent process when it is operating effectively so is often unnoticed when things are running smoothly. Because information security tends to be intangible, a general lack of awareness and understanding can easily develop. This can make the purpose of information security less convincing, leading to the question ‘why should any attention be paid to information security?’ This can result in a lack of ownership. Ownership and responsibility must be accepted, however, not just by one person, but must be embraced by the organisation.

Dickie (1996) asserts that information security is a management responsibility and forms one of the internal control systems monitored and reviewed by audit. Information security compliance, however, is not just a matter of applying controls and procedures. The potential conflicts between various stakeholders within universities preclude such a simple approach. A tension exists between those who want to provide open access to information, those who want to protect information, and those who require privacy of information yet expect information to be shared. The balance between transparency and privacy of information continues to be a challenge requiring a comprehensive organisational specific approach.

Additionally, when the work practices of the organisation are threatened, unless there is an understanding of the clear and present requirement for change, resistance will follow. An effective security program or strategy that introduces changes in a managed way, taking into account the conflict between security requirements and working practices, is necessary (Gaunt, 2000). Other factors that can reduce the potential for developing a culture of compliance include a lack of information security process in human resource recruitment and training, non acceptance of the importance of information security education and training, ignorance, the attitude of users, the conflicting demands of users,
the inadequacy of systems and inconsistently applied policies and procedures (Gaunt, 2000).

In the Educause book, ‘Computer Network Security in Higher Education’, Luker and Petersen (2003) discuss the principals of academic freedom in relation to strategies employable by universities for successful information security awareness and compliance. They note the difficulties and challenges in this area. Luker and Petersen suggest that achieving an acceptable security strategy can often result in conflict and challenges to achieving a balance between information security and the survival of academic freedom or ingrained work practices. Achieving a culture of compliance is a goal recognised therefore as being difficult to achieve in the higher education sector. It is necessary to carefully balance work practices with security control to make any headway.
What aspects of computer security management does your organisation find most challenging or problematic?

<table>
<thead>
<tr>
<th>Issue</th>
<th>2004</th>
<th>2003</th>
<th>2002</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insufficient support or commitment by senior management to address information security issues</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>Lack of senior management understanding of information security issues</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>Changing personnel (users) attitudes and behaviour regarding computer security practices</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>Accurately prioritising information security against other business needs</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>Applying risk management principles</td>
<td>0%</td>
<td>19%</td>
<td>19%</td>
</tr>
<tr>
<td>Keeping up to date with changes in technology</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>Keeping up to date with computer threats and vulnerabilities</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>Responding appropriately and in a timely manner to computer security incidents</td>
<td>0%</td>
<td>30%</td>
<td>20%</td>
</tr>
<tr>
<td>Configuration management</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>None, organisation is managing all computer security issues reasonably well</td>
<td>5%</td>
<td>11%</td>
<td>11%</td>
</tr>
<tr>
<td>Other</td>
<td>4%</td>
<td>4%</td>
<td>0%</td>
</tr>
</tbody>
</table>

Figure 3 AusCERT Survey 2004 Challenged Computer Security Management Issues
Conclusions on Security Compliance

It can be concluded from the research that improving the level of compliance in the organisation should be based on developing a culture of compliance. This should be achieved through developing an effective information security strategy that targets all levels of the organisation, which aims to bring information security to the level of corporate governance.

Compliance in information security needs to be based on a balance between corporate security needs and yet remain supportive of academic requirements and work practices. The concept of creating a ‘culture of compliance’ within the university community is a central point and is likely to be improved when the rationale for security requirements is understood.

This research focuses on understanding what measures are taken to achieve a culture of compliance within universities, what issues or influencing factors exist as a result, and how a culture of compliance in universities could be further developed.

2.6 Conclusion on Literature Review

This review on literature has explored four key areas of information security. This included an analysis of Information Security Management Systems (ISMSs) as an effective management approach, an exploration of the importance of policy and issues related to content, development and implementation, a contrast of the importance of security awareness against the lack of awareness activities generally undertaken, and finally, an investigation of the concept of creating a culture of compliance towards information security.

In recognising that universities rely heavily on information, they also rely on information security to protect that information. Thus these key areas play a significant role in helping understand effective information security management within universities. The areas that have been explored are all key to understanding existing
issues with information security management in universities. These areas are also strategic for recommending improvements in information security management.

Although the need for information security is acknowledged and considered important, in many cases security is not prioritised in line with its accepted importance. This is reflected by a lack of commitment, inadequate funding and a general lack of understanding by top management due to several factors. These include a lack of awareness of information security issues, a lack of effective security management governance, a reactive approach generally and importantly, difficulties in the impacts on users regarding their work practices. Additionally, the fact that top management has not incorporated information security as part of corporate governance impedes the resources and prioritisation towards information security. This in turn affects how much effort is put towards raising awareness and ensuring compliance, leading to less recognition overall.

The literature studied to date offers insights into these problems, the possible reasons for them and offers suggestions that have the potential to be further articulated and expanded to improve information security management at Australian universities. What is required from here is to continue searching out additional literature, conduct the investigations at the university level, gain a greater understanding of the issues at hand and develop commensurate strategies for improvement.
3 Methods

This section provides a description of the research methodology, beginning with a high level overview followed by a detailed description of the methods used for data generation, data sources and data analysis.

3.1 Research Design

Overview of Methods

The research applied a qualitative method to undertake an exploratory investigation of information security management in Australian universities. The intention was to explore the current status, existing issues and to identify ways to improve current security management approaches. The methodology approach conformed broadly to thematic qualitative methods recommended by Miles and Huberman (1994). For robustness, the approach was also referenced against other qualitative research recommendations found in the literature. This included qualitative methods and recommendations offered by Coffey and Atkinson (1996), Marshall and Rossman (1999), Mason (2002), O’Leary (2004), Patton (1990) and Ritchie and Lewis (2003).

The main data source, a survey instrument, was developed, piloted and then administered to all 38 Australian Vice Chancellor listed universities (constituting a 100% participation rate). The survey included structured and semi-structured closed and open ended questions. The questions were broadly categorised in several areas for the purpose of facilitating discussion to gather data on the following research questions:

1) What is the current status of information security management practices in the Australian university sector?

2) What are the key issues and influencing factors surrounding the effectiveness of information security management practices?

3) How could improvements in information security management be achieved?
The interview participants included either the university IT Director or equivalent and/or the IT Security Manager or equivalent. This provided input from the perspective of a senior manager’s position within IT. It also provided for a compare and contrast from the ‘front line’ security practitioner. The interviews were conducted over the telephone and digitally recorded for future downloading to a personal computer and transcription. The transcribed interviews produced over 70 000 words of text. After generating the text, responses for each question were grouped to facilitate a rich data set for analysis. Data analysis was performed on the interview transcripts using qualitative methods that conformed broadly to thematic qualitative data analysis methods as recommended in the literature (Coffey and Atkinson (1996), Marshall and Rossman (1999), Mason (2002), Miles and Huberman (1994), O’Leary (2004), Patton (1990), Ritchie and Lewis (2003)).

As part of the analysis process, the interview transcripts were coded using the Atlas.ti qualitative analysis software. This allowed the initial stages of data reduction to occur by way of assigning codes to phrases and commonly recurring themes. The process of data display was then used to graphically represent coded network relationships. These were further subjected to thematic analyses for patterns, connectedness and relationships. This then gave way to inductively elaborating several key generalisations which progressed to a theoretical construct by way of proposing the security practitioner’s management model (Figure 1).

The security practitioner’s model represents the synthesised findings of the research project. The model was developed and underpinned by not only a structured approach to data generation and analysis, but also by the findings of the study referenced against extant research literature and theory. This specifically includes enterprise security architecture models recommended by Kelley and Moritz (2006), Sherwood (2003), Stephenson (2005) and Zachman (1987). Additionally, behavioural theory including Self Determination Theory, motivational theory and Technology Acceptance Model was referenced in the model based on work by Detert et al., (2000), Siponen (2000), Ryan and Deci (2000) and Yin (2003).
Credibility and Validity of Methods

The researcher took great care to ensure that the research methodology would robustly stand up to tests of credibility and validity. In this section a summary is provided which lists three main areas identified as important and which are addressed in relation to credibility and validity (Patton, 1990). A discussion on the methodology follows which provides the higher level framework as well as detail on procedures and techniques used.

1) The researcher’s qualifications, skills and experience in relation to the research project - The researcher has previously completed an Associate Diploma in Information Technology and a Bachelor of Management and Professional Studies, as well as a unit at QUT in Research Methodologies. During this course work, a wide variety of units was covered, including information technology subjects, management subjects, behavioural, sociology and psychology subjects, change management, leadership and planning based subjects. The researcher has also undertaken a wide variety of employment-based IT and management oriented short industry courses. These include computing, networking and security related courses, as well as project management, planning, communicating and management courses.

The researcher has approximately sixteen years experience in the IT industry, over ten years of which are in the university IT environment, with five years of information security experience. Additionally the researcher has experience in the management of large projects across diverse areas of IT. These include high level networking projects, PABX, video over IP, security, Internet accounting and broadband technologies.

The researcher’s role as an instrument in this research also displays many of the qualities ascribed to by Miles and Huberman (1994) as desirable including familiarity with the phenomena under study, strong conceptual interests, a multi-disciplinary approach, and good investigative skills.
2) The researcher’s paradigm orientation and assumptions that underpin the study in terms of philosophical beliefs and views on knowledge - these orientations are covered in detail later in this section. In essence the researcher has endeavoured to be fully aware of mindset paradigms in relation to philosophical beliefs and epistemological perspectives that could have influenced either the data generation or data analysis processes. These outlooks have provided perhaps greater depth to the study by allowing the researcher to be cognisant of the interdependencies between facts of the study and preconceived notions or perceptions within study related matter.

3) The specific lower level methods, techniques and procedures used to undertake the research in an effort to ensure the integrity, validity and accuracy of the findings and interpretation of those findings - the methods, techniques and procedures are covered in great detail later in this section. An approach was adopted and documented that conformed to thematic-based qualitative research using a post positivist and inductive stance. Data collection and analysis were robustly tested for accuracy, consistency and validity. This included gaining initial feedback from participants on data analysis via a key findings report, triangulation methods, and cross testing analysis of findings against other data sources including the literature.

**Research Framework**

Although qualitative research was used in the project, it is recognised that qualitative research is a subjective area. To improve the process used for the research project, a research framework was adopted to ensure structure, credibility and validity (Figure 4). This framework provides for the maintenance of a critique of traditional social science balanced by a contemporary challenge of historic assumptions of neutrality in inquiry. Additionally this diagram provides a ‘hierarchy’ aimed at clarifying the methodology used, from high-level genres to lower-level procedures. In presenting a discussion on methodology, the researcher firmly believes that locating the methodology within these higher to lower level perspectives is beneficial for both the researcher and for readers to gain an overall context to the study. This ensured that the research was located in a higher-level research genre from an ontological and epistemological perspective.
Figure 4  Research Methodology Framework
The researcher’s framework provides a diagrammatic representation of the methodology used and importantly acknowledges Marshall and Rossman (1999), who argue that all research is interpretive and is fundamentally guided by beliefs and feelings about the world and how it should be understood and studied. Providing the context to this research project is, therefore, enhanced by stating the researcher’s perspectives about the world and about knowledge itself.

**Ontological and Epistemological Position**

Identifying both the ontological perspective as well as the epistemological context ensures that the overall approach, methodology and process allows for scrutiny to ensure both validity and relative objectivity. Importantly, describing the broad approach as well as the specific methodology should allow another researcher to potentially replicate the methodology and to find similar results, or at least to understand its derivation - an important aspect to attune to the qualitative process. The ontological and epistemological stance therefore provides a higher level context for understanding the selected qualitative research methodology and provides the ‘philosophy’ of the approach, whilst the lower level procedure and process are designed to provide a level of transparency and examination to implementation of the approach.

A generally accepted range of ontological approaches reflects a continuum of the idea of ways in which one can view the concept of reality in our lives. The range of approaches includes realism which suggests the idea that facts are out there just waiting to be discovered, empiricism which supports the idea that one can observe the world and then evaluate those observations in relation to facts, and positivism which focuses on the observations themselves with the focus more on ideas about facts than facts themselves. Lastly postmodernism embraces the concept that facts are fluid and elusive, so that we should focus *only* on our observational claims. This last approach is interesting because it links loosely into contemporary thinking on areas such as string theory and modern quantum physics, both of which investigate differing potential of realities. Again the researcher strives for balance and relates to the notion that although facts exist (an
ontological perspective of realism), reality ultimately needs to be interpreted and defined to have any meaning (an ontological perspective of postmodernism).

The researcher’s epistemological perspective is a balance between empiricism and foundationalism. These two theories constitute a stance that fundamentally supports the idea that knowledge needs to consist of both a statement of what is thought to be true, plus the belief that it is true, and for it to be scientifically validated as much as possible.

**Qualitative Exploratory Method**

Qualitative methods are particularly well-suited to exploration and inductive logic according to Patton (1990). The exploratory and descriptive nature of the research confirms the importance of the context to which a qualitative research method is appropriate (Marshall and Rossman, 1999). A qualitative design often unfolds as the study progresses and is partially emergent as the study itself unfolds (Patton, 1990).

Marshall and Rossman (1999) identify the types of research to which a qualitative approach is suited, many of which are directly relevant and apply to this research project. The characteristics of qualitative research as well as situational applicability as defined by Marshall and Rossman (1999) are described in Table 2.

The researcher contends that understanding the research problem involved understanding people’s thoughts, feelings and perceptions, whereby the researcher needed to capture these intricacies in a real-world setting. The research involved primarily exploratory approaches that took place in a real-world setting, denoting the use of a qualitative approach according to Marshall and Rossman (1999). Marshall and Rossman (1999) further describe the qualitative researcher as someone who:

- views social phenomena holistically,
- systematically reflects on who they are in relation to the inquiry,
- is sensitive to the personal biography and how it shapes the study, and
- uses complex reasoning that is multifaceted and iterative.
Table 2 Characteristics of Qualitative Research and Applicability to Project

<table>
<thead>
<tr>
<th>Characteristic of Qualitative Research</th>
<th>Applicability in This Research Project</th>
</tr>
</thead>
<tbody>
<tr>
<td>Takes place in the natural world.</td>
<td>Took place in the natural setting of the Australian University environment.</td>
</tr>
<tr>
<td>Uses multiple methods that are interactive and humanistic.</td>
<td>A combination of survey instrument, literature review, observation and peer discussion was used to integrate results.</td>
</tr>
<tr>
<td>Emergent rather than tightly prefigured.</td>
<td>The conceptual model was emergent and stemmed from thematic pattern development and theory building.</td>
</tr>
<tr>
<td>Fundamentally interpretive.</td>
<td>The research used a post-positivist, interpretive method to balance traditional logical positivism.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Situational Use of Qualitative Research</th>
<th>Applicability in This Research Project</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delves in depth in complexities and processes.</td>
<td>The complexities between behaviour, process and technology were considered.</td>
</tr>
<tr>
<td>Seeks to explore where and why policy and local knowledge and practice are at odds.</td>
<td>A primary aim of the research was to understand existing status and practice and to develop strategies for improvement based on findings.</td>
</tr>
<tr>
<td>Relates to information and unstructured linkages and processes in organisations.</td>
<td>The information gathered through the survey instrument was a relatively open based discussion and focused on existing status, process and issues.</td>
</tr>
</tbody>
</table>
Marshall and Rossman (1999) contend that a wide range of qualitative research genres exist, with many different texts serving as guides to their respective assumptions and approaches. In an effort to help locate an overall approach, the researcher explored Marshalls and Rossman’s (1999) analysis of over 20 different typologies of qualitative research, across three major genres. The main genres proposed by Marshalls and Rossman (1999) include (a) a focus on individual lived experience exemplified by mainly phenomenological approaches, (b) a focus on society and culture as seen in ethnography and qualitative sociology and (c) a focus on language and communication expressed by sociolinguistic and semiotic approaches. The research project very broadly fits into the qualitative research genre of (a) a focus on individual lived experience exemplified by phenomenological approaches.

The rationale for the qualitative research method applied to the project is therefore grounded firmly in recognition and actual application of this method to the specific context of the phenomena studied.

**Post Positivist, Inductive-Interpretive Method**

A qualitative approach based on a post positivist and interpretive method was selected as being appropriate. Within the qualitative method, post positivism describes the research approach most appropriately, given the study of phenomena within a loosely prescribed structure and use of a relatively inductive method. O’Leary (2004) suggests that, where methods are often inductive, the process moves from specific observations to broader generalisations and theories. In bringing further structure to this vividly loose and inductive approach, the research strongly leverages off the methodology put forward largely by Miles and Huberman (1994).

**Structured Data Generation and Data Analysis**

In order for the interpretive and therefore potentially highly subjective stance to be validated, the researcher made a serious effort to incorporate an acknowledged and accepted structure to ensure credibility in the overall process. A methodology was selected that would not unnecessarily constrain the explorative nature of the project, yet
would enhance the objectivity and creativity with which results could be interpreted, support the phenomena explained and finally justify meaning given between relationships.

Within this approach, systematic and rigorous methods were adopted. The main protocols used were those recommended by Miles and Huberman (1994) in relation to thematic qualitative analysis. Having this structured approach further facilitated the credibility of the research project, as it was recognised that while the context-specific nature of the research project may not lend itself to exact reproducibility, research should be verifiable through full and transparent explication of method (O’Leary, 2004).

Yin (2003) contends that data analysis consists of examining, categorising, tabulating, or otherwise recombining the evidence to address the initial proposition of study. The process for data analysis therefore required careful assessment of data to move beyond any pre-existing cognitions or rationalisations regarding certain outcomes to improve on the accuracy and validity of findings. The essential protocols recommended by Yin (2003) adopted for data generation and later analysis included:

1) triangulation of information, whereby multiple sources were used,
2) maintaining a record of information sources,
3) maintaining a chain of evidence (used to help develop theoretical constructs).

Structure was also brought about to data generation and data analysis through a number of practical applications. Part of this process was validation through triangulation. Yin (2003) promotes the concept of triangulation of information to increase the validity of the information that is being collected for analysis. This is integral to ensuring that as many viewpoints are considered, as the data collection and analysis methods can often hide details. Triangulation of information helped reinforce construct validity and the researcher used triangulation of information to gather data from multiple sources to strengthen research findings and recommendations.
The role and applicability of the survey instrument itself was carefully considered as the primary tool to gather data, supplemented by analysis of documentation and observation. The areas of data collection closely corresponded with the main focus of the research aims, objectives and specific questions. Stringent coding and data analysis methods were used to generate theoretical constructs which were later synthesised into the security practitioner’s management model.

Summary of Methods

The research project adopted a qualitative research model with a methodological discourse involving a broad approach to the study of phenomena. This broad approach is reflected through a pragmatic, inductive and interpretive method based in a natural setting (the university environment), and enhanced through an attempt to capture and define people’s experiences (Marshall and Rossman, 1999). Data generation was achieved primarily through a rigorously tested survey instrument which captured a large amount of data from the real-world setting and was triangulated against other data sources. Data analysis was thematic in nature and evolved to allow emergent themes to develop into theoretical constructs. These theoretical constructs ultimately combined to form the proposed security practitioner’s management model – a synthesised representation of the findings of the study.

3.2 Data Generation

Data Collection

Activities associated with the collection of data were intended to facilitate the collection of information relevant to the research questions. The main data collection tools included a survey instrument, analysis of documentation (written material), and observation in the real-world setting of IT security at Southern Cross University.

The use of a survey instrument was therefore applied in interviews as it suited the loosely structured, emergent theme inductive to gathering data (Miles and Huberman,
1994). Mason (2002) describes the processes of qualitative interviewing as referring to in-depth, semi-structured or loosely structured forms of interviewing. Miles and Huberman (1994) also make a case for an approach that could involve either a tight, pre-structured qualitative design or a loose, emergent one. Taking these theories into account, the survey instrument used qualitative interviewing and was designed to achieve a balance between tight structure and loosely emergent approaches.

The research questions started out as general but became more specific as clarity of the study emerged. This approach is acceptable if the research questions are associated with an inductive model (Miles and Huberman, 1994). In the early stages some information was known conceptually about the phenomena but was not necessarily enough to house a theory or framework in the early stages (Miles and Huberman, 1994). The researcher had some initial ideas about how to gather the information – through interviews, observations and documentation collection. Thus the researcher recognised that some identifiable parts of the research were not well-understood but knew where to look for these things (Miles and Huberman, 1994).

Although the research questions were formulated prior to the complete development of the security practitioner’s management model, initially the research project began with some orientating constructs. From here an extraction of the questions to be used for the survey occurred, then matching the questions against an appropriate sampling methodology was undertaken. This process helped form a basic framework involving a set of questions using a survey instrument, and some ideas about how and where to collect data (directly through interviews in universities).

This emergent approach is noted as being useful for particularly complex social realities and can be compared to the concept of starting with a preconceived conceptual framework and attempting to prove or disprove the theory behind this framework (Miles and Huberman, 1994). In this case the approach was relevant to the emerging and inductive development of the security practitioner’s management model. In culmination, the process led to a decision to begin to sample a survey instrument as the
primary method and collect data via two secondary methods. This is explained in more
detail in the next section on data sources.

Data Sources

On a practical level, the research involved administration of a survey instrument to all
Australian universities, together with additional data gathered through observation,
documentation and discussion. In particular this latter data gathering occurred on site
through the researcher as an instrument in the capacity of Information Security Manager
at Southern Cross University. The survey, together with ‘hands on’ practical experience
and observation, provided a consistent and objective snapshot of the current status of
information security, reinforced through depth of insight via the literature and
observation of phenomena in the sector. The data collection method therefore involved
one primary data source and two secondary sources. These three sources constitute the
main data collection sources described by Marshall and Rossman (1999) that are used in
qualitative research. The application of these data sources relates to the research project
as:

1) Survey Instrument – this was the primary data source involving a pre-arranged
interview administered to all 38 Australian universities.

2) Participation and Observation – this was a secondary data source as a result of the
researcher being a participant in the university setting in the role of Information Security
Manager.

3) Analysing Documentation and Other Material – this was also a secondary data
source and included an extensive amount of material internally and externally to the
university setting.

In-depth interviews are a main method of data collection in qualitative research and are
considered to be valuable in part due to their ability to contribute to structure whilst
retaining the power of flexibility (Ritchie and Lewis, 2003). This flexibility can be
useful to gain insight into phenomena. For the purposes of this research interviews were
used as they allowed direct conversation with the participants to get a ‘behind the scenes’ look at what was occurring. An interpretive approach such as used within this research project often sees people as the primary data source and seeks their perceptions as to what they see as the ‘insider view’, with interviews commonly used (Mason, 2002). In this way interviews can be considered a controlled ‘conversation’.

Secondary data sources were also used as they are increasingly considered important in qualitative research data (Ritchie and Lewis, 2003). The role of secondary data was essentially used to supplement the primary data as it provided a new perspective to existing primary data and formed a base for comparison (Ritchie and Lewis, 2003). Secondary data sources in this research project included participation and observation in the university environment and analysing documentation and other material available.

**Sampling Strategy**

The research leverages off previous work by Miles and Huberman (1994), who provide a typology of sampling strategies in qualitative theory, including **opportunistic**, **snowball or chain**, and **intensity** sampling strategies, all of which benefit inductive, theory building analysis. The sampling strategy builds on these theories in support of the inductive nature of the study. The sampling strategy used in the study is described using the sampling parameters suggested by Miles and Huberman (1994) which include the **setting**, **actors**, **events and processes**. Actual data collection within the sampling strategy is described using the concepts of focusing and bounding the data (Miles and Huberman, 1994). In order to describe the context of the study under a common framework, a sampling strategy for the study consisting of the parameters of ‘Setting, Actors, Events and Processes’ as suggested by Miles and Huberman (1994) was used:

**Setting**

The research was site specific (Marshall and Rossman, 1999) for this study involving Australian universities as the setting. Specifically each of the 38 Australian Vice Chancellor Committee (AVCC) listed universities was selected with the setting focusing on the central IT area. An important aspect of the setting was the researcher as an
instrument within the research design (i.e. the researcher holding the role as Information Security Program Manager at Southern Cross University); therefore Southern Cross University was also one of the focuses of the study. All other universities were focused on through the administration of the survey instrument, although additional informal contact and observation with other universities also contributed to an understanding of the phenomena under the study. This occurred through activities such as peer interactions at conferences such as AusCERT, university workshops on IT related areas, and broader discussion through electronic security forums.

The study builds on theory provided by Marshall and Rossman (1999) to include attributes that validate the setting used in the study. The choice to select universities as the setting was logically linked to both the construct of the study and the phenomena being studied. In theory it may have been possible to case study just Southern Cross University. From there it may have been possible to inductively generalise and theorise on other universities.

However increased robustness and credibility was achieved by administering interviews via the survey instrument to all universities. This was then supplemented with an ongoing and specific focus at Southern Cross University in order to enrich and include more meaningful data collected from a diverse range of settings. Supporting the selection of the universities themselves as settings, Marshall and Rossman (1999) provide four attributes that contribute to the choice of the setting being realistic in this study:

1) **Entry is possible** – in this case, as the researcher was both an instrument to the research and also a current practitioner of security in an existing Australian university, access was enabled to other universities, albeit primarily via telephone to participants. Entry to Southern Cross University was already in place, due to the researcher holding the position of Information Security Program Manager.
2) **There is a high probability that a rich mix of the processes, people, programs, interactions and structures of interest are present** – the survey instrument was used directly within the environment under study, and the role of the researcher as a practitioner of security in a university setting ensured a high availability of, and exposure to, the phenomena under study.

3) **The researcher is likely to be able to build trusting relationships with the participants in the study** – a combination of the ethical clearance process, a peer role, and the formal role of security practitioner ensured a level of credibility was established with participants, as well as already existing in the setting at Southern Cross University. Due to the level of confidentiality of the study material itself (i.e. the relative security of universities under management), the researcher’s ethical clearance and acknowledgement of respect for this situation further contributed to a position of trust.

4) **Data quality and credibility of the study are reasonably assured** – the study rigorously identified and adapted both respected and recommended qualitative research principles from several sources. This included but was not limited to the authors ‘Miles and Huberman’ and ‘Marshall and Rossman’, to ensure the entire design of the study was both valid and credible. This is covered in detail in Section 3 ‘Methods’ of the thesis. The research principles related to the data quality. Credibility also extends to obtaining a balance between bounding the collection of data (Miles and Huberman, 1994) and ensuring that sampling includes reasonable variation in the phenomena, settings and people under study (Marhsall and Rossman, 1999).

**Actors**

The actors in the study consisted of the IT Director or equivalent and the IT Security Coordinator or equivalent. The participants targeted for the survey were selected as either the person charged with the responsibility for coordination of information security (i.e. the Information Security Manager, Coordinator, Officer or similar), or the Director of IT (or equivalent). In some cases, both the security coordinator and IT Director
participated in the survey interview, whereas in other cases either the security coordinator or IT Director participated.

The benefit in having a variation in the actors is supported by Marshall and Rossman (1999) who contend that variation assists in ensuring that the ‘universe and all its variables’ are reasonably covered within the scope of the setting and actors. In practical terms, having cross participation between security coordinators and IT Directors meant that a divergence of organisational and technical perspectives were offered. Based on their higher level organisational understanding, knowledge and awareness, the IT Directors were able to substantiate links within organisational processes, explaining the ‘why’ of events, whereas the security coordinators tended to focus predominantly on the ‘what’ of events that occurred.

Within the setting at Southern Cross University, the actors were the researcher as the instrument, followed by the IT staff involved in the process of IT and security, and this included security contact with various levels of other staff internal and external to the IT department, as well as some student contact.

**Events and Processes**

The events and processes link tightly to the idea of instrumentation (Miles and Huberman, 1994) from the perspective that the researcher, as an instrument, needed to capture information on areas that were key to the fundamental processes of information security management. The key areas of senior management involvement, the management approach, security policy, awareness and compliance were identified as appropriate to encompass headings on which to base a series of questions. Each of these areas was highly variable in terms of its impact on effective management, but was expected to contribute either positively or negatively to overall effectiveness. From this viewpoint they were therefore important areas to explore in order to understand issues and phenomena associated with information security management.
Senior management was explored from the perspective of understanding to what extent senior management understood security, were involved in processes, direction or high level decisions surrounding security, and whether senior management considered security as important or a priority. The security management approach was explored in an attempt to qualify how security management was being addressed, the extent to which ad hoc or structured approaches were being applied, whether standards or some other type of best-practice frameworks were in use, and overall whether the adopted approach was effective. Additionally, how improvements could be introduced was an essential aspect of this area.

Security policy involved understanding the process for both developing and implementing policy, whether this was effective, and why. Following security policy, awareness levels and the attempts to improve awareness were examined. The area of compliance involved a range of questions designed to gather information on indicators and levels of compliance, including the culture of compliance, technology in use, funding available, and how compliance could be improved. The sources of data collection were:

**Survey Instrument**

Information security research is recognised as one of the most intrusive types of organisational research, and there is often mistrust or a reluctance to provide any ‘outsider’ information about the status and actions of security. Due to the perceived difficulties in extracting information of this nature by mail from universities when attempting to collect data of a sensitive nature (Kotulic and Clark, 2004), it was decided to use a survey and interview process.

The interviewing method was thus used to collect qualitative data for the purposes of thematic analysis based on an analysis of words, concepts and literary devices (O’Leary, 2004). Ritchie and Lewis (2003) consider that very complex systems, processes or experiences are generally best addressed through in-depth interviews because of the depth of focus and the opportunity for clarification and detailed understanding.
survey instrument was selected as it was considered appropriate in order to obtain detailed information and get an ‘inside track’ on what issues were really occurring in Universities. The survey instrument and associated in-depth interviews therefore constituted the main data collection method.

The survey instrument was designed after reviewing as many other survey instruments on information security that the researcher could find. This included a review of well-recognised, annually based security surveys such as those produced by AusCERT, the CIS/FBI surveys, the Ernst and Young Global surveys, the Anderson survey, Price Waterhouse and Cooper surveys, the International Information Systems Security Certification Consortium (ISC²) surveys, the Information Systems Security Association, Deloitte, Touche and Tohmatsu global surveys and various surveys conducted by Educause. An analysis of these surveys found that they were mostly quantitative and tended to be normative in nature, stating what was deployed or maintained in the organisation. These surveys did not reveal the why of what was occurring.

The survey instrument was designed on a qualitative basis to allow organised interviews to be conducted by including a range of open and closed questions. The structure for the questions included the use of both semi-open and open questions and a Likert four point bipolar scaling method used as a force choice method. The survey instrument contained a range of questions covering broad based areas, which for the purpose of the survey instrument were categorised into areas within security. These areas included questions on senior management involvement, the management approach taken for security, security policy, questions on security awareness levels and processes, and a mixture of questions contained under an area entitled ‘compliance’ to measure status.

Initially the survey instrument was developed and feedback from a review by the researcher’s supervisors indicated that commitment to the survey would be problematic due to its length. The survey initially involved approximately sixty questions, and was estimated to take one hour to complete. This potentially onerous survey instrument was considered unlikely to result in full participation which was an aim of the project. As a
result the survey instrument was scaled back in both the number of questions and the estimated time taken for administration.

After a second review, the survey was initially conducted in a pilot test in four universities. This provided an ideal test of the survey and valuable feedback was gained from the pilot participants in terms of suggestions and expressed interest in the research itself. Subsequent to the pilot test, the survey was further rationalised, with steps taken to eliminate redundancies and ambiguity, increase flow and order, and ensure that the instrument was well-structured. The survey instrument was then administered to all 38 listed Australian Vice Chancellor Committee (AVCC) Australian universities.

This process was achieved through gaining ethical clearance status for the project through QUT, and subsequently distributing an ‘information pack’ including the survey instrument to the universities. The Executive of the Council of Australian Directors of IT (CAUDIT) assisted in this process by contacting all university Directors of IT through the CAUDIT email forum, with an invitation to participate. At first a total of 17 universities responded to the invitation. The researcher persisted with contacting the remaining 21 universities over a period to confirm their willingness to participate. Ultimately all 38 universities agreed to participate in the survey, representing a 100% participation rate which was an extremely satisfying result.

The surveys were administered via telephone, except for two which were responded to in writing. Prior to the interview, the objectives and confidentially aspects of the interview were described. The telephone interview was recorded with the consent of the interviewee using a digital recorder, and the audio files downloaded to a PC for future transcription into a text editor. The process of transcribing the interviews involved writing out verbatim each and every conversation by using the interview template and writing the responses against each question. This process produced over 70 000 words of very rich data for analysis through a qualitative data coding and analysis process.
Participation and Observation

The researcher’s role as an instrument in this study was fundamental to the data collection method. The role of the researcher involved both being a participant and an observer of phenomena and other participants, as well as being able to read available documentation and material available in general on security.

This was achieved primarily in the workplace setting, in lieu of the researcher’s role as Information Security Manager at Southern Cross University. However participation and observation was also achieved in other settings, including security conferences, presentations, workshops and training seminars. The data collection process included making notes and defining key distinctions along the way. Miles and Huberman (1994) support the process of this style of data collection as essential techniques for qualitative analysis, as notes not only record data but also allow important pieces of information to be tied together into a meaningful structure and support abstract thinking.

Analysing Documentation and Other Material

The range of documentation and material included information found in the literature, data gathered during active participation in three higher education based information security email forums (one in Australia and two based in the United States), research conducted on the Internet, various whitepapers and reports, as well as industry conference and workshop distributed materials. This type of material contributed significantly to reflective thinking and assisted in the generation of concepts, linked ideas and theory and proved to be very helpful in triangulation of information.
Table 3 Matrix Showing Research Question and Data Gathering

<table>
<thead>
<tr>
<th>Research Question</th>
<th>Inductive Propositions</th>
<th>Data Gathered</th>
<th>Anticipated Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>What is the current status of information security management practices in the Australian university sector?</strong></td>
<td>The level of security management will be disparate between institutions, tending towards ad hoc rather than structured, and non-standardised.</td>
<td><strong>Interviews</strong>&lt;br&gt;- Interview Instrument administered to 38 AVCC universities.&lt;br&gt;- Unstructured workplace interviews.</td>
<td>An understanding of current management approaches which highlight deficiencies as well as enabling attributes.</td>
</tr>
<tr>
<td><strong>What are the key issues and influencing factors surrounding the effectiveness of information security management practices?</strong></td>
<td>The intangibility of risk in a diverse environment holding a culture of relative non-compliance.</td>
<td><strong>Observation and Participation</strong>&lt;br&gt;- Observation and participation within the workplace.&lt;br&gt;- Observation through contact with other higher education institutions.&lt;br&gt;- Participation in higher education institution security email discussion forums.&lt;br&gt;- Field notes and memos.</td>
<td>Cultural, organisational, funding and prioritization issues.</td>
</tr>
<tr>
<td><strong>How could improvements in information security management be achieved?</strong></td>
<td>Prioritization at a corporate governance level, grassroots networking, hybrid adaptation of standards and best practice.</td>
<td><strong>Documentation and Material</strong>&lt;br&gt;- Security forums, written security material, literature, research, Internet whitepapers, electronic journals, business plans, the media.</td>
<td>Structure, external and internal drivers and influences, peer benchmarking.</td>
</tr>
</tbody>
</table>
3.3 Data Analysis

Overview of Analysis Approach

In defining an overall framework for data analysis, recommendations were adopted from Miles and Huberman (1994). To further enhance broad conformance to Miles and Huberman’s (1994) recommendation of structure, several other researchers’ methodologies were reviewed to ensure that appropriate structure existed. This included the methodologies written by Coffey and Atkinson (1996), Marshall and Rossman (1999), Mason (2002), O’Leary (2004), Patton (1990) and Ritchie and Lewis (2003).

Coffey and Atkinson (1996) describe the approach recommended by Miles and Huberman (1994) as a systematic approach but not overly prescriptive, and they observe that in order to describe and explain qualitative data, it is necessary to work towards a set of analytic categories that are conceptually specified. They acknowledge however that these categories can be arrived at and explored deductively or inductively. In this case more of an inductive approach was used. This method suited the ontological perspective of the researcher.

The main technique used in this research was thematic analysis involving cross referencing of data to identify emerging themes and patterns. This thematic approach was supported by the triangulation of observations, participation, literature reviews and the survey instrument. This approach tended towards the use of an inductive model for illuminating processes and is one that is recommended by Miles and Huberman (1994) to include a recognisable and objective method. Miles and Huberman (1994) contend that phenomena exist objectively in the world because people construe them in agreed upon ways, so therefore it is important to evolve and use a valid and verifiable method for capturing these relationships and their causes.

The aim therefore was to use an approach to data analysis that could be replicated by other researchers so as to ensure validity and objectivity in the approach. It is
recognised that qualitative data when compared to quantitative data, needs to be justified more stringently as there are more established methods for analysis in quantitative data (Miles and Huberman, 1994). It was noted that the requirement to adhere to a structure and ensure that documentation of the process for qualitative data analysis for the purpose of both auditing and learning was integral to quality research. This therefore forms an integral component of the final write up.

The data analysis methods are frameworked primarily against the methodology espoused by Miles and Huberman (1994), who stress the need for the analysis of data to be undertaken with explicit and systematic methods for drawing conclusions. The broad method for analysis conformed to further recommendations by Miles and Huberman (1994) which included a defined coding and interpretation method, based on a staged approach to data analysis. This staged approach largely conformed to a process of reducing the volume of information, identifying significant patterns and constructing a framework for communicating the essence of what the data reveals (Patton, 1990). The following distinct stages were involved:

1) data reduction
2) data categorisation
3) conclusion clarification

Data analysis therefore involved a process beginning with specific observations about the data, representing a strategy of inductive design to allow important analysis dimensions to emerge from patterns found in the data (Patton, 1990). This led to the building of general patterns and from here these thematic patterns were then elaborated on to reach more solid theoretical constructs. The theoretical constructs were eventually synthesized into a conceptual framework represented by the security practitioner’s management model. This conceptual framework provides the capacity for understanding specific observations and analysis of data (Patton, 1990).
Data Reduction

Data reduction was an integral part of analysis and refers to the process of selecting, focusing, simplifying, abstracting and transforming the ‘raw’ data (Miles and Huberman, 1994) so that ‘final’ conclusions can be reached. Data reduction as a process occurred in anticipatory ways as conceptual frameworks were developed and as instruments, cases and questions were better understood through analysis (Coffey and Atkinson, 1996).

The study involved data reduction over three main phases. Phase one involved a transcription phase which began by transcribing the 38 audio recorded interviews into text format, as well as the field memos and observation notes. This provided for the researcher to read verbatim interview transcripts and to make memos and notes of key points and issues. A cross-interview data reduction technique was used to group together answers from different people to common questions and to allow for analysis of different perspectives on central issues (Patton, 1990). This information was then used to construct an ‘interview map’ in the data display phase, which displayed key words and descriptive phrases.

Data Display

Data display was largely achieved by taking the transcribed interviews which had been grouped by questions for all institutions and to begin to code them. The coding process was aimed at identifying, categorizing and then actually coding primary patterns in the data (Patton, 1990). The process of data display involved coding in Atlas.ti, as well as the construction of relationship diagrams as recommended by Miles and Huberman (1994). This process was used to describe the way in which data is represented through diagrammatical or visual forms in order to show what those data imply (Coffey and Atkinson, 1996).

Data display was used for further refinement of data through familiarisation, reduction and display. The data display process took narrative text and organized it into an assembly of information including quotations and codes (Miles and Huberman, 1994).
From here a list of the top ten super codes was generated. The advantage of the coding and the use of quotations was that it provided succinct representations and distinguished relationships arising from the data collected to shape emergent themes. This process was conceptualized as a primary tool for the formulation of propositions.

A facilitation of emergent themes and recognizable patterns to take shape occurred, some of which previously constituted tentative ideas and key points of interest. Following recommendations by Patton (1990), as a test of credibility and validity, the data categorizations generated for coding were tested against the following criteria:

- Internal and external plausibility was gauged by an internal test of consistency and an external test of completeness i.e. the categories could be seen to fully represent the data.
- The categories were seen to reflect the basic research questions and could be referenced against the research problem itself that was being researched. There were no cases of data that could not be assigned.
- Given the research problem and the questions, the codes could be reasonably duplicated by another person.
- Feedback gained on the set was given credibility by the participants. This occurred by way of an initial key findings report being provided to members of CAUDIT, which was based on the first pass generation of categories and findings.

The researcher recognised that an onus existed to use a combination of experience, knowledge and gathered information to present and interpret evidence in a variety of ways. The data gathered was therefore also assessed to corroborate and strengthen themes and conversely to look for conflicting information that disconfirmed analysis. The density or grounding of coded words was measured, and relationships between codes defined. Super codes were used to define major constructs and display themes.
Conclusion Drawing/Verification

Inductive analysis was used to determine patterns, themes and categories of analysis emerging from the data (Patton, 1990). During the coding process this manifested as inductively generated categories provided for central emergent themes apparent through recurring patterns. This process led to a categorization system which could be further used to generate meaningfulness from the information collected.

Miles and Huberman (1994) offer twelve different tactics for generating meaning from information. These tactics range from descriptive to explanatory and from concrete to conceptual or abstract. The tactics begin with a counting tactic (literally to see what is there). This occurred in the coding process by word counts. Additional techniques included the identification of patterns and themes, determining plausibility, clustering of ideas, making metaphors and splitting variables (Miles and Huberman, 1994). These were all used as initial strategies to achieve a level of integration and differentiation of information.

Following on from this, the capacity to see relationships more abstractly was achieved through an iterative process of subsuming particulars into the general, factoring, noting relationships between variables, and finding intervening variables (Miles and Huberman, 1994). The integrated coherence of the data was further brought together through building a logical chain of evidence and making conceptual and theoretical constructs. The use of this methodology allowed the display data to be interpreted and meaning to be drawn through a variety of different tactics. This included for example, looking for comparative and contrasting cases, exploring themes, patterns and regularities, and by using metaphors and variables.

Essentially this phase involved an interpretation of causal relationships, by noting regularities, patterns, explanations, possible configurations, causal flows and propositions (Miles and Huberman, 1994). This phase was set within the context of the initial development of propositions and an examination of whether the emerging
conceptual framework (the security practitioner’s management model) could be supported or refuted. Once this conceptual framework began to emerge from an established set of propositions, the entire data was re-examined for supporting or refuting evidence, with further refinement demonstrated in the ‘Findings’ and ‘Discussion’ sections of this thesis.

**Coding Methodology**

In line with the overall inductive approach, no coding was developed prior to data collection – in this way coding was developed after seeing how the data functioned in its context (Miles and Huberman, 1994). Coding names were chosen to most closely match the concept they were representing, as recommended by Miles and Huberman (1994), and to generate propositions from connected sets of statements, to reflect findings and conclusions of the study.

The process began on a practical level by transcribing the 38 audio recorded interviews, memos and field notes into verbatim text. An initial analysis followed, involving re-reading and re-listening of transcripts and audio files, constituting the data reduction stage. This was followed by data sorting and coding, involving looking for themes which in turn further influenced the sorting and subsequent coding of data. Later, this extended to the development of propositions, constructs and theories embedded in and emergent from the data. The focus of the audio transcripts in terms of data analysis was to explore the perspective of each participant, and to identify any themes that emerged from the data.

The researcher prescribed the use of coding as a common solution for analysis of qualitative data as large narrative text existed, and the process of coding was therefore applied in order to ‘classify the words’ (Miles and Huberman, 1994). Descriptive and explanatory codes were used so that coding allowed narrative text to be categorised and to permit clustering of relevant themes which could then be related to the specific research problem.
Allocation of descriptive codes did not necessarily provide for full interpretation but was used for the application of an ‘attribution of a class of phenomena to a segment of text’ (Miles and Huberman, 1994). The higher level class order (referred to as super codes in Atlas, the software program used for coding), was then followed in the latter stages with explanatory coding used to allow more of an interpretative application to text. Explanatory coding involved linking and relationship building between categories, prior to data display stage. These relationship diagrams are provided in Section Four ‘Findings’.

Explanatory coding involved the four summaries as recommended by Miles and Huberman (1994). These included themes, causes/explanations, relationships among people, and more theoretical constructs. The textual words from the study and interviews are therefore interpreted so that a concrete, vivid, meaningful flavour is provided to the reader (Miles and Huberman, 1994). This approach is essential for discussion of the findings of the data.

**Coding Software**

As a result of conducting the 38 interviews in Australian universities, the raw data from transcription of the interviews exceeded 70,000 words. After some preliminary research it was decided to use a ‘Computer Assisted Qualitative Data Analysis Software’ (CAQDAS) package for coding. The free version of Atlas.ti was selected for this purpose, based on researching various qualitative analysis approaches. The sheer volume of textual information required a systematic approach to coding for analysis. According to Barry (1998), who compared and contrasted Atlas.ti against Nudist, a CAQDAS is useful in order to help automate and therefore speed up the coding process. Use of the software also provides a formal structure for writing and storing codes, quotations and memos. It also facilitates more conceptual and theoretical thinking about the data through an in-depth examination of data relationships.
Barry (1998) suggests that incorporating risk mitigation with using CAQDAS is necessary. Risk mitigation was therefore used in order to avoid some of the commonly acknowledged risks. These were identified as the potential for distancing to occur between the researcher and the data, the possibility of qualitative data being assessed from a quantitative perspective, and an increase in homogeneity in methods of data analysis, whereby the software can ultimately ‘hijack’ the analysis process.

These risks were considered to be minimal after adopting the approach of using technology to facilitate the process of analysis for balance. In removing the concept for coding software to be an epistemological standpoint itself, and instead establishing this stance prior to coding, the software was merely a facilitator. A superficial analysis of text without proper depth would return poor results regardless of whether coding software is used or not. The methodology used for this research involved becoming extremely familiar with the text, through reading the text in depth and considering many angles and patterns prior to actual coding.

Balancing this process with an adopted epistemological standpoint, so as not to corrupt the coding process was an important aspect. The development of coding through technology with an epistemological stance helped to develop a conceptual framework aimed at making sense of the findings and integrating the relationships between them. This idea is supported by Miles and Huberman (1994), who describe a conceptual framework as explaining the key factors, constructs or variables and the presumed relationships between them, where frameworks can be ‘rudimentary or elaborate, theory-driven or commonsensical, descriptive or causal’. Importantly, the conceptual framework from this study shows the relationship between key factors and as such meets the explanation of the conceptual framework as described by Miles and Huberman (1994).
4 Key Findings

4.1 Introduction

This section discusses the research results and key findings. The information provided in this section is without detailed analysis and is presented as results – an expanded discussion and elaboration on these results follows in Section 5 ‘Discussion’. This section includes:

- Summary of key findings,
- Links between findings and research questions,
- Coding results, represented as:
  - tabular form showing coding density,
  - network view showing relationships, and
  - interview findings,

Summary of Key Findings

The findings were wide ranging for each research question; however the key findings for each question are succinctly summarised in this section. These findings largely underpin the proposed security practitioner’s management model.

1. What is the current status of information security management practices in the Australian university sector? The survey results primarily indicated that the status of information security management in Australian universities varied between each institution dependent on a number of factors. These factors included the security management method, senior management support and involvement, resourcing and funding, the capacity to defend against security threats, the level of IT centralisation, and the overall culture of the organisation. An important finding was that the ‘champion’ of
information security often occupied a non-senior position within the central IT department, reported mainly within the IT department, and yet had wide ranging responsibilities for security impacts across the business. This person often had the most specialised knowledge of security and its impacts, yet was not always positioned with much authority over systems or people.

A critical finding was that a common method adopted to manage information security was cited as being based largely on incident management, reflecting a reactive approach. Comments and views expressed by participants supported the notion that a relatively unstructured and reactive approach to managing security existed in many institutions. This situation was reflected by an ad hoc approach to managing security, a general lack of adoption of standards, a lack of security strategic plans and a cited lack of full integration of security within the business processes and budgets for IT. In summary an enterprise approach to security was not easily identifiable.

2. **What are the key issues and influencing factors surrounding the effectiveness of information security management practices?** The key findings indicated that a lack of structure in managing information security impacted its effectiveness across the organisation. The lack of an appropriate structure to integrate throughout the enterprise business processes caused security to operate in an ad hoc manner, for a reactive nature to be apparent and for shortcomings in resourcing and funding. A significant gap also existed between desired and actual awareness of information security risks across the university community at large. A major cause for this was cited as the intangibility of security in conjunction with low perception of threat levels. This in turn impacted a broad number of other issues, including work practices, allocation of resources and funding, prioritisation of security, acceptance of the reality of risk, development of clearly written and communicated policy, and general compliance with security.

3. **How could improvements in information security management be achieved?** A structured and coordinated approach was needed to improve effectiveness of current information security management approaches. Developing a more structured and
coordinated management framework for progressing security within the university community was seen as an essential step in delivering improved security management.

The human element of information security was seen as one of the greatest barriers to improving security and therefore one of the key factors to focus on for improvement. In fact it is suggested by the author Mitnick and Simon (2002) that social engineering exploits will increase as technology improves to the point that human weaknesses must be used. Mitnick and Simon (2002) focus on the human factor as a weakness that is exploited and cites many examples of how security is generally an illusion. This illusion results from the fact that people from an inherently behavioural viewpoint wish to be secure, and tend to believe that others are acting in a manner conducive to overall security, when in fact this may not be the case. The goal of a culture of compliance towards security was commonly highlighted through the research as the best strategic goal to aim for, involving increased awareness of security issues.

Engaging senior management involvement to help security resourcing and funding was additionally seen as a key step. A gap was highlighted in that the use of existing common management frameworks such as AS/NZS 17799, AS13335 etc. was seen as helpful in what to implement but did not necessarily assist in understanding how to progress security more effectively. An integrated, structured approach was cited as being necessary to improve security management throughout Australian universities.

**Links Between Findings and Research Questions**

The research gathered information relevant to the key research questions. The findings are closely linked to the three research questions aimed at providing information on the current status of information security management, an identification of the key influencing issues and factors impacting security management, and how improvements in security management could be achieved. The primary data source, the survey instrument, covered a range of questions broadly categorised under five key areas for convenience. These were senior management involvement, security management approach, security policy, security awareness and security compliance.
The results of the interviews provide rich information regarding the three key research questions. Due to the nature of the survey instrument and the interview process, probing allowed a ‘behind the scenes’ look at phenomena occurring. This allowed the ‘current status’ of security management to be determined from several perspectives. Valuable information was able to be obtained on the type of management structures in place, reporting styles and the application of management frameworks. This information provided a foundation to further explore information relevant to research Question 2, ‘an identification of the key influencing issues and factors impacting security management’. Issues and factors covering senior management, cultural aspects, funding, work practices and approaches were identified.

This data helped to highlight the types of issues that occur and how these can be addressed. A primary aim of the research is to promote an improved understanding of issues that impact on security management effectiveness. The final research question incorporated interview results on improvements in security management. These results, supported by the literature, were used in the development of a security practitioner’s management model (Figure 1). This model is a key outcome based on a holistic approach to improving security management in Australian universities. The model is discussed further in Section Five, ‘Discussion’.
4.2 Summary Coding Results

Coding was performed using the Atlas.ti software program using interview transcriptions of over 70,000 words. The textual coding generated several tables and network views depicting code based density and coding relationships. Table 4.1 provides a ‘super code’ summary for all interview data. The data in this table is then provided from a network view in Figure 5.

Table 4 Super Code Summary - Assigned Codes and Density

<table>
<thead>
<tr>
<th>Code</th>
<th>Density</th>
</tr>
</thead>
<tbody>
<tr>
<td>Structured Management Approach</td>
<td>96</td>
</tr>
<tr>
<td>Security Awareness and Communication</td>
<td>84</td>
</tr>
<tr>
<td>Human Resourcing</td>
<td>68</td>
</tr>
<tr>
<td>Senior Management Support</td>
<td>63</td>
</tr>
<tr>
<td>Funding</td>
<td>49</td>
</tr>
<tr>
<td>Cultural Compliance</td>
<td>34</td>
</tr>
<tr>
<td>Conflict in Work Priorities</td>
<td>28</td>
</tr>
<tr>
<td>Reactive Approach</td>
<td>27</td>
</tr>
<tr>
<td>Security Policy</td>
<td>25</td>
</tr>
<tr>
<td>Decentralisation of IT</td>
<td>25</td>
</tr>
</tbody>
</table>
Figure 5  Assigned Codes for Security Practitioner’s Management Model
4.3 Coding Results for Senior Management Involvement

Participants were asked a number of questions pertaining to the level of involvement from senior management in relation to information security. For the purposes of the survey, questions related only to senior management outside of the IT domain. This was deliberate in an attempt to capture information about management not normally associated with IT in order to ensure that wider university views were captured.

Table 5 Coding Summary for Senior Management Involvement

<table>
<thead>
<tr>
<th>Code</th>
<th>Density</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allocation of Funding</td>
<td>38</td>
</tr>
<tr>
<td>Awareness and Understanding of Risk</td>
<td>36</td>
</tr>
<tr>
<td>Senior Management Engagement</td>
<td>32</td>
</tr>
<tr>
<td>Security Reporting</td>
<td>33</td>
</tr>
<tr>
<td>Allocation of Human Resources</td>
<td>22</td>
</tr>
<tr>
<td>Reactive</td>
<td>15</td>
</tr>
<tr>
<td>Support of Security Policy</td>
<td>12</td>
</tr>
<tr>
<td>Competing Work Priorities</td>
<td>5</td>
</tr>
<tr>
<td>Information Security Governance</td>
<td>4</td>
</tr>
<tr>
<td>Intangibility of Security</td>
<td>2</td>
</tr>
<tr>
<td>Culture of Compliance</td>
<td>1</td>
</tr>
</tbody>
</table>
Figure 6 Assigned Codes for Senior Management and Information Security
INFORMATION SECURITY MANAGEMENT IN AUSTRALIAN UNIVERSITIES – AN EXPLORATORY ANALYSIS

Table 5 provides a coding summary for this area, and Figure 6 depicts coding relationships. The questions contained in the survey instrument on senior management involvement related to a number of areas. These areas included the level of reporting they received, the perceived level of senior management’s understanding of the importance of information security, whether or not senior management provide the required level of support, and finally, what changes would be required for senior management involvement and support to be improved.

Findings on Senior Management Reporting

Participants were asked whether senior management received regular (established, ongoing and consistent) reporting on information security.

![Senior Management Receives Regular Reporting on Information Security](image)

**Figure 7 Participants Who Regularly Provide Reports to Senior Management**

Less than one third of universities indicated that they regularly engaged and reported to senior management on information security matters (Figure 7). Comments that typified the existence of regular reporting included:

‘*Yes through our IT committee, every 6 weeks*’ and ‘*We have quarterly reporting including security*’

‘*they get regular IT reports with information security on it*’
In contrast, most reporting was cited as ad hoc, occurring primarily in reaction to incident activity, followed to a lesser extent by reporting occurring as a result of audit or annual reports. Typical comments on incident reporting are:

‘The only reporting senior Executive receive is security incident reporting’

‘we send copies of all our security incident reports through to the Executive’

Findings on Senior Management Understanding and Support for Security

Links were established between regular reporting and engagement of senior management and the subsequent support (and understanding of security issues) from senior management. The institutions who reported regularly to senior management also correlated closely with the institutions who considered senior management provided appropriate support for security (Figure 8). This support was mostly expressed as appropriate funding and resourcing, or a demonstrated interest shown by senior management towards the status of security.

![Bar Chart](image)

Figure 8 Participants’ Perception of Senior Management Support
The overall lack of regular reporting to senior management affected senior management’s levels of understanding of security, and the commensurate support provided for security (Figure 9). In some situations, senior management was considered to have very little idea of security, often interpreted as a low interest in security. This situation is reflected by the following types of comments:

‘the VC would have no idea’

‘I don’t believe they understand the magnitude and the complexity of the problem’

A majority of participants suggested that extant levels of understanding did not translate into appropriate acknowledgement or actions to provide the required level of funding and resourcing for security. In many instances, the lack of resourcing and funding was cited as being due to the fact that there were ‘many competing priorities’. While a perception by senior management existed that ‘all was under control’, security took a backseat. The following quote provides an example:

‘I think they see it as important but whether they appreciate what that means in terms of how we have changed what we do, and how much money is involved, so I think there is a concept of the practical issues around that are not fully appreciated’

‘the message really hasn’t got through that information security is a major activity’

‘They sort of say, well ITD (the Information Technology Directorate) looks after that. It is only really when there is a major incident…’
The findings also indicate that in institutions where senior management was less supportive of information security, controls in place tended to be less observed or adhered to. Conversely, effective senior management engagement more adequately set the ‘tone at the top’ resulting in more effective policy enforcement and improved behavioural change.

**Findings on Improving Senior Management Involvement in Security**

A consistent theme was noted with participants who considered that the levels of funding received were a direct representation of senior management support. Measurement of support from senior management was strongly gauged in terms of financial support; either funding for human resourcing or other security related expenditure. Most participants indicated that they saw a need for increased funding. When asked what senior management needed to do to improve support for security typical comments were:

‘*More money. More money and resourcing’*

‘*the first and easy way to answer the question is I would have to say financially’*
‘It really comes back to priorities and funding’

‘we need to have the time and funding to investigate appropriate security solutions’

Several other areas were cited in relation to achieving improved senior management support. Some participants held the view that senior management had a responsibility to support initiatives to increase security awareness and compliance across the organisation, and to ensure a more consistent understanding of security at all levels.

‘I mean my couple of points would be more about the consistency of understanding across the university, in the faculties and divisions in particular, there is a number of faculties and divisions that don’t have the same sort of understanding, so it would be really good for me to see a consistent understanding right across the schools’

‘Some support for University wide awareness initiatives’

Other views included senior management providing improved governance and direction on IT overall, with articulation from senior management on the business direction, expectations and business requirements for IT systems (and therefore establishing business drivers for security). Typical comments reflect this finding:

‘So at that point we need active involvement from senior management, we need an indication of their long term expectations of the corporate systems’

‘We need a security architecture and a security policy, prior to that we need to look at our business systems, the corporate systems, and look at the architecture, the information flow between them, the intended audience, the
levels of security and risk, what the university actually wants to do with these systems’

A commitment to back the security policy and provide direction and governance was seen as a necessary step by senior management for improvements:

‘a little bit more corporate governance and business direction translated into security from them (senior management)’

‘Greater enforcement of our IT policy’
‘we need a strong information security governance framework, and underpinning that we need policy around information security’

‘helping describe what it is that they (senior management) believe is acceptable policy’

‘perhaps a more active role, with our top management or senior managers in organisations taking an active role in ensuring that their staff are aware of security policy’

A need for closer integration between strategic planning and the security program was also noted, due to problematic, ad hoc or reactive processes in existence. Emerging requirements for senior management to take up the challenge of responsibility for higher level compliance issues were raised. This included corporate governance over security to ensure that legal and regulatory compliance requirements were being met in line with corporate risk management. The following comment typifies participants’ views of the need for senior management to understand risk:

‘The best answer I could think of for this one is understanding risk, so in terms of changes it is really
understanding what the current security challenges are and understanding the risk’

Some participants held the view that senior management did not need to improve, but instead the IT centre needed to improve senior management’s awareness, understanding of risk and ultimately, to facilitate an improved senior management position on security. The following comments typify this statement:

‘they are supporting it to the best of their ability and we are doing a bad job, or IT is, of educating and informing them of how it might be done better’

‘they probably do support information security but we are not telling them enough about what they need to be supporting’

‘Anyway for them to improve, they don’t need to improve, it is us that needs to improve to help them become more aware’

In achieving an improved relationship, bridging the gap of a combination of trust, willingness to enforce compliance, and consistency of priorities needed to be addressed. This was seen as occurring primarily through increasing security as an agenda item on senior management meetings and discussion, and for senior management to listen and be willing to get behind security:

‘we come up and say to them ‘we need more money’, and they either trust us and say yes, or they don’t trust you and you don’t get what we need, and then you are extremely vulnerable, so the only way to connect this I think is that they have to take on some responsibility for understanding the IT issues’
Summary of Findings on Senior Management Involvement

In terms of current status, the findings in this section indicate that senior management’s involvement in information security plays an important role in the funding and support for security as a function. Links between consistent reporting to senior management and their understanding and support of the security function are evidenced. However, the level of reporting or otherwise engagement of senior management currently tends to be low. This impacts senior management’s awareness and understanding of security, further impacting involvement and subsequent support.

As funding appears to be both a key constraint and an indicator of support, the currently low levels of reporting and engagement with senior management regarding information security are of concern. The results of the survey indicate that improvements from senior management require a greater awareness and understanding of the issues associated with security, which necessarily translate into support, primarily through funding and resourcing. The cultural issue of the security function being seen as an ‘IT problem’ is still pervasive, and without due recognition of this limitation, security remains out of the minds of many institutions’ senior management at present.
4.4 Coding Results for Security Management Approach

Participants were asked a range of questions on the operational structure for security, the main approaches taken to manage security, if the approach was effective and if standards had been adopted as part of the approach, and how improvements could be made. Table 6 provides a coding summary for this area, and Figure 10 depicts coding relationships.

Table 6 Coding Summary for Security Management Approach

<table>
<thead>
<tr>
<th>Code</th>
<th>Density</th>
</tr>
</thead>
<tbody>
<tr>
<td>Benefit of Structured Approach</td>
<td>41</td>
</tr>
<tr>
<td>Intended or Actual use of 17799</td>
<td>28</td>
</tr>
<tr>
<td>Ad Hoc Use or No Use of Standards</td>
<td>17</td>
</tr>
<tr>
<td>Inadequate Human Resourcing</td>
<td>12</td>
</tr>
<tr>
<td>Raise Awareness and Understanding</td>
<td>12</td>
</tr>
<tr>
<td>Issues with Decentralisation of IT</td>
<td>7</td>
</tr>
<tr>
<td>Allocation of Funding</td>
<td>5</td>
</tr>
<tr>
<td>Reactive Approach</td>
<td>5</td>
</tr>
<tr>
<td>Senior Management Engagement</td>
<td>4</td>
</tr>
<tr>
<td>Information Security Governance</td>
<td>2</td>
</tr>
<tr>
<td>IT Security Seen as IT Problem</td>
<td>2</td>
</tr>
<tr>
<td>Competing Work Priorities</td>
<td>1</td>
</tr>
<tr>
<td>Lack of Measurement</td>
<td>1</td>
</tr>
</tbody>
</table>
Structured Approach Necessary

Intended or Actual use of 17799

Ad Hoc Use or No Use of Standards

Inadequate Human Resourcing

Raise Awareness and Understanding

Information Security Governance

IT Security Seen as IT Problem

Reactive Approach

Lack of Measurement

Senior Management Engagement

Issues with Decentralisation of IT

Allocation of Funding

Competing Work Priorities

Figure 10 Assigned Codes for Security Management Approach
Findings on Security Management Operational Structure

Participants were asked a number of questions in relation to the approach taken to operationally manage information security. This included gathering information on the operational and reporting structure. In all cases, security practitioners reported that they reported internally within IT. Within IT, this was generally a level such as Infrastructure Manager, Communications Manager, Network Manager and sometimes the IT Director. What was noticeable was that no security practitioner reported directly outside of IT, to a Senior Management level, Risk Manager or similar.

Some (very few) organisations, stated that they still lacked a dedicated role for the management of Information Security. It was apparent in those cases where the institution lacked a dedicated security function, led by a full time resource, those institutions suffered a substantial disadvantage compared to those institutions that had one or more resources allocated to security. The absence of a dedicated security coordinator impacted the institution’s ability to establish and drive a centralised and coordinated approach to security. In most cases, the institution had a security practitioner who operated with a ‘virtualised team’, with team members physically in other sections, but accessible by the security practitioner. Only some of the large institutions had dedicated technical staff in a dedicated security team environment. A typical comment which sums up both the common ‘virtualised structure’, as well as the lack of coordinating role without a security practitioner is:

'We don’t have a body or group responsible for that all encompassing view of security, so there is no operational structure per se, although I guess the defacto structure is individuals in other areas have responsibility for their area, so there is the server people looking at your server security, the applications people who have DBAs (Database Administrators) looking after that component, the network services people looking after the physical security and looking at Mac (Media Access Control) addresses for
registration to permit access etc, so looking at the big picture it’s quite distributed, and what has occurred to me thinking about this question for you, is that we lack the coordinating role’

Findings on Approaches Adopted for Managing Security

Participants overall were positive on their management approach to security. The most common approach for management was cited by 60% of participants based on incident management (Figure 11). This was followed closely by risk management and managing as part of the IT plan. However, approximately one third of participants indicated the use of an ad hoc approach to managing security. The management of security in relation to incidents was described as being either ad hoc or reactive. A few organisations described their management of security as being well-defined through a framework or coordinated structure.

![Approach Adopted for Managing Information Security](image)

**Figure 11 Approach Adopted for Managing Information Security**

Findings on Effectiveness of Management Approach

When participants were asked if they thought the existing approach taken to manage information security was effective, the majority of participants were relatively positive about how effective their approach was (Figure 12). However, many participants noted
that room for improvement existed. In some cases it was considered by participants that while the actual management approach in itself was appropriate, its effectiveness was hindered by other organisational constraints, priorities, or cultural barriers. In some cases it was considered that the enforceability of the security approach needed to be enabled, requiring senior management backing or support.

![Bar chart showing participants' views on the existing approach for managing security effectiveness.]

**Figure 12 Participants Who Considered Existing Security Management Effective**

**Findings on Changes Required to Improve Effectiveness of Management Approach**

A pattern emerged where the single issue considered necessary to improve the management approach for security was to move away from existing ad-hoc activities towards a structured, holistic approach (Figure 13). This approach should integrate more effectively with the business, indicating that point solutions needed to be replaced with a more cohesive model. The current ad-hoc approach resulted in risks improperly quantified, or not fully understood and acted upon. This also affected other activities such as development of policy, standards and guidelines for security, as well as awareness raising and the promulgation of security information in general.
Additional Resourcing
Improved Awareness
More Structured Approach

Figure 13 Changes Required to Improve the Security Management Approach

Comments follow which typify this finding, and conversely, the last comment describes the effectiveness of having a structured approach:

‘I think at the moment it is fragmented though, we have got web security, we have got data security, we have got server security, we have got holes in firewalls as a result of faculties doing their own thing, and so there is a variety of areas where standards and policies even though they may exist to varying levels of completeness, are not being held together in a neat tight way, because the management of it is weak, and I think that is the challenge together, to draw those strands together and to lay over it a structure’

‘it is achieving security requirements however I would like things to be more structured’

‘We have a concern that we don’t have enough coordination, and thus a standards based approach’

‘It is more of an ad hoc approach. It is also very
reactive. I guess not totally effective, it would be nice to have some sort of structured strategy’

‘Agree - the framework exists to make sure we can manage it properly, the planning exist to make sure we can stay up with the act, the policy and the procedures exist to make sure that we are following things in a way routine manner, and the awareness exists, clearly we can do better, always, but I think it is doing what it needs to do’

Consistent referral was made to specific areas that cohesively would improve levels of governance. Participants indicated they saw a need for security to be more structured and for strategic alignment to the business function within the organisation. This was seen as necessary for security to be driven by organisational requirements, to achieve better integration with the business, and for the security function to match the actual processes used within the organisation.

Due to competing priorities, the necessity to prioritise and distribute efforts to areas with the greatest impact was noted as being critical to ensuring appropriate security adding value. The need to highlight information security as a business issue (rather than an IT owned issue), and to illustrate the enabling of security to the business involved moving the focus away from security as being restrictive. Another identified issue was establishing university applicable security practices. Many participants saw a need to draw from the vast array of already existing security practices and establish a set of university sector relevant security practices and guidelines.

A second theme predominant in the finding was that of raising awareness and understanding towards security:

‘So it comes down to increased awareness, and a strategic ICT plan, like at this institution it is too ad hoc’
‘It sort of goes back to the old one, a better understanding, a broader and better understanding of risk’

‘The management approach itself is ok, it comes down to awareness, so basically more funding and a higher level of awareness’

‘so we think more than anything we need to get this awareness happening’

‘The other thing is improved awareness at all levels’

The issue of funding was also raised, with the following types of comments reflecting findings:

‘I think having a link into the budget process, so that there are opportunities for us to say ‘going forward these are major risks in this area’, and for us to be able to prioritise all of the demands for money in a more structured manner I think would be really beneficial’

‘some funding for centralised security management’

‘Looking at the strategy, to meet the needs of those functional needs, and resources required’

Findings on the Use of Security Management Standards

Less than half of the participants stated they used security management standards. Of those that did, almost all indicated 17799, or a state level adaptation of that standard. Many participants stated that they would like to see university sector applicable standards - standards that were designed to provide universities with a baseline, allow
benchmarking, and prevent universities from having to ‘reinvent the wheel’. This was despite less than 50% of participants citing an active use of existing standards.

It was evident that many university security practitioners and administrators already had some well-developed locally based, technical standards that they applied to security. Although 17799 was often quoted as being a preferred management standard, several participants were critical of the standard, suggesting that following it would be highly time consuming and resource intensive, and that it was not necessarily applicable to the university environment.

Similarly, feedback indicated that auditors used a different standard to 17799 for auditing of security (primarily COBIT). Although several state governments have mandated state level adaptations of 17799, not all universities are proceeding in this area. The standard recommends that organisations develop an information security management system based on organisational requirements, and then adapt the standard as necessary. Findings from the survey indicate that 17799 is the preferred choice for a security standard, but clarity is lacking on implementation.
4.5 Coding Results for Security Policy

Participants were asked a number of questions in relation to the approach taken to the policy process, associated with policy development, implementation and effectiveness of policy. Table 7 provides a coding summary for this area, and Figure 14 depicts coding relationships.

Table 7 Coding Summary for Security Policy

<table>
<thead>
<tr>
<th>Code</th>
<th>Density</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inadequate Human Resources</td>
<td>14</td>
</tr>
<tr>
<td>Cultural Compliance</td>
<td>14</td>
</tr>
<tr>
<td>Senior Management Engagement</td>
<td>13</td>
</tr>
<tr>
<td>Awareness and Communication of Risk</td>
<td>13</td>
</tr>
<tr>
<td>Benefits of a Structured Approach</td>
<td>9</td>
</tr>
<tr>
<td>Issues with IT Decentralisation</td>
<td>9</td>
</tr>
<tr>
<td>Policy Process</td>
<td>9</td>
</tr>
<tr>
<td>Issues with Enforcement of Policy</td>
<td>8</td>
</tr>
<tr>
<td>Information Security Governance</td>
<td>6</td>
</tr>
<tr>
<td>Aligning IT Security with Business</td>
<td>2</td>
</tr>
<tr>
<td>Intangibility of Risk</td>
<td>2</td>
</tr>
</tbody>
</table>
Figure 14 Assigned Codes for Security Policy
Findings on Technical Stakeholder Input on Policy

Participants were asked whether they considered the policy process resulted in appropriate technical stakeholder involvement. The majority of participants either agreed or mostly agreed, however comments surrounding the extent of involvement varied (Figure 15).

![Technical Stakeholders Involved and Support Policy](image)

**Figure 15 Technical Stakeholders are Involved and Supportive of Policy Process**

In many cases getting stakeholder input and involvement outside the central IT group was difficult due to the devolved nature of IT. The issues of decentralisation were reinforced by participants who suggested that centralisation was a situation that facilitated stakeholder involvement. Typical comments by participants who agreed that technical stakeholder involvement existed include:

‘Agree – yes in fact we probably get more from technical stakeholders than we do from the others, so we are probably leaning more towards getting more involvement from the business end of the house, and part of the recommendations from the audit review was to form a information infrastructure security coordination group, and have representative from our teaching, learning, research, IT
environment as well as the business and administration environment, a cross section of the university community, because I think IT tends to be too much of a closed shop sometimes’

’Agree – as much as we could reasonably do, our server security policy, our device security policy and the operations manual were done in consultation with a steering committee made up of technical staff all over campus, so we’ve got buy in, they understand it and in principle agree to comply with what it is that we have got developed so that’s good, how that works in operational management, some of them get it and some don’t, even though they agreed in principle with what we are talking about’

’Agree, any policy is circulated widely to IT staff – we have staff who are more than willing to contribute to that, and I think it helps to have the centralisation of IT’

Examples of comments by participants who ‘Somewhat Agreed’ are:

‘Somewhat Agree – because as I mentioned before the devolved nature of our IT support here, and thus some lack of control over that group makes implementation campus wide difficult. While we’ve got, just as an example, SUS servers and Sophos servers that can provide automatic updates, we are aware that that is, while it is probably about an 85% hit rate I think, (we had an estimate before in our Operations section), we’ve got patches that are a problem’
'Somewhat agree – I guess we probably get the involvement from people within our own unit, I am not sure how well we do with getting involvement from IT people that are not part of our central group’

An example of a comment by a participant who ‘Disagreed’ is:

'Disagree – I was in two minds with this, there is the opportunity for the required level of involvement from the technical stakeholders, as in we draft the policy and circulate it around and there is lots of opportunity for them to have input in there, but again in practice it tends to be 'well when this becomes a policy as far as we are concerned it is just a guideline, so we are not going to worry about it anyway’, so they don’t actually participate. I mean you could wait three months and pass it out every week and you’d get no feedback’

Findings on Management Stakeholder Input on Policy

Participants were asked whether they considered senior management to be involved and supportive of policy. Again most participants indicated that they ‘Somewhat Agreed’ (Figure 16).
Examples of comments by participants who ‘Somewhat Agreed’ include:

‘Somewhat Agree – it does, particularly where, well it is variable to some degree, some managers would understand the security implications more than others, and then again it depends on the system we are looking at, or the incident we are looking at, or the particular school or faculty we are working with, but some of them are better placed to understand it, and it comes back to the communication and the understanding people have with security risks’

‘Somewhat Agree- the majority of people in campus are supporting the process, they know it’s hard to argue with because we went about it right with the process of getting it in, but there are people that say ‘look it is really not that a big deal, don’t worry about it’’.

Findings on Effectiveness of Policy Process

Participants were questioned on the approach taken to the policy process, including policy development and implementation.
Asked if the policy process was an effective one, most participants were positive (Figure 17). It was noted however that the actual status of information security policy in terms of maturity of process varied considerably between institutions. Several factors were cited as contributing to the effectiveness of the policy process. These included having a structured policy development process, having a policy template, and engaging stakeholders in the policy development process. Additionally, ensuring that both responsibilities and accountabilities were clearly articulated and agreed to in policy was important. An active policy approval forum, promoting awareness and communication of policy and ensuring monitoring and compliance of policy was noted. Participants who thought the policy process was ineffective referred to a lack of standard policy process, lack of resources, lack of participation and delays in policy approval.

Policies that were too ‘unwieldy’, problems with non enforceable policy, or policies that are not effective in achieving compliance due to cultural factors were noted:

'We have an 85 page security policy, that covers the Internet, administration procedures, password procedures etc etc. One thing we didn’t do very well last year was actually manage the administrator passwords, a lot of people are administrators of their own box, information
security hadn’t gone to all of them and said by the way where is the password, so we did send out a paper request to put the passwords on paper, seal the envelope, and without opening it, we’ve put it in a safe, we didn’t get a good response to that, so we still got some servers out there that there might be one person with a password in their head, and we have run some tests that we are going to expand and run on a lot more servers, we found that there are even servers out there with the default logon still enabled, which is pretty bad’

While many participants agreed that the policy process was effective, an issue of enforcement was seen as the major challenge to overall policy effectiveness. Those institutions that actually disagreed that the policy process was effective, stated the reasons primarily as being a lack of support for having a policy approved, or a lack of capacity to ensure its enforceability across a (frequently) decentralised environment.

The participation needs to be improved, everyone is busy doing something else, they say ‘if someone else is writing the policy well that’s great’, but they don’t participate in it, so it is participation and ownership, because there is no need to be compliant with it, you can write whatever you like, it is not enforced.

‘We don’t have security policy, but we certainly have a draft set of security guidelines, it’s been in draft for about 11 years, I have had people ask me for copies of it but I said that’s fine but we have not implemented it yet. There is a draft policy but to try and see how that would ever be accepted by the University it defies me because the place is very decentralised, so to get people to sign of on that, we will probably try again, we are in the middle of a
business continuity planning process for the whole university, and I think out of that we might be able to start to talk about a security policy for the University as well’

Findings on Compliance with Security Policy

In decentralised environments, enforcing policy was more of an issue than in centralised environments. Improving the policy process included initially ensuring an effective process for policy development and implementation was in place, following by establishing an appropriate supportive environment to increase compliance levels to policy (Figure 18). Some organisations reflected that they had either an absence of, very little, or very outdated security policy. Others stated that existing policy was far too unwieldy, while others cited existing policy as being adequate, but commented on the challenges associated with reinforcing desirable security behaviour and thus enforcement of policy across the organisation.

![Compliance to Policies](image_url)

**Figure 18 Participants Who Considered Policy was Complied With**

Many participants distinguished between the IT centre taking policies seriously as opposed to the overall organisation taking them seriously.

‘ITS looks at them seriously, but the institution doesn’t’
'The biggest problem is that to my way of thinking that the business thinks security is an IT issue not a business issue'

Other participants cited that although policy is viewed as an important regulatory mechanism, challenges existed to the ultimate enforcement of policy, particularly in decentralised environments – thus a perception of dispersed responsibility and liability can lead to adoption of poor security practices.

'Implementing them is very difficult basically because of the lack of authority for compliance, so yeh... as far as developing goes, we try to get input for technical and management stakeholders and take that into account'

'Certainly the impression I get is that they (management) take it more like a pain in the ass, or as guideline at best. The problem we’ve got is we’ve had security incidents in the last 12 months, some quite serious, involving IT staff, and the way that, you know you put all the facts on the table to their managers or to the Director of the Division, or the Deans of the Faculty, and it seems to get brushed under the carpet, you know you tend to sit back and say why we are bothering'

A common theme was the lack of resourcing, or inadequate resourcing to allocate to the policy process from development through to ultimate enforcement and the monitoring of compliance.

'Quite often it will come down to simply resources, you know best of intentions and everything else but we wont necessarily have enough people at the time to review the logs or running the logs etc etc. You know the process is
there and the intent is there and you know it is something that is planned for and part of anything, but we just don’t have the resources to do it justice and we should’
‘We treat it very seriously, and the benefits we have, you asked me before if we are centrally controlled, I have got absolute control over the network and the data we hold within the University’

Findings on Improving Policy

When asked how the policy process could be improved, responses ranged depending on the existing relative maturity of the security management function and the policy process. Responses ranged from ‘need to start’ to ‘need to refine existing policies’. A prominent emergent theme was the requirement to dedicate either existing resources to the policy process or to achieve additional resources, and secondarily to improve the capacity to ensure compliance with policy.

‘More resources basically you know, as I said he was employed to be the information security officer, and we immediately ran into some internal audit issues, and he has been spending literally most of his time resolving those and developing policy, and meeting that instead of getting onto the actual security systems, and so it is one of resources, more resources would improve the speed’

‘Resources, skills, time, funding for consulting, importance placed on the you know, on the profile of this activity, processes for policy implementation, and getting management to business rules, business processes, business process analysis, finding out what the hell it is that we want to do would be a good start’
'We find that even when do you develop the policy, the people that are crying out for it ignore it, they want it but wont get engaged in the process. Enforcing policy is something that is critical, otherwise people won’t refer to them'

Ensuring compliance with policy, particularly in heavily decentralised environments, was seen as requiring both awareness raising activities, and commitment from senior management to set the tone at the top and to be seen to be actively supporting compliance measures from a cultural perspective.

'We’ve got to have some representation to that peak steering MIS that has senior executive on it. If you don’t actually have management championing things because they say ‘well I don’t know what the hell IT does’, that becomes the culture of the whole organisation. It can be a significant challenge to get senior management support'

'Yes and large and older universities like our own have a long history of totally devolved activity and are therefore a cultural impediment in some cases for security policies. I think frightening people can help change that culture, pointing out the danger and risk, the danger needs to be very real and very present, IT security dangers are real but not as obvious to people that are not familiar with IT security, so what you have got to do is try and make it more tangible'

'One thing that we need to be clear about is forcing the policies, it is all very well to have policies but if they are not prepared to enforce them when necessary, the whole process is pointless really'
‘I think the policy development no, the implementation process I think there has to be a general acceptance that security to some measure must be run in a central way. So in a decentralised organisation like our own... that sometimes counter culture, that acceptance is necessary, and that is one of the things that could improve the implementation process’

This raises the issue for universities that policies require active monitoring, as well as the capacity to be enforced, to support the security function. An important aspect of policy is that effective security policy, when developed in a collaborative manner, is in fact no less than a form of documenting the accepted and complied with, security culture or posture of the organisation.

A prominent theme also noted was the need to increase awareness and understanding of both risk and policy:

‘More on understanding from the users point of view, why it is important’

‘Improved relationships with stakeholders and other resources will help to develop useful, practical policy. Clearly identified roles and responsibilities are required to ensure awareness’

‘I don’t believe they have, as I said before somewhat agree that they have a reasonable awareness, but they have been lulled into a false sense of security, given that we have had no incidents. Most of the time we have to play up the risk factor’
4.6 Coding Results for Security Awareness

Participants were asked a number of questions in relation to both the approach taken to security awareness, as well as perceptions of existing awareness levels and requirements. Questions focused on current levels of awareness, steps taken to raise security, and how awareness levels could be improved.

Table 8 provides a coding summary for this area, and Figure 19 depicts coding relationships.

Table 8 Coding Summary for Security Awareness

<table>
<thead>
<tr>
<th>Code</th>
<th>Density</th>
</tr>
</thead>
<tbody>
<tr>
<td>Awareness Raised by Security Incidents</td>
<td>40</td>
</tr>
<tr>
<td>Ad-hoc Approach to Raising Awareness</td>
<td>31</td>
</tr>
<tr>
<td>Inadequate Human Resourcing</td>
<td>24</td>
</tr>
<tr>
<td>Awareness Activities Inadequate</td>
<td>20</td>
</tr>
<tr>
<td>Conflict in Work Priorities</td>
<td>19</td>
</tr>
<tr>
<td>Developing a Culture of Compliance</td>
<td>15</td>
</tr>
<tr>
<td>Email Based Awareness</td>
<td>13</td>
</tr>
<tr>
<td>IT Staff Awareness</td>
<td>13</td>
</tr>
</tbody>
</table>
Figure 19 Assigned Codes for Security Awareness
Findings on Security Awareness Program

Participants were asked if their organisation operated a structured awareness program. Less than 15% of participants indicated they had an awareness program in place aimed at both staff and students in a structured, targeted manner (Figure 20). Despite the great majority of participants indicating that low security awareness levels were a barrier to achieving improved compliance with information security, the actual factor cited as having played the largest role in raising awareness levels was attributable to security incidents or breaches, rather than specific, targeted education. This indicates that universities are currently relying on security incidents to help raise awareness. It is likely that this is a reactive rather than planned approach.

Many participants indicate an intention to obtain more structure, as evidenced by:

‘It is more ad hoc but we are planning to move to a more structured process’

‘It is Ad hoc, we don’t have a structured and formal process at the moment’

‘It has been ad hoc but we are starting to formalise it’

‘It is more an ad hoc process but hopefully in a short time there will be an awareness program, things like organising seminars, posters and flyers’
Findings on Priority Given to Raising Security Awareness

Responses were mixed on the question of whether raising security awareness was given a priority, with many participants advocating it was a priority (Figure 21). However, the stated priority did not match the actual outcome of awareness raising based activities. In other terms, less than 15% of participants are effectively targeting awareness raising activities, despite a much higher rate of participants stating that raising security awareness was an important priority in their organisation.
Typical comments from participants are:

‘It is again, it is one of these things, when you ask someone it is given high priority, but that doesn’t translate to outcomes that match that thought process, people would argue that it is important and urgent, but it is just that when those other even more urgent things happen, the security falls down. We are just implementing ITIL so it might help to go through that process, it might come under that banner, in a formal sense’

‘probably not as high a priority as it should have. Half the problem is we actually spend a lot of time putting out fires, rather than finding the time to educate people how not to start them in the first place’

‘maybe it ought to be but it is not’

‘I think it is acknowledged it is important but the actions are just not there yet’

Findings on Types of Awareness Activities Undertaken

Participants were asked what type of awareness activities were undertaken in their organisation in an effort to determine what is actually occurring (Figure 22). Due to the fact that most organisations undertook awareness activities on an ad hoc basis, the nature of activities varied to a large extent in relation to type, comprehensiveness and regularity. Types of activities in general included email communication, Web based information, staff and student presentations, committee meetings, training sessions, posters, awareness themes, threat alerts, general discussion, risk management, security awareness brochures, videos, orientation activities, inductions, electronic IT system agreements and communication within IT.
A prominent theme was the reliance on email for communication, particularly in relation to virus activity, code of conduct or policy compliance. Presentations and staff discussions tended to focus on IT staff, as opposed to general and academic staff, unless a structured board or committee existed, or a structured program was in place. Several participants indicated their intention to further address security awareness activities through actions such as online training, web based information, presentations and more structured processes. These stated intentions were often in relation to the acknowledgement of the ad hoc processes in place.

**Findings on Adequacy of Awareness Raising Activities**

Ultimately, very few participants actually agreed that existing awareness activities were adequate in raising security awareness to the level that it should be, although many participants partially agreed.

‘*no we are not doing enough, I have put somewhat agree in that you know something is better than nothing, but it could be and you know, more is required*’

‘*it is not adequate in many ways but we are doing the best we can and have to live with the resources we have got*’

‘*No there is definitely more we could do, I mean we need to run a full on campaign*’

‘*we need to pursue a greater awareness program*’
Findings on Factors Effective in Raising Awareness Levels

Incidents outweighed other factors in being singularly attributable for raising security awareness levels (Figure 23). Education through alerting, training or other targeted activities was next cited as effective in raising the profile of security, followed by media and audits.

Despite the great majority of participants indicating that low security awareness levels were a barrier to achieving improved compliance with information security, the actual
factor cited as having played the *largest* role in raising awareness levels was attributable to security incidents or breaches, rather than specific, targeted education. This indicates that awareness in universities is predominantly shaped in reaction to incidents, reflecting a reactive rather than planned approach.

Additionally, reaction to incidents was cited as being more likely to have an initially higher profile, but to then quickly fade into the background once the ‘reality of risk’ had subsided. The findings from this indicate a necessity to have in place effective preventive, detective and corrective controls (both processes and technology) to deal with the inevitable, rather than waiting and then reacting in an ad hoc manner to incidents. This situation is also supported by comments that, where there had not been an incident, the reality of risk was not apparent and was largely ignored. A lack of incidents therefore is a cause of complacency.

‘*It is interesting, people are only aware of security when there is a security breach’*

‘*Actual incidents, when a virus explodes, when a server is compromised, or when the movie industry write to us and say ‘someone has got this movie or this music file’, nothing gets attention like that, incidents mainly’*

‘*Well in reality the best types of activity or events to raise awareness is an external attack’*

‘*I think the most likely ones for that are outbreaks of something or phishing attempts where we’ve told staff about and you can see the reaction for a while after, people reporting things even though they are not quite relevant to what we are telling them about, but at least we have got them thinking about it’*
'when various viruses and worms have got through, one even got through that was introduced by a laptop that has come from somebody’s home from their ISP which has been unprotected, and that has been useful in focusing people’s attention on the need to maintain up to date data files for their anti virus software’

‘The most effective thing is when something gets broken unfortunately, or people misbehave, and that impacts on other people, then at that point, where it affects a group, their admonishment and some activities to try and mitigate the circumstances in the future’

‘It nothing that we have done, it has been just the fact that IT security has got a higher profile in the press, and I suppose little things like the QLD government having legislation that requires us to be a certain standard, and I suppose the fact that every day you see a new incident in the media, like slammer etc that is more than anything we have ever done’

**Findings on Barriers to Improving Awareness Levels**

When asked what barriers impacted achieving improved awareness levels, almost half of the participants indicated barriers associated with resourcing (Figure 24). This included having available time to allocate to awareness raising activities. The second most common barrier was cited as involving cultural issues, including people’s motivation to take security seriously, or an unwillingness to acknowledge the risks, a lack of inducement to retain relevant knowledge surrounding security, and resistance to adopt work practice changes. This area also included cultural barriers due to decentralisation, where the establishing of awareness levels in a decentralised environment was perceived as being more difficult. Several participants also commented on their perception that
security awareness activities were ‘important’, but ‘took a back seat’ due to other, more urgent priorities.

![Figure 24 Barriers to Improving Awareness](image)

Figure 24 Barriers to Improving Awareness

Typical comments are:

‘**Inadequate resourcing - not enough time to do it all**’

‘**Resourcing, yep simple as that**’

‘**Well it is really time and resources**’

‘**Resourcing, and a follow through is another issue**’

‘**Resourcing would be a first one obviously; the other thing would be the general cultural environment that we work in, it is very open in the higher education in the sense that you know, you want your academic freedom and your other bits and pieces, and the capacity to learn, and so that’s an obstacle in one way because there is again that cultural perception that it is a bit of a free for all so to speak,**’
in that the rules are very loose, or the guidelines so to speak, and it is overcoming that perception, you know 'No this is an important matter and it will, you know, have a long term impact if we don’t address it and abide by the rules', so I just see that cultural barrier there’

'It is more the fact that our University have their priorities elsewhere, it doesn’t see immediate benefits of investing money in that’

'I think probably the common thing is getting the resources to provide the information’

'I think not everybody would agree with that particular approach (above), so we don’t have a unified or consistent approach and we don’t have the resources’

'Time and priorities you know’

'Time to do it, where it fits in with other priorities, I guess then the time and resources to get out and do it, coordinating it all, and the other barrier is that you can tell people a message but they have to have an interest for it to make a difference, so you have to tell them at the right time, the right things at the right time’

'Priorities - and I suppose security is still viewed something that stops me doing things, rather than an enabler’

'I have taken approach of chipping away and changing culture slightly rather than a big bang approach'
'I think some of the barriers are that people are not interested, they are only interested in using their systems, I think that some Heads of organisational units are less interested, I think the main barrier is that so many people don’t perceive as a real threat'

Findings on How to Improve Awareness Levels

While specific suggestions on how to improve awareness levels varied, a common thread amongst participants involved several predominant factors: having a structured awareness program, targeting all levels of the organisation, and being properly resourced. Automating awareness as much as possible through basic information and training and electronic agreements was also seen as beneficial.

‘you need that coordinating view that looks across security and sees the dependencies or the interrelationships, so it’s that shared information, from different people in different boxes, that understand the consequences, that might flow laterally instead of vertically’

‘We need a more focused program on what security is to the University. It’s got to have senior management championship of it, it’s got to have both technical resources and management resources at the operational level to actually develop the program and manage it to be implemented’

‘We need to increase staff and student awareness through a program’

‘Well development of a formal program with information to people about IT security issues I think’
4.7 Coding Results for Security Compliance

Participants were asked a number of questions in relation to compliance with security. This included questions related to behavioural compliance, technology and security threats, funding and barriers to compliance. This area also included a question on identification of the critical success factors that participants considered essential to effective security management. Table 9 provides a coding summary for this area, and Figure 25 depicts coding relationships.

Table 9 Coding Summary for Security Compliance

<table>
<thead>
<tr>
<th>Code</th>
<th>Density</th>
</tr>
</thead>
<tbody>
<tr>
<td>Awareness and Understanding of Risk</td>
<td>25</td>
</tr>
<tr>
<td>Response Capability</td>
<td>17</td>
</tr>
<tr>
<td>Culture of Compliance</td>
<td>16</td>
</tr>
<tr>
<td>Measurement of Incidents</td>
<td>16</td>
</tr>
<tr>
<td>Inadequate Human Resources</td>
<td>12</td>
</tr>
<tr>
<td>Benefits of a Structured Approach</td>
<td>11</td>
</tr>
<tr>
<td>IT Centralisation</td>
<td>10</td>
</tr>
<tr>
<td>Information Security Governance</td>
<td>9</td>
</tr>
<tr>
<td>ITIL</td>
<td>8</td>
</tr>
<tr>
<td>Allocation of Funding</td>
<td>7</td>
</tr>
<tr>
<td>Improved Security Management</td>
<td>5</td>
</tr>
<tr>
<td>Academic Freedoms</td>
<td>3</td>
</tr>
<tr>
<td>Issues with Enforcement of Security</td>
<td>1</td>
</tr>
</tbody>
</table>
**Figure 25 Assigned Codes for Security Compliance**
Findings on Measuring Security Compliance

When asked if the effectiveness of security or the value of security was somehow measured, few universities indicated that this occurred. The primary methods stated for measurement of security involved Key Performance Indicators (KPIs) against business goals and plans, also empirical data on security incidents, viruses and availability. Most Australian universities are not currently measuring the performance of security against these benchmarks (Figure 26), instead focusing on security incidents as a measurement as opposed to the enabling nature and value of security. This continues to context security as a cost function. Examples of this are:

‘Only in the sense that we certainly measure the number of viruses that are hitting the Uni’

‘We release periodic KPIs to senior management on various factors for example the number of viruses trying to get in vs. how it breaks down what we are doing to them etc.’

‘Probably really comes down to you know how many incidents we get through our job system and everything else, that have to do with related security issues’

‘We do have a repository of incidences which we collect and analyse it’

Several participants indicated that measurement of security was difficult, due to the intangible nature of both risk and risk mitigation, and the difficulty in illustrating the enabling value of information security.

‘It is always difficult to measure how effective IT security is, because there aren’t very well established baselines, so you can’t say ‘well we are adhering to.....’
Those participants who were measuring security against benchmarks, tended to use Key Performance Indicators, (KPIs), business goals or audits, as reflected by:

‘IT security and stuff is rated as a service, it has KPIs to see how compliant they are with 17799, and it gives us what is called the capability maturity model. We engaged an external auditor to come and do the KPI for us’

‘I guess the measure for me and I will speak from an audit perspective, compliance is measured against KPIs that audit have in place, and those set by our own management, now they are also measured against some Australian standards for some things, but are not broad enough in my opinion’

‘17799, that audit was done externally by an external consultant, it gives a whole lot of issues, and then each of those issues are actually planned and actually monitored that we carry them out’

‘Self assessment against our structured approach, but no KPIs, we have business goals’
'We measure everything against our stated technical or strategic goals in our business plans'

Findings on the Culture of Compliance

Participants were asked if they considered that a culture of compliance existed across their organisation, reflected in work practices (Figure 27). Participants tended to be relatively evenly distributed across overall agreeing or disagreeing with this question.

![Culture of Compliance Towards Security Reflected in Organisation](image)

Figure 27 Participants Whose Organisation Had a Culture of Compliance

Typically, those participants that agreed tended to have a centralised model of IT and offered the following type of views:

'Agree - absolutely, in the context of a central body, with absolute certainty, and you know, growing out there with people that use the services'

'Agree, yes there is a culture of compliance, because again it is easy because you are centrally driven, it is easy for us to drive things'

'Because it is so centralised it is easy for us, it helps'
'I have got absolute control over the network'

'Yes we don’t give them any choice'

'The business I think as a whole sees security as an important process that needs to be done, the majority of staff are security conscious and as usual you get some that aren’t'

Participants who tended to disagree cited a lack of knowledge and awareness as an issue, or cultural issues with comments such as:

'Disagree that we have a culture of compliance through our institution, the comment is that ‘not yet possible due to a lack of awareness and technical solutions by the majority of system user’

'It is not their fault but they are ignorant of the issues involved'

'There is reasonable compliance there but I think some people just don’t understand'

'It is driven by lack of knowledge; partly it is an educational issue'

'No I don’t think so, somewhat disagree, it comes back to the levels of awareness'

'No I think they don’t really know what to comply with, the ambiguity and misunderstanding over security in particular'

'I think it is a cultural issue, because there are groups of academics out there who resent the managerial aspects of
security, it never happened to Unis in the last decade or so, so while some academics are ok and understand the need for compliance and that sort of thing, there are others that really resent other trying to tell them what to do’

‘Culture of compliance is only in the services side, not in the wider community’

Findings on the Capacity to Detect and Defend Against Threats

The majority of universities indicated that they are reasonably confident of their capacity to detect and defend against incidents (Figure 28). However, universities did raise concern over their inability to strictly control the workstation environment.

While the majority of participants were confident of their institution’s capacity to detect and defend against security incidents, they cited the top causes of security incidents as being viruses and malicious software, user errors or non-compliance, system administrator errors or non-compliance, followed closely by cyber or internal attacks. These results should be considered in light of the fact that detection rates for incidents are unknown, and therefore the incidents that are most visible (i.e. viruses and malicious code) are being cited as the highest cause of incidents. There remains the possibility that
incidents that are not being detected are of great concern, particularly considering that insufficient ‘Incident Detection and Response Capability’ was rated as one of the top five barriers to improving compliance. The responses that reflected general consensus include:

‘Yes I think we are, again it is once somebody has told us, it is that reactive thing but I think when we do find out about things we do have a lot of information we can go and look through and work out what has really happened’

‘Yeh it is interesting, but it’s that positioning that is not just about the technology, but it is also about the people and process and the relationships’

‘I think we have good response procedures, we also have fairly robust defence mechanisms in place, we are looking to improve upon this’

‘Surprisingly, after having said we don’t have this or that, we are well-positioned to detect and defend, because of the architecture and the things that are now in place’

‘Unfortunately the university is poorly placed to respond to anything but the simplest incidents. There are only elementary technical controls in place to defend from incidents, and little to no monitoring to detect attempted or successful attacks. At present, the university is very reactive and primarily relies on third-parties to alert it to issues’
Findings on the Main Causes of Security Incidents

Most participants stated that they believe they are well-prepared with counter measures to viruses at the gateway level, suggesting a larger problem with viruses is user awareness and work practices.

The number one cause of security incidents was cited as viruses and malicious software, followed closely by errors or non-compliance by the user community (Figure 29). Chief among the concerns was the sophistication of virus related threats combined with a lack of user awareness. Typical statements that reflect each category in Figure 29 include:

‘Viruses and malicious software - because people don’t report incidents as much as we would like, we don’t get the full picture as to what is happening, you really only know when something goes wrong’

‘User errors or non compliance - business users with trusted privileges, not being sensible’

‘System administrator errors or non compliance - we have had some security incidents with IT support staff in the faculties through a lack of knowledge or awareness’
'Cyber or internal based attacks...obviously just your own staff, that is what I mean by internal attacks'

Findings on Current Security Issues of Concern

When asked about concerns with specific security issues, participants indicated that the increased frequency and sophistication of viruses, worms, spyware and other malicious software, caused most concern (Figure 30). In particular, the advancements in social engineering and keystroke loggers, and the resultant capacity for system compromise were raised. This concern is extremely valid. Symantec Corporation release their ‘Internet Security Threat Report’ each year. The 2004 report identifies a 64% increase from the previous six months in Windows-based virus and worm variants.

![Figure 30 Top Three Security Threat Concerns](image)

The Symantec report also identified emerging trends and indicated that an exponential increase is likely to be seen in the use of bot distributed worms and malicious scripts for illegal and financial gain, client side attacks, increased attacks through audio and visual files, increased risks with spyware and adware, and in general an increase in the frequency and sophistication of attacks.

Access control was also rated highly, both in terms of account management and use, but also the lack of access control management for workstations, network access control in
relation to corporate systems and databases, and authentication. Access control also encompassed a lack of regular firewall auditing.

'I am concerned about the new threats in the non traditional viruses, like the mobile phone virus, that is one example, and also the cost and complexity, because every solution is like a piece meal response for it from the industry’

'I am becoming more concerned about the smarter types of spyware, the sorts of little utilities that get installed on a PC that might do keystroke logging that then report back to base through some means’

Several participants indicated their concern at the system compromises now widely publicised in American universities, and the potential for this type of attack to be more commonplace in Australian universities. Additionally, poor security applied in systems development, particularly in Web applications, was noted. Pertinent comments relevant to this question are:

'I essentially have gone for cyber or internally based attacks. IF someone compromises our web front end to get to the Oracle database end and do this without us ever knowing’

'I am looking at all of the data break ins in the states, and the personal data coming out of that is a worry’

'It is that internal attack by a knowing party’

Other areas that will grow for Universities is financial risks, in terms of their financial management systems, other internal administrative systems... people looking to
gain access to corporate information’

‘I think again, because of our exposure to the Internet and the broadness of our networks, access to that corporate information I think is a big security risk, or it will be a growing security risk’

‘I guess as I said system administrator errors or non compliance, that tends to flow through with you know change management’

‘It is not the be all and end all the fact that we have had firewalls, we have had them in place but not the configuration in place, and then we have got to manage those, and at the end of the day it gets down to process and people, because 99% of the time the technology will do what it is meant to do’

‘It is strongly for me as a manager, the whole organisational culture, the threats vs. the Academic freedom cries’

Findings on Security Spend

Most (80%) of organisations indicated that investment in security constituted between 1-5% of the central IT budget (Figure 31). A reasonable benchmark for funding based on global surveys for IT, shows that security spending is 3-5% of total IT budgets, rising to 10% for organisations with higher security requirements (such as finance and medical organisations). It is only when security becomes established as a multi-disciplined, multi-team facet of the organisation with a dedicated budget does it get the required recognition by the organisation.
Findings on Plans for New Security Technologies

Participants were asked what new security technologies they were considering in the future. Participants generally referenced firewalls, Intrusion Detection Systems, stronger authentication, workstation registration and security event management-based systems.

Findings on Barriers to Improved Security Compliance

Concern was expressed by several universities, in particular those that had incurred a serious breach on one or more corporate systems in the past, and suggested that attacks on university corporate systems are likely to rise (Figure 32). Participants suggested the rise in attacks on American universities reflected cause for concern for Australian universities as well. Those universities that do not have corporate systems protected by internal firewalls also expressed a priority to move to minimise risk in this area. The core issue surrounding compliance with security is the fact that drivers for regulatory compliance in relation to security are still emerging for Australian universities. At the same time, universities lack an intimate understanding of how well their systems are actually protected in relation to requirements. It is likely however that regulatory compliance and corporate policy management drivers will grow, and therefore be key determinants in how security management models look in the future.
Another issue for compliance is associated with the fact that the tangibility of measuring the effectiveness of security spending is very difficult. Therefore loose compliance drivers linked with the difficulty in understanding the effectiveness of approaches has resulted in compliance being fragmented across the organisation.

Figure 32 Barriers to Improving Compliance

'What keeps me awake at night is the possibility that someone in some part of the organisation has some dysfunctional culture going on which is causing an individual to go absolute bananas and trying to take the place apart'

'The threats vs. the Academic freedom cries'

'I think funding and resourcing is tied to the inability to the last point (measurement), it is a cyclic thing, we have to justify the benefits of having a good security program, and from there resources will be allocated, and then from there we justify it again, and it goes round and round, it is a cost centre and a ROI or benefit figure'
Findings on Improving Security Compliance

Although technology is a key factor in protecting systems, the people and processes that are integral to ensuring that technology is appropriately placed, also need to be coordinated under a successful management framework. This is particularly the case considering that as demand for open systems expands, more threats emerge, more point based technology solutions appear, and consequently a patchwork of technology-based systems develops. An integrated security management system that provides meaningful reporting on security would assist.

There is a need to bring together information from existing disparate technologies. It is becoming increasingly necessary to effectively manage emerging threats and at the same time increasingly difficult to manage the technology responses by industry to those threats. So far, the main guiding framework that offers a security management model, 17799, does not necessarily overlay well with the actual operational functions of security, and comments from participants indicate that its adaptation is difficult. Moving forward it will be increasingly vital that universities are able to understand, measure and demonstrate the effectiveness of security approaches, in order to ensure that standards and regulatory compliance are met.

Improved governance, being adequately funded and resourced and increased awareness and training rated as the top three areas necessary to make major improvements in compliance with security. Within a structured approach, having the right framework not only applied to management of processes, but also to technology controls including standards for systems development, operating standards, best practices and the ‘nuts and bolts’ of tightening security controls. The main focus from a technical perspective that participants indicated that they should focus on in the future, included improving network security architectures, particularly in relation to use of virtual firewalling technology, especially for internal corporate systems (Figure 33).

Rated highly also was embedding security more effectively in systems development, VPN and encryption methods for wireless, and attempting to gain improved control over
the account management process and desktop environment. Participants noted that without adequate user awareness, increased reliance on technology-based controls could often be helpful in ensuring that a transparent process for safeguarding systems was in place, mitigating the lack of end user awareness.

![Figure 33 Areas for Improved Compliance](image)

**Figure 33 Areas for Improved Compliance**

‘**Culture of commitment and support**’

‘I think we have covered it, we’ve got to put a focus on it and develop the program, and we’ve got to have the resources to implement it’

‘**Better funding and resourced, better understanding and knowledge at all levels**’

‘I just would be repeating, adequate staff to implement a security plan, measure effectiveness, and to attract necessary resources and funding’

‘**An increased awareness and understanding, a continual communication message and engagement of key stakeholders**’
‘Resourcing and funding, increased education, communication and user awareness’

‘I think the biggest thing is user awareness of policy, understanding the risks’

Findings on Critical Success Factors

Participants were asked what they considered to be the critical or essential factors to enable effective security management (Figure 34).

Figure 34 Top Three Critical Success Factors

A broad categorisation of responses resulted in three major areas: senior management support, governance framework and structure, and awareness and education. The first area, senior management support, cannot be over-estimated, as it significantly affects the other two areas, supporting a governance framework, together with backing and supporting an overall awareness and understanding throughout the university community. These results also corresponded with a major theme emerging from this survey, being a requirement for an increased focus and sustained efforts by participants in improving the overall approach, structure and governance of security. Although awareness and education ranked highly and consistently, and despite the fact that it was ranked as an area requiring improvement, awareness and education remains a difficult,
time-consuming and resource-intensive task. This would be made easier through automated processes, awareness tools and resources, and senior management support.

‘There has to be organisational understanding that security is an organisational wide responsibility’

‘I think awareness and user education is critical, I think it is critical that the university works as a whole to resolve the issue instead of each decentralised group working in isolation to solve a specific problem’

‘first thing would be a coordinated approach to security’

It’s gotta be investment of the Executive – that is the absolute key, the rest of it doesn’t matter a toss if you don’t get buy in at that level’

‘You need commitment from management to actually appreciate that you need to do these things to mitigate risk’

‘First of all a structured approach’

‘Can I give you a text book answer? Senior management support’

‘I think we just have to get some sort of acceptable framework in place’

‘The right technologies in place, a structured approach for it, and as much as possible integrating security from a business point of view rather than just a technology point of view’
Findings on CAUDIT Involvement

Participants were asked how CAUDIT could assist with the security management process, policy, awareness and overall compliance. Overall most participants were positive towards CAUDIT’s potential to assist with university sector based policy, standards and general awareness raising. The general view was that CAUDIT could assist by facilitating workshops where institutions could exchange information, and that CAUDIT could assist with the development of national standards relevant to the higher education sector for policy, best practice and security management. Table 10 provides a coding summary for this area, and Figure 35 depicts coding relationships.

Table 10 Coding Summary for CAUDIT Involvement

<table>
<thead>
<tr>
<th>Code</th>
<th>Density</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workshops and Information Sharing</td>
<td>31</td>
</tr>
<tr>
<td>Input on Security Policy</td>
<td>25</td>
</tr>
<tr>
<td>Provide Best Practice</td>
<td>21</td>
</tr>
<tr>
<td>Guide Security Management</td>
<td>13</td>
</tr>
<tr>
<td>Assist Benchmarking Universities</td>
<td>11</td>
</tr>
<tr>
<td>Improve Senior Management Awareness</td>
<td>11</td>
</tr>
<tr>
<td>CAUDIT Register of Security Incidents</td>
<td>6</td>
</tr>
<tr>
<td>Provide Security Awareness</td>
<td>5</td>
</tr>
<tr>
<td>Develop ROI Model</td>
<td>3</td>
</tr>
<tr>
<td>CAUDIT Security Group</td>
<td>2</td>
</tr>
<tr>
<td>Security Risk Management</td>
<td>2</td>
</tr>
<tr>
<td>Vendor Collaboration</td>
<td>2</td>
</tr>
</tbody>
</table>
Figure 35 Assigned Codes for CAUDIT Involvement
The concept of CAUDIT facilitating or participating in workshops, meetings or general ‘get togethers’ was a prominent feature of participants’ feedback. This is reflected through comments such as:

'I think also there is an opportunity for best practice, workshops to get together and share what we should be doing and how to implement it’

'I think what would be beneficial to all of us, for CAUDIT or the AVCC perhaps, to fund a retreat for the IT Security staff in Universities, so that we can get together, share ideas, learn from each other’

'So it might be organising conferences or sharing experiences, because I would suspect a lot of people fighting bushfires around the place, so it might be a good idea to just find a day or two and sit down together, share our experience, strategy, perspective on how higher education trend is going’

'One day workshops through CAUDIT that organise with AusCERT would be good’

'As member of CAUDIT I see great value in people involved in sharing information if nothing else and how that is implemented’

'It would fall into the short-circuiting category by coordinating or being able to produce a library of reference material that can be accessed rather than everyone having to reinvent the wheel’
'From my point of view I would be interested in some sort of workshop, that deals with, I am not sure if any other Universities have implemented their security management to a standard'

'More collaboration across the Universities'

'If there was a forum where security staff from different Universities could meet that would not be wasted'

Participants expressed consistent views that CAUDIT could assist with providing best practice and policy, and raising awareness. The types of comment that typify this view include:

'I think it would be useful to compare the policies of the different universities and try and come up with some standards'

'Something about the CAUDIT best practice guideline that says we should have a security policy committee. Benchmarking and best practice guidelines are what CAUDIT could do, so we can see what it is that other Universities do'

'Because when is all said and done, we are all working with the same issues.....typically we are re-inventing the wheel all the time, whereas if you could compare what we’ve got, it would be to the benefit of everyone. It would be a great help if CAUDIT could have a template for security policies'

'Yes, by assembling a set of policies known to be effective
Participants were extremely interested in being able to rate or benchmark themselves against other higher education institutions:

'It would be interesting to know how other Universities approach security with their organisational structures'

'Yes they could help with training and awareness, and benchmarking, providing sharing of information across the Universities'

'I am also wanting to know what others are doing, we are all in the same boat'

'The role that you are playing, in publishing of this survey, is fantastic, it’s always great to see what other Universities are doing'

'I think it would be useful to compare the policies of the different universities and try and come up with some standards'

'Something about the CAUDIT best practice guideline that says we should have a security policy committee. Benchmarking and best practice guidelines are what CAUDIT could do, so we can see what it is that other Universities do'
5 Discussion

This section provides a critical interpretation of the key findings from Section 4. In addition, a discussion specific to each of the five major areas upon which the survey focused is provided. Key themes are then used to further provide an explanation and build support for the ‘security practitioner’s management model’, and are supported by relevant literature.

5.1 Discussion on Senior Management Involvement

Current Status of Senior Management Involvement

An interpretation of the findings on senior management involvement indicates several key patterns. The coding results established that funding and resourcing is considered to be significantly important and is a major function provided by senior management. This is a function that impacts directly on the capacity to deliver security and associated services.

As evidenced through the coding results, participants tended to focus on funding as a primary gauge of support levels by senior management. In other terms, participants tended to view the level of support received by senior management as being represented by the overall provision of funding and resourcing. In broad terms, participants consider senior management support as critical and essential to information security in the organisation. This was evident by comments in the survey within the ‘Senior Management Involvement’ section, as well as the area of ‘Senior Management Support’ ranking first out of the top three critical success factors as ranked by participants.

Following from this, the survey established benefits to those organisations that had in place active reporting and communication structures with senior management. This was due to the engagement of senior management which in turn led to a level of commitment. However, despite the requirement for senior management support for
information security, less than one third of universities indicated that they regularly reported on information security to senior management. The percentage of organisations reporting regularly to senior management also correlated closely with the approximately one third of participants who indicated that they believed senior management provided an appropriate level of support for information security. Those organisations that actively engaged senior management reported a higher level of understanding from senior management regarding the importance of information security.

Key Issues Surrounding Senior Management Involvement

A number of key issues emerged in relation to senior management. These include the levels of senior management support, the overall culture of compliance with security fostered by senior management and challenges in enforcing policy within a decentralised, non-compliant culture. Additionally, inconsistent standards applied across the organisation, the belief that security in universities is less applicable compared with other institutions such as financial or telecommunication institutions impacting the overall prioritisation of security. Additionally, the perception that a culture of non-compliance is fostered when regulatory initiatives are not able to be monitored or enforced was raised in this area.

A strong correlation existed between participants who considered senior management to be ‘involved and engaged’ in security, and corresponding levels of support received from senior management. Similarly, institutions who indicated that support was lacking correlated with those institutions who reported that senior management was either not ‘engaged’ with security or had a low level of awareness surrounding security issues. The findings from this survey are also supported by findings from Knapp et al., (2006) in their survey which involved open-ended questions answered by 220 certified information system security professionals. The results of their study indicate that senior management support positively impacts security culture and policy enforcement. Specifically, their research found that ‘evidence suggests that top management support is a significant predictor of an organisation’s security culture and level of policy enforcement’. Similarly, another survey published in 2004 of key information security
issues found that senior management support was ranked number one out of the top 25 security issues (Knapp et al., 2006).

These findings lead to several primary interpretations. Firstly, senior management support is considered to be critical to the success of the information security function, particularly by way of funding and resourcing. A range of issues however was raised with funding and resourcing. These include competing priorities, lack of funding to allocate appropriate staff to specific functions in security, funding for security not incorporated in the IT budget process, projects not including funding for security, security taking a back seat and lower priority, security being seen as an expense (as opposed to an investment), security funding not being justifiable due to lack of measurement, and lack of time to complete security comprehensively.

Secondly, not withstanding other organisational constraints, senior management is more likely to be supportive of security if they are informed and engaged. Again the findings from this survey reflect similar findings to the survey undertaken by Knapp et al., (2006). Evidence from the findings indicates that a significant relationship exists between senior management support and the status of security overall. It is noted that in organisations where low levels of senior management support exists, the culture and enforcement of security policy is likely to be lowered and the culture will reflect a tolerance of reduced security compliance. The practical impact is that security practitioners should understand the impact of senior management support on achieving security effectiveness.

Although previous research (Detert et al., 2000) indicates that most efforts towards cultural change mainly proceed based on senior management culture, other approaches are also possible. An interesting theme that emerged from the data was the level of polarisation that occurred between IT Directors’ views on whether senior management ought to be, or was required to be, involved and engaged in information security. While most participants tended to express a desire for more involvement, support and direction from senior management, not all participants agreed. In some circumstances IT
Directors expressed the view that senior management culture alone provided a unique organisational-wide culture platform. Conversely, little attention was given to the values and beliefs of lower-level employees and their potential to impact sub-cultures of support for security.

Thirdly, increasing senior management awareness is most likely to be achieved by ensuring that senior management is included with the overall ‘structure’ of security management. This is achieved through the process of regular liaison and reporting with the view of increasing understanding and awareness of risk. Dutta and McCrohan (2002) argue that the three cornerstones of security include critical infrastructures, organisation and technology. Within these cornerstones, they argue that security lapses are generally a management failure as opposed to a technical failure. This is because when the security function is left primarily to the IT technical section, it mainly strengthens only the technology cornerstone. Therefore, balancing the three cornerstones is an issue of corporate governance and requires senior management involvement.

**Improving Senior Management Involvement**

Funding was a prominent and major issue raised by participants. Some participants held the view that as long as funds to IT were flowing, all was well and security could simply be provided without further direct senior management involvement. Within limited circumstances, this can be adequate, with the desire to get the utmost value from security funding common. In part the difficulty in funding is linked to the fact that a key attribute of security spending results in mostly intangible results (i.e. you do not see what it is that you are protected from). A realistic approach therefore for spending on security is to rely on a business impact analysis to justify the costs associated with risks. Research indicates that management experiencing tight budgets is likely to want to implement the most amount of security possible for the least cost. Achieving this requires the input of information security staff for the best methods of remediation in terms of equipment and people (Templeton, 2004). Therefore a combination of
appropriately addressing security risks in a business context is necessary for improved funding.

In order to elevate information security out of the technical realm into the business realm, it is argued that having a structure for security provides a tangible context for senior management (Dutta and McCrohan, 2002). This facilitates senior management viewing security from an enterprise approach and lends support to the security practitioner’s management model, which advocates that a structured approach be applied to all layers of the organisation. The proposed model represents senior management within both the ‘contextual’ and ‘conceptual’ layer of the model, and is traceable throughout the various layers of abstraction for the model.

An emergent theme from the analysis was that the universities that reported appropriate senior management buy-in also typically involved adequate representation of senior management on various committee structures. Security committees that include senior management representation can provide an appropriate mechanism to represent the information security program by establishing buy-in across the enterprise. Fitzgerald (2005) suggests that a security committee has the capacity to facilitate collaboration, ensuring that representative view points are taken into consideration. Without a council or committee, the Information Security officer is effectively working in isolation, attempting to move initiatives forward, and obtaining business management support one person at a time. Similarly, Peltier (2004) maintains that for an information security management program to be effective, an information security steering committee must be established, to act as a champion of security.

Von Solms (2001) argues that ensuring senior management includes information security as part of corporate governance would greatly simplify the efforts of security managers. This is most likely to be achieved through proper representation of senior management through a committee or forum. The establishment of a security committee provides the opportunity for security to be on the corporate agenda for Universities. Von Solms (2001) specifically states that ‘information security is a direct corporate
governance responsibility’. Unfortunately security is not always considered as being an essential part of good corporate governance by senior management, reflected in the lack of established forums or committees regarding security and the fact that security is rarely cited on documentation related to Universities’ corporate governance.

Where possible, the role and importance of information security should be included in documentation that relates to corporate governance. From a business perspective, documentation and publications that link the requirement for senior management corporate governance to include the responsibility for solid internal controls would be an effective mechanism. The literature supports the necessity for internal controls to rely on information security – therefore establishing security as an integral part of corporate governance, be it indirectly.

Without senior management support, the challenge is greater. A grass roots approach to information security support however is still possible. The importance of subcultures cannot be underrated. For the purposes of this section, however, it is appropriate to note that although a strong correlation existed between senior management involvement and senior management support for security, the net result of this tends to be reflected in levels of funding for security. This means that there is still capacity to drive security from a ‘grass roots’ level with cultural norms being driven from within IT for good practice. The idea that a grass roots initiative towards affecting a culture of compliance towards information security is further expanded on in Section 5.7 ‘Security Practitioner’s Management Model’.

5.2 Discussion on Security Management Approach

This section discusses the current status of security management approaches, emerging issues and how security management could be improved.
Current Status of Security Management Approach

In this section, the single most recurring theme to emerge was the requirement for an improved security management structure, and the need for a coordinated approach. The use of terms such as ‘ad hoc’, ‘reactive’, ‘structure’ and ‘coordination’ were frequently used by participants, both in terms of describing issues as well as solutions for security management. A thematic pattern to emerge was that increased or improved structure and coordination would improve the ways in which security was being managed. This extended to how security would be perceived by management and staff.

Almost half the participants only ‘Somewhat Agreed’ that the existing management approach adopted for managing security was effective, and less than one third agreed that their approach was effective. Almost 60% of participants cited ‘More Structured Approach’ as being required to improve the current management approach, followed by improved awareness and additional resourcing. The most commonly cited approach for management of security was through incident management, which tended to be reactive in nature.

Adoption of a more structured management approach was therefore the number one factor cited by participants as a necessary step to improve the security management process. Improvement of security management was cited by the majority of universities as firstly requiring a dedicated and focused resource for coordinating information security, then adopting a well-defined, structured and coordinated approach, and ensuring that this approach effectively integrated across the business as an enabler.

Many participants stated that they would like to see university sector applicable standards - standards that were designed to provide universities with a baseline, allow benchmarking, and prevent universities from having to ‘reinvent the wheel’. This was stated despite less than 50% of participants citing an active use of existing standards. It was acknowledged that many university security practitioners and administrators already had well-developed locally based, technical standards that they apply to security, but lacked a management framework.
This situation indicates that a structured approach is deficient, despite the availability of references such as the ‘AS/NZS 17799 Code of Practice for Information Security Management’, as well as a large range of other security best practices, guidelines, standards and frameworks. The pertinent question here is not ‘what’ to implement (although this is extremely important), but more ‘how’ to implement security. This problem appears to be common-place across higher education institutions in Australia, and is reflective of the cultural impediments to security, as well as the general lack of maturity of security implementation.

**Key Issues Surrounding Security Management Approach**

The key issues that emerged with management of security included problems associated with the current management approaches adopted for information security, the lack of coordination of information security impacting effectiveness, conflicting priorities and standards within universities, and the difficulty in easily identifying industry applicable standards. A significant challenge put forward by participants was that existing management standards were not always applicable to Universities. Although 17799 was often quoted as being a preferred management standard, several participants were critical of the standard, suggesting that conforming to this standard would be highly time-consuming and resource intensive, and that they were not necessarily applicable to the university environment.

Another prominent issue arising for many security practitioners was cited as not having control over the IT environment (both technically and culturally) due to IT decentralisation. Conversely, many participants stated that centralisation of IT made life easier in that control over the network could be established more readily. Arguments could be stated for and against centralisation. The main argument for centralisation is centralised control over decision making, standards and enforcement of policy. The main argument for decentralisation centres on the increased access to resources outside of the main IT department that can, in theory, apply a security focus to their IT environment.
The issue of centralised and decentralised environments appears in many universities, not just in Australia. Templeton (2004) provides interesting comments on the culture of Indiana University in the United States. These comparisons are equally applicable to the Australian university environment. Indiana University has a significant focus on security and has developed a comprehensive information security management program.

Despite this Templeton (2004) describes the university environment, attitudes and opinions of technicians as varying considerably. In relating the experience of advancing information security in the Indiana University, Templeton (2004) stated that having documentation telling people how to secure their systems and network alone was not enough. For example, faculty staff may have concerns that security will be a mechanism to restrict operations of computers and use of the network. This can be seen as an impingement upon rights or an inhibition to academic freedom.

Additionally, Templeton (2004) cites that when problems arise with computers, perspectives take a dramatic shift. Ownership of the computer and its contents is retained by the system user, but ownership of the problem and responsibility for its remediation can often be relinquished to IT staff. Templeton (2004) notes that design and architecture often spawn differences of opinion between technical staff.

Technical staff often adopt a very strong sense of ownership of the infrastructure under their technical control, and are not always willing to have other people interfere or tell them how it should be done. Also technical staff often focus mostly on system availability, suggesting that influencing technical staff in either a centralised or decentralised environment should take into account the technical staff focus.

By focusing on a balance of the aspects of confidentiality, and integrity as well as availability, security managers have a common interface to work with technical staff. If this is done well, it can allow an expansion of focus to include highly functional and reliable infrastructure (Templeton, 20004). This issue is applicable to Australian
universities and of concern from the study was the reactive approach adopted, and the lack of compliance outside of IT to security.

**Improving the Security Management Approach**

The main three suggestions for improving the security management approach included having a more structured approach, improving awareness and additional resourcing. It was obvious from some comments that a fragmented approach existing in managing security. In part this exists because of a lack of an enterprise security approach, but also decentralisation plays a part.

In comparison a large international university, the Indiana University in the U.S. maintains a structured framework which they advocate is necessary to establish a valid authority to develop and enforce the information security initiative (Templeton, 2004). This authority needed to be seen as coming from the top. Having a framework supported by top management is important for acceptance of security by the entire campus. Indiana University necessarily adopts an approach that spans the enterprise within a framework perspective.

In terms of decision making and cost allocation for IT security, security should be not seen as spanning homogenous entities, but rather across divisions that use varied information systems according to Kumar, Telang and Mukhopadhyay (2006). Decisions for individual entities relating to allocation of funding and controls should be applied within an enterprise framework. This framework needs to take into account the fact that the security of each division or entity may affect other entities resulting in inter-dependencies giving way to a ‘lowest common denominator’ level of security (Kumar, Telang and Mukhopadhyay, 2006). This is important from the perspective that decisions to implement uniform security controls may result in inappropriate allocation of resources and controls to different sections throughout universities.

One of the most compelling pieces of information that reflected a reactive approach for managing security in universities was the fact that incident management was cited as the
number one approach to managing security. This highlights the reactive nature of how security is being managed, as many participants stated that managing and responding to incidents formed a large component of their work. While incidents may be unavoidable, an analysis of the data indicated that an improved structure would see threats better mitigated in the first instance.

Universities are typically inundated with security information that stems from disparate and often decentralized security systems, often operating in individual silos. On the technology side, a lack of integrated security event information provided by IT systems contributes to current fragmented approaches in security. One of the factors impacting the capacity of information security practitioners to manage security is the existing disparate and fragmented approach to implementing point based technical solutions.

These technical solutions result in fragmented security event management. To redress the current fragmented approach to security event management, security practitioners require centralised real-time management capability, associated with contemporary Network Operation Centers (NOCs). Many universities have deployed NOCs that manage and monitor the network traffic. The NOC's primary function is to establish and maintain the health and wellness of infrastructure and keep the network running.

An effective Security Operations Centre (SOC) has the capacity to provide situational awareness - a correlated picture of what is occurring across the enterprise. By gathering information from a variety of devices (firewalls, antivirus, intrusion detection systems, etc.) and normalizing and correlating the information, the SOC provides real-time reporting on what is happening in the environment. One of the benefits of a Security Operations Centre is that it provides an opportunity for security practitioners to manage and respond to intrusions before they put the organisation at risk (Kelly and Moritz, 2006). Therefore this tool is an important aspect to grow and mature in the university security environment, particularly considering the large amount of security incident response that occurs and the current overwhelming amount of information that is not adequately collated and synthesized in a meaningful way.
Although complete incident prevention is not possible, an effective SOC allows security practitioners to identify attacks and limit the damage before it spreads. To address these problems, Kelly and Moritz (2006) suggest that organisations must carefully plan and deploy an SOC that centrally manages and monitors the network and security systems across a diverse IT environment. For effectiveness, a SOC requires the use of a comprehensive security information management solution. This involves taking the time to understand business needs and technical requirements in order for the SOC to complement security policies and network infrastructure.

In considering the reactive approach to security incidents and management, it is noted that the perception of risk is often used as the basis for responding. This was an issue that was raised many times, by way of ‘it won’t happen to us’ where perception was dominant. Kotulic and Clark (2004) note that threats and vulnerabilities are generally not considered until after a security breach has occurred, a view reinforced by participant comments in the interviews. This highlights and reinforces that the reactive state of managing via security incidents is due to risk management being implemented in accordance with the perception that ‘it won’t happen to us’.

From this perspective two human issues emerge, according to Kotulic and Clark (2004), which may help explain the reactive nature to security incidents. Firstly, people themselves cause security incidents, either intentionally or unintentionally and secondly, people make risky decisions that impact an organisation’s response to threats. Kotulic and Clark (2004) propose that the increased importance and potential business risks associated with security threats intensify the potential business impact of a security incident. This position means that adopting a proactive and comprehensively structured approach is preferable. The proposed security practitioner’s management model attempts to address this gap, by providing a structured approach to implementing security. This provides the ‘how’ as opposed to the ‘what’ of security implementation.

Finally, feedback indicated that auditors often used a different standard to 17799 for auditing of security (primarily auditors used COBIT). Although several state
governments have mandated state level adaptations of 17799, not all universities are proceeding in this area. The standard recommends that organisations develop an information security management system based on organisational requirements, and then adapt the standard as necessary. Findings from the survey indicate that 17799 is the preferred choice for a security standard, but a lack of clarity surrounding its adaptation exists. This is partly due to the fact that the existing areas of 17799 do not always map well logically against the operational components of managing security. A suggestion for improvement in this area is to maintain a well-documented management framework that spans across more than one standard to ensure auditor compliance.

The existing standards and frameworks are many and varied, and it is likely that few organisations are comprehensively across all of them. Many participants called on CAUDIT to assist in the development of a set of university sector applicable standards and a best practice framework. In an effort to provide clarity on standards, best practice frameworks and comparisons, the IT Governance Institute has issued a paper entitled ‘COBIT Mapping’. This paper is helpful in providing a common framework for mapping some of the more prevalent standards and frameworks, including COBIT, ITIL, ISO/IEC 17799:2000, ISO/IEC TR13335, ISO/IEC 15408:1999/Common Criteria/ITSEC, TickIT, NIST 800-14 and COSO.

5.3 Discussion on Security Policy

Current Status of Security Policy

The area of security policy highlighted several key aspects. The current status of security policy in higher education institutions is reflected by the fact that most participants tended to consider their policy areas to have received reasonable representation from both technical and managerial stakeholders alike. Participants considered that the policy development process was reasonably satisfactory, and that enforcement of policy, although not always mandated, was basically supported.
Universities did vary widely in how ‘organised’ they were with policies. This could be seen in differences such as some universities having active committees reviewing and signing off on template based policies with active input from policy developers. Other institutions cited that they ‘need to start’ on policy development. The majority of interview feedback occurred in the final question on what could be done to improve on the policy process.

A large majority of participants considered policy to be instrumental in establishing a culture of compliance with security, although many acknowledged challenges associated with policy enforcement. Factors contributing to the effectiveness of policy included having an established policy process that included a formal approval mechanism, engagement of key stakeholders, backing from senior management, as well as active communication and awareness of policy. Those participants that felt the policy process was ineffective cited a lack of participation, delays in policy approval, ‘unwieldy’ policies, a lack of policy review, and difficulties in gaining policy compliance.

**Key Issues Surrounding Security Policy**

While the majority of institutions appear satisfied with extant written policy, the central problem with security policy that was cited is the capacity for policy implementation. This brings into play cultural issues, and as highlighted by the coding results, issues with the human resources side to ensure policy is appropriate to, and adapted by, the organisation.

For policy to be effective, several attributes were noted as being required. These include senior management support, appropriateness of policy to the organisation, awareness of policy and its meaning, and available procedures for implementation. The major themes stemming from this area are several. Development of policy in terms of the actual writing of policy, coverage of policy and how policy should be constructed were raised as issues. The appropriate context for policies, including business requirements down to the low level procedures for policies appeared to often be ‘missing links’ for final implementation of policy. The security practitioner’s model attempts to capture this
requirement through its layered approach by ensuring the ‘Contextual’ layer provides business requirements, and that the ‘Operational’ layer includes procedures and operational support.

During the interview process with university participants, questions focused on both the development and implementation of policies. Many participants advocated the concept of having university applicable policy developed for all universities to share (such as by CAUDIT). In support of this were the facts that many participants considered that developing policy involved re-inventing the wheel, and that universities faced the same or similar situations in terms of risks, technologies and system users. Participants suggested that having pre-defined policy templates would be a useful tool.

Within the literature, there are several different process models for security policy development. Most models focus on the security lifecycle, regardless of the aspect of security that the policy is governing. Most security policy processes omit any serious discussion on issues associated with policy formulation itself. In practice, there is little evidence to suggest that any of the recognised and documented policy development processes are rigorously adopted. Instead, anecdotal evidence suggests that areas of risk are considered and policy statements are basically adapted from existing sources, (Maynard and Ruighaver, 2002).

This approach is taken because it gives institutions an easy and inexpensive method for obtaining a policy. In fact policy development can be achieved virtually automatically for example by purchasing ‘Information Security Policies Made Easy’ (Wood, 2002) or, through Pentasafe Technologies, a company specialising in security policy development who sell a ready made document with 1000+ predefined security policy statements.

This approach can be adopted by some institutions when the policy process is needed in a short timeframe or is perceived as being difficult (Hone and Eloff, 2002a) but there are risks. Broadly speaking, if a process is used to simply ‘cut and paste’ policies and policy statements without context to risk, then a highly inadequate end process is likely
to result (Maynard and Ruighaver 2002, Hone and Eloff, 2002a). By contrast, if areas of risk are focused on, and then policies are ‘cut and pasted’ to address these risks, a more focused and applicable end result is likely. This assumes that policy statements themselves are effective and are of high quality. The issue with pre-developed policy or re-use of existing policies, which is applicable to not only universities but most organisations in general, is that this approach is not necessarily valid for lower level policies.

It was revealed in the interviews that overall responsibility for security policy development often defaults to technical administrators or security officers with insufficient authority or knowledge of the university’s higher objectives. This is often due to information security being seen as ‘IT Security’ instead of ‘Information Security’. Although this is a seemingly slight difference it is one that differentiates between a perception of ‘it’s an IT problem’ and a perception of ‘it’s a business problem’. Policy developed under these circumstances tends to lack ownership and stakeholder collaboration, and can result in important objectives not being considered properly, particularly business goals. Further, adopting this approach does not address enforceability or maintenance of policy.

As noted by Hone and Eloff (2002a), difficulties are also associated with this process in that they do not truly reflect the culture of the organisation. An end result of this is that they do not result in a document that effectively provides relevant direction for information security in the organisation. This is a key issue as a theme emerging from data analysis indicated that the relevant issues were more associated with engaging people in policy development and gaining compliance with policy, rather than obtaining written policy statements.

An analysis of these issues concludes that several factors contribute to policy ineffectiveness. Firstly and foremost, ensuring and monitoring compliance with security policy is difficult. Secondly, the process of policy development itself does not ensure that policies are going to be supported by the university. Policies can often be
statements that are simply accepted by a committee without adequate review of risk mitigation or enforceability. Thirdly, difficulties in actually writing policies were quoted. These typically involved long winded policies (one participant admitted to a 180 page security policy!). Other issues included policies that were not of adequate quality, or provided inadequate policy coverage including a lack of generating specific policies for certain risk areas.

The findings from this research are also supported in previous work by Maynard and Ruighaver (2002), who highlight the fact that very little investigation has been undertaken into an evaluation of how security policies are developed or an evaluation of the process used to generate policies. Findings from this research support the concepts that issues with compliance arise from the process used for both generating and implementing polices.

A large amount of research on security policy has been normative, focusing on stating what should be done rather than the actual impact of security policy on the organisation (Maynard and Ruighaver, 2002, Fulford and Doherty, 2003). Therefore very little research has been forthcoming on what is happening within organisations in relation to security policy. Warman (1995, cited in Maynard and Ruighaver, 2002) notes the contrast between what policy in theory states should be happening and what actually happens in practice with implementation of policy. Additionally, even though audits measure implementation of controls on systems, there is often an inference that the policies have been evaluated as well. A problem in this approach is that any issues with the development and implementation of policy are not necessarily factored into security management processes.

It was evidenced from the interviews that many participants acknowledged that while policy existed, system users did not understand the impact from them. This is a common problem with security policies in that they fail to impact the users ‘on the ground’, according to Hone and Eloff (2002a). To be fully effective the information security policy needs to incorporate and convey both the users’ need for accurate low level
information and direction, as well as high level organisational direction (Hone and Eloff, 2002a). The information security policy should be written in a way that is completely user focused. Using copies of other organisation policies or policies obtained from the Internet can lead to creating a mismatched document that users may not relate to effectively. The main policy should be fairly brief, with supplementary policies and guidelines developed to support the main document and detail the specific topics. An effective information security policy is one in which users can identify what is expected of them.

Many participants in the interviews suggested that developing security policy was in fact a difficult process, and suggested that CAUDIT developed university applicable security policy. In looking for a more ‘universal solution’ to developing policy, it is important that policy is developed appropriate to the risks of the organisation, and that policy development has support from within the organisation. One approach to determine what should be in an information security policy is to consult with the international standards (Hone and Eloff, 2002a).

**Improving Security Policy**

There is wide agreement that good information security policy is the foundation for an organisation’s information security (Baskerville and Siponen, 2002). An effective information security policy is the cornerstone of an information security management program (Peltier, 2004, Maynard and Ruighaver, 2002). Importantly, the policy establishes the concept that information is an asset of the organisation, and that members of the organisation have a responsibility to protect it (Peltier, 2004, Maynard and Ruighaver, 2002). It follows therefore that assessing the end product (the status of actual security), should also be accompanied by an evaluation of the quality of the security policy process. This includes both the development and maintenance of security policy.

Development of security policy has involved considerable emphasis on examining assets to be protected, followed by revolving policy around principles and actions required to
protect those assets. However an approach is required where not only the assets are included, but an understanding of and contribution towards developing a culture of compliance within the organisation is required. This necessitates developing policy with an organisational context in mind.

General characteristics of a policy should ensure that it is short and easy to read, with general length of between one and five pages being adequate. If the policy is too long, people will not read it. One participant remarked that a draft policy they produced was initially 30 pages long, which was unacceptable by senior management. As previously mentioned, another participant admitted to a 180 page long security policy. The rationale was that the length of the policy allowed specific recommendations, and that without these there was no record of how things should be done.

The policy should be reviewed on a regular and consistent basis, and updated if necessary in line with major organisational, regulatory or technological changes. The policy needs to be realistic, achievable, must be able to be practically implemented and also needs to be enforceable. The policy must be distributed and communicated throughout the organisation. Distribution and communication can be achieved in a number of ways, which should be matched to the requirements of the organisation. These ways could include emails, Web presence or workshops where the policy is explained.

One of the mechanisms available for improving the security policy process in universities would be to adopt some of the supporting documentation that is currently used in the process of IT system development. This involves documentation surrounding the development of systems, covering critical information such as requirements, objectives, and specifically for policies, political subjectivities necessitating policy. From a systems development process, documentation is quite mature and has no doubt resulted in preventing the failure of many IT projects. Similarly, evaluation of and commensurate documentation of support security policy has
the capacity to support the security policy development and implementation process (Maynard and Ruighaver, 2002).

It is also worth examining models for policy development in relation to advocates of meta-policy development and abstraction and refinement models for policy development such as those put forward by Baskerville and Siponen (2002) and Abrams and Bailey (2001). Meta-policy is effectively a ‘policy on policies’, and provides an important framework for security policy development, as it provides guidance on traditionally difficult areas of development (i.e. structure, content, format and process). The aim of meta-policy includes establishing how information security policies are created, implemented and enforced (Baskerville and Siponen, 2002).

In this sense, meta-policy is a ‘policy about policies’, stating the organisation’s plan for creating and maintaining information security policies. The writing style of the policy should reflect the organisation’s culture, including the use of a template if the organisation uses one. The careful and select use of language including terminology, acronyms etc should be considered carefully, allowing the policy to be clear and comprehensible to the entire audience of the organisation.

The abstraction and refinement model effectively looks at ‘abstracting’ and ‘refining’ policy at a level where it is most effective and relevant to the end user. This approach generally avoids the development of excessively long policies that are never read, and instead extracts components of policies and shapes them to a more dynamic and usable context. An analysis of the essential elements contained in the international standards further gives way to what should be included in a security policy (Hone and Eloff, 2002a).

It should be noted however that developing security policy solely on information security international standards has some shortcomings (Baskerville and Siponen, 2002). Firstly, these standards do not take into account that organisations differ, and therefore security requirements will differ. Secondly, the standards do not take into account the
social nature of the problem. Thirdly, generic standards overlook the normal business requirements of an organisation which can result in a conflict between business and security requirements. Universities should take these shortcomings into account when assessing the validity of international standards and literature recommendations on policy development.
Based on the international standards, the essential elements are summarised in Tables 11, 12 and Figure 36 (Hone and Eloff, 2000a):

Table 11 International Standards’ Recommendations for Security Policy

<table>
<thead>
<tr>
<th>Standard</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS/NZS ISO/IEC 27001—2005. Information technology - Security techniques – Information security management systems – Requirements</td>
<td>This standard and its variants provide a point by point description of what should be included as a minimum in an information security policy. The standard also specifies what should occur within the organisation with the security policy (i.e. it should be approved by management, published and communicated throughout the organisation and a section on review and evaluation of the policy based on a policy owner).</td>
</tr>
<tr>
<td>ISACAF’s COBIT</td>
<td>The Information Systems Audit and Control Association and Foundation (ISACAF) developed COBIT which describes the processes and controls needed for implementing an effective information security policy, rather than focusing on the document itself.</td>
</tr>
<tr>
<td>GASSP (Generally Accepted System Security Principles)</td>
<td>The US National’ Research Council published a report ‘Computers at Risk’, and GASSP have taken general recommendations out of this report. GASSP’s reference to information security policy is minimal and focuses on the rationale for policy. It does cover some processes necessary for defining, maintaining and implementing the policy.</td>
</tr>
<tr>
<td>GMITS (Guidelines for the Management of IT Security)</td>
<td>GMITS describes the policy hierarchy and provides a point list of the topics a security policy should cover.</td>
</tr>
<tr>
<td>ISF’s (Information Security Forum) Standard of Good Practice</td>
<td>Contains a brief point by point section on information security policy, focusing to a large extent on user behaviour and the characteristics of policy.</td>
</tr>
<tr>
<td>BSI IT Baseline Protection Manual</td>
<td>This manual presents a set of recommended standard security controls and provides a comprehensive description on developing a security policy. Topics covered include management responsibilities for policy, convening a team responsible for security policy development, and the content and distribution of the policy. The section on the content of the policy gives guidance on the minimum requirements for inclusion and tips on style and review of policy.</td>
</tr>
</tbody>
</table>
This figure is not available online. Please consult the hardcopy thesis available from the QUT Library.
### Table 12 International Standards’ Essential Elements of Security Policy

<table>
<thead>
<tr>
<th>Essential Element of Security Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Need for and Scope of Information Security</td>
<td>A brief introductory statement outlining the organisation’s dependence on information as an asset, and therefore its dependence on information security. A background as to why the policy is needed in the organisation.</td>
</tr>
<tr>
<td>Objectives of Information Security</td>
<td>Objectives should give the reader the aim of the policy and be clearly linked to the business strategies, goals and objectives.</td>
</tr>
<tr>
<td>Definition of Information Security</td>
<td>A security policy may reach a diverse target and therefore an explanation of what security is and what it represents is important.</td>
</tr>
<tr>
<td>Management Commitment to Information Security</td>
<td>A statement of management commitment is singularly important and represents management intention.</td>
</tr>
<tr>
<td>Approval of the Information Security Policy</td>
<td>Endorsement of the security policy should be at the highest level within the organisation as a further sign of management commitment.</td>
</tr>
<tr>
<td>Purpose or Objective of the Information Security Policy</td>
<td>The purpose of the information security policy is related to the reasons for it and is linked to legal compliance. The main goals of the policy should also be included.</td>
</tr>
<tr>
<td>Information Security Principles</td>
<td>Information security principles relate to the general and specific rules that form the policy. These are aimed at influencing the behaviour of the organisation.</td>
</tr>
<tr>
<td>Roles and Responsibilities</td>
<td>Roles and responsibilities should convey what is expected of individuals and of the organisation in general.</td>
</tr>
<tr>
<td>Information Security Policy Violations and Disciplinary Action</td>
<td>A statement in this section should ensure that disciplinary action can be taken against non-compliance of policy. This statement should be directly related to the organisation’s disciplinary policy.</td>
</tr>
<tr>
<td>Monitoring and Review</td>
<td>This statement deals with the requirement to regularly and consistently review and update the policy to ensure its effectiveness and relevance.</td>
</tr>
<tr>
<td>User Declaration and Acknowledgement</td>
<td>A user declaration and acknowledgment is not found on all policies however it generally forms a signed abridged version of the policy, which often forces a user to read the entire policy.</td>
</tr>
<tr>
<td>Cross References</td>
<td>The security policy should not be written in isolation and should be cross referenced against other relevant policies, standards and procedures.</td>
</tr>
<tr>
<td>General Elements</td>
<td>Authors, policy version and date, review date.</td>
</tr>
</tbody>
</table>
One of the main problems with policies is inappropriate abstraction according to Gaskell (2000). Gaskell (2000) recommends avoiding writing long, wieldy policies and instead based policies on relevant, abstracted sections for specific policies. As an example, a policy could be written specifically to cover required anti-virus measures as opposed to having one long security policy that included all areas of security. This was an issue mentioned in the interviews, where policies were inappropriately written as either high level or very detailed, where the level of abstraction is inappropriate for the audience.

A differentiation between security policy and supporting security procedures is required in these types of circumstances. This links in to layered policy abstraction and refinement as advocated by Abrams and Bailey (2001), where policies are short and specific and layered to the appropriate area in the organisation. Alternatively Abrams and Bailey (2001) differentiate three views regarding policy:

1) Corporate security policy, reflecting top management’s view,
2) Organisational security policy, a users view, and
3) Technical security policy (reflecting a designers or architect’s view).

The security policy is the top level documentation from which all other documentation is derived. The lower levels of documentation should be a further abstraction of the high level documentation. Gaskell (2000) applies a ‘security engineering’ concept to policy, referring to a set of documents that make up what should be labelled security management documents, rather than security policy. Based on a level of abstraction Gaskell (2000) refers to a hierarchy of documentation, including business requirements defined in a security policy document, a set of security design/plans in a security architecture document, and a set of configuration guidelines and operations procedures.

Information security policy formulation is often reported to be an ad hoc process. It is suggested therefore that information security policies should be developed with the
guidance of information security management standards and guidelines (Gaskell, 2000; Baskerville and Siponen, 2002; Hone and Eloff, 2002a).

5.4 Discussion on Security Awareness

This section discusses the current status of security awareness, emerging issues and a discussion on how security awareness could be improved.

Discussion on the Current Status of Security Awareness

The area of security awareness highlighted that awareness raising activities are not well-structured. Awareness is raised predominantly by occurrence of incidents rather than a structured, targeted program of activities. Although many institutions do engage in security awareness activities, these tend to be along the lines of bulletins, emails etc and are neither comprehensive nor targeted in their approach, or cannot in any way be described as active campaigns. The ad hoc approach to raising awareness is reflected by the fact that less than 15% of participants stated they had adopted a formal or structured awareness program.

Despite opinions that raising security awareness was an important priority, less than five percent of participants agreed that existing activities resulted in raising security awareness levels adequately. Nearly 50% of participants 'somewhat agreed', and over one third ‘disagreed’ on the adequacy of activities, indicating that awareness raising activities are far below requirements. Although many participants indicated they intend to do something about increasing awareness activities, its current status is relegated to that of recognition of its importance but lacking in action. When asked what factors had been effective in raising awareness levels, participants indicated that the occurrence of security incidents had been the most effective in increasing awareness, indicating an unstructured approach to raising security awareness.
Key Issues Surrounding Security Awareness

The findings from this survey and security literature in general indicate that security awareness is lacking. Additionally, the overall lack of security awareness is directly linked to the major challenge of improving security controls and responses to incidents. One of the concerns in this research is that although participants readily acknowledge that lack of security awareness is a problem, the responses to increasing awareness are not targeted or even apparently prioritised. While this situation is less than desirable, it is necessary to understand why this situation exists.

Although resourcing was cited as the main barrier to increasing awareness, cultural reasons and a lack of prioritisation also impacted raising awareness activities. The issue appears to be one of a lack of mandate for structured awareness activities. Despite its acknowledged importance, focus and effort on security activities was lacking. A conflict exists between the importance placed on security awareness and the priority actually given to improvements in this area. Therefore it is concluded that the commitment to raising security awareness is generally lacklustre. The types of issues raised included the lack of awareness of the university community, particularly end users, a transient student base, and lack of awareness by Management and Executive. The lack of a skill set for security, the lack of a coordinated approach to raising security awareness, the resources and time required to raise awareness were also mentioned.

In the university environment a commitment to security involves more than just security awareness campaigns, posters, videos, stickers, booklets and the like. Gaining commitment involves a process which fits with the culture of the organisation and ensures that a quality service is provided (Spurling, 1995). According to Spurling (1995), increasing and promoting security awareness is centred on the following:

1) Promoting a poor service is difficult so make sure the service is applicable,

2) It is easier to get commitment if people are involved,

3) You need to keep the issues in front of everyone constantly.
Spurling (1995) cites experience in a work environment in some ways very similar to the university environment. This environment included having a user base where a lot of task oriented people who just wanted to get the job done saw controls and restrictions as unnecessary bureaucracy. Where controls are seen to get in the way, ways will be found to divert from them or pressure brought about to change the controls. If this is the case, then those controls cannot be implemented successfully even if awareness is raised.

Insufficient communication from security sections in universities causes users to construct their own models of reality on possible security threats and the importance of security. This study indicated the model of reality constructed by the user could be wildly inaccurate due to insufficient knowledge. This caused security areas to view users as inherently insecure, and users to view security people as obstructionist in mechanisms deployed, creating a vicious cycle. Therefore, understanding people’s motivation and deconstructing any false sense of realities towards information security is a useful exercise when undertaking awareness activities.

One of the key issues in security awareness in universities is exacerbated by the fact that universities have a transient student base. This means the message needs to be repeated every year to students, and less often to staff. Therefore not having a framework approach to security awareness means a continuous re-inventing of the wheel or worse, simply avoiding the situation. Siponen (2000) argues that all information security awareness programmes should use a ‘framework and content’ approach. The framework aspect would use an appropriate structure and leverage from the use of standards and guidelines.

**Improving Security Awareness**

In proposing a conceptual foundation for organisational information security awareness, Siponen (2000) suggests that the occurrences of human error in information security need to be mitigated by a security awareness programme based on or reflecting a framework similar to the one proposed by NIST (1998). The NIST guideline recommends: identify programme scope, goals and objectives; identify training staff and
identify target audiences, motivate management and employees; administer the programme, maintain the programme; and finally evaluate the programme.

Siponen (2000) maintains that security awareness issues are not well-understood, resulting in ineffective security guidelines or programs in practice. The need for a structured security awareness programme would appear to be reasonably epidemic. Siponen (2000) is critical of existing approaches to information security awareness and education, citing them as being too descriptive (and therefore not accomplishment oriented). What is needed, according to Siponen, is the creation of an information security awareness programme through a systematic approach. The aim of the programme is ultimately an effort to minimise end-user errors and non-compliance.

Siponen (2000) suggests that the possibilities of motivational and behavioural theory have not been explored adequately in relation to information security awareness, but suggests they can be explored more thoroughly in ‘content’ categories of programmes. The aforementioned NIST guideline uses what Siponen (2000) describes as the ‘framework and content’ category. The framework category involves explicit knowledge, is mostly used in awareness programs currently, and involves a structural approach. Conversely, the content category involves tacit knowledge and a more qualitative approach. Shortcomings in this second area, the content area, usually invalidate the second area with issues surrounding things such as people, time and money, and by wasting security techniques. Motivation of end users to comply with frameworks really lies in understanding the content area, according to Siponen (2000).

Additionally, it is worth considering that the approaches used in information security awareness programmes should satisfy the requirements of behavioural theories in order for end users to understand why they should follow security guidelines. For end users to internalise the security guidelines, the content part of the programme needs to be seriously considered. This would increase effectiveness, as many existing programmes are simply descriptive, and users may not follow guidelines without adequately understanding why they should be followed (Siponen, 2000). On this basis, simply
using the framework category is not enough in itself. This is the case because information security awareness based on guidelines (which reflect imperatives), is more associated with the internalisation of needs than with other issues such as straight facts. Too often security guidelines are not justified in a relevant way, therefore end users do not internalise their adoption.

There needs to be a strategic, targeted and continuous program in place to increase awareness in universities, one that is adequately funded and resourced. Users will resist change if they cannot see the benefits, or the process is difficult or time consuming. It is also necessary to balance awareness raising activities with transparent technology processes that minimise requirements for end user awareness. A classic example is using network admission control for end user workstation registration instead of relying on end user diligence and awareness to use anti virus software and maintain operating system updates.

5.5 Discussion on Security Compliance

Current Status of Security Compliance

The section on compliance covered a diverse range of areas related to security which indicate that higher education institutions could benefit from improved governance over information security. The fact that a lack of measurement presides over security indicates that coming to terms with the management of security is not only difficult, but that imperatives for improved management do not exist. The lack of measurement also indicates that security has attributes of intangibility of risk, and its value to the organisation is not always recognised. The reactive mode of security is reflected by way of measurement of incidents due to a lack of established baselines.

A poor ‘culture of compliance’ was cited by participants as the number one barrier to improving overall compliance with security, particularly in a decentralised environment. This was followed by issues with funding and resourcing, and then awareness and understanding. The perceived inability to ensure standards across a decentralised
environment was a concern frequently expressed, together with the lack of capacity to monitor compliance. Span of control over information security management was cited as being impacted by the culture of the organisation, effected by leadership within IT, centralisation of IT and resistance to work practice changes.

The culture of compliance towards security in higher education sectors could be significantly improved on current levels. Currently around only 10% of participants agree that a culture of compliance towards security was reflected in the institution’s work practices and processes. This compares with over 40% who disagreed and around 45% of participants who only ‘somewhat agreed’. The culture of compliance was cited as the major barrier to compliance, followed by funding and resourcing, then by awareness and education.

Most universities (over 80%) allocate 5% or less of the central IT budget to security. Approximately 20% of universities estimated that they spent less than 1% of the central IT budget on security, less than 10% of universities indicated a spend of 5-10% and just over five percent of universities indicated they spent between 10-15% of the central IT budget on security. This low level of security budget corresponds with the fact that funding and resourcing was cited as the second largest barrier or obstacle to achieving improved security compliance.

When asked if the effectiveness of security or the value of security was somehow measured, few universities indicated that this occurred. Several participants indicated that measurement of security was difficult, due to the intangible nature of both risk and risk mitigation, and the difficulty in illustrating the enabling value of information security. The primary methods stated for measurement of security involved Key Performance Indicators (KPIs) against business goals and plans, as well as empirical data on security incidents, viruses and availability. Measurement of the value of security or its effectiveness remains challenging and is a largely unaddressed area for universities.
A significant proportion of participants agreed or somewhat agreed that they were positioned to defend against incidents, mostly cited as viruses and malware. This area was representative of the major security threats of concern to institutions. The most frequent source of security incidents was attributed to viruses and malicious software, despite counter measures in place at the gateway. This was followed by user errors or non-compliance, system administrator errors or non-compliance and finally, cyber or internal based attacks. The capacity to effectively monitor and obtain summarised alert and logging information from systems was also cited as an issue, with many organisations having already deployed, or stating they intend to deploy, intrusion detection systems.

Factors ‘critical to the success of information security management’ focused on senior management support, strategic governance, and awareness and education. When asked what the critical success factors were for effective security management, participants responded largely with a focus on the engagement and support from senior management, ensuring that the correct structure and governance framework was in place, underpinned by policy (structure and framework included both governance structure and technical architecture), followed by ensuring that awareness and education rates were high so as to facilitate a culture of compliance.

Reaction to incidents was cited as being more likely to have an initially higher profile, but to then quickly fade in the background once the ‘reality of risk’ had subsided. This situation is also supported by comments that where there had not been an incident, the reality of risk was not apparent and was largely ignored. A lack of incidents therefore is a cause of complacency. The findings from this indicate a necessity to have in place effective preventive, detective and corrective controls (both processes and technology) to deal with the inevitable, rather than waiting and then reacting in an ad hoc manner to incidents.
Key Issues Surrounding Security Compliance

Key issues raised included network architecture, access control over the network and workstations, improving network architecture, allocation of specific secure areas for corporate systems, improving access control in the areas of network, account management, Web applications and incorporating security into systems development, authentication, identity theft, maintaining control over the end user workstation environment, patching, viruses and malicious software, intrusion detection and protection systems.

Participants were asked what they considered to be the critical or essential factors to enable effective security management. A broad categorisation of responses resulted in three major areas: senior management support, governance framework and structure, and awareness and education. The first area, senior management support, cannot be over estimated as it significantly affects the other two areas, supporting a governance framework together with backing and supporting an overall awareness and understanding throughout the university community.

These results also corresponded with a major theme emerging from this survey, being a requirement for an increased focus and sustained efforts by participants in improving the overall approach, structure and governance of security. Although awareness and education ranked highly and consistently, and despite the fact that it was ranked as an area requiring improvement, awareness and education remains a difficult, time consuming and resource intensive task. This would be made easier through more automated processes, awareness tools and resources, and by having more support from the top.

Concern was expressed by several universities, in particular those that had incurred a serious breach on one or more corporate systems in the past, and suggested that the number of attacks on university corporate systems is likely to rise. Participants suggested the rise in attacks on American universities reflected cause for concern for Australian universities as well. Those universities that do not have corporate systems
protected by internal firewalls also expressed a priority to move to minimise risk in this area.

The core issue surrounding compliance with security centred on the fact that drivers for regulatory compliance are still emerging for Australian universities. At the same time, universities lack the ability to understand how well their systems are actually protected in relation to requirements. It is likely however that regulatory compliance and corporate policy management drivers will grow and therefore be key determinants in how security management models look in the future. Another issue for compliance is associated with the fact that the tangibility of measuring the effectiveness of security spending is very difficult. Therefore loose compliance drivers linked with the difficulty in understanding the effectiveness of approaches has resulted in compliance being fragmented across the organisation.

Although technology is a key factor in protecting systems, the people and processes that are integral to ensuring that technology is appropriately placed were indicated as needing to be coordinated under a successful management framework. This is particularly the case considering that as demand for open systems expands, more threats emerge, more point based technology solutions appear, and consequently a patchwork of technology based systems develops. There is a need to bring together information from existing disparate technologies. An integrated security management system that provides meaningful reporting on security would assist.

It is becoming increasingly necessary to effectively manage emerging threats and at the same time increasingly difficult to maintain a comprehensive overview of the technology responses by industry to those threats. So far, the main guiding framework that offers a security management model, 17799, does not necessarily overlay well with the actual operational functions of security, and comments from participants indicate that its adaptation is difficult. Moving forward it will be increasingly vital that universities are able to understand, measure and demonstrate the effectiveness of
security approaches, in order to ensure that necessary standards can be met to achieve emerging regulatory compliance.

Increasingly, IT functions need to expand, and compliance and safeguarding of information needs to be focused on. The most effective way to justify the security function is to assess the value and impact brought by security to the organisation. Understanding how to evaluate security in terms of how it can enable the organisation and finding a common language between IT and senior management is critical to aligning security with the business needs. The measure of security value overall is elusive as the benefits are only visible through events that do not happen. Most Australian universities are not currently measuring the performance of security, or tend to focus on the costs and returns as opposed to the enabling nature and value of security. This continues to context security as a liability.

When asked about concerns with specific security issues, participants indicated that the increased frequency and sophistication of viruses, worms, spyware and other malicious software, caused most concern. In particular, the advancements in social engineering and keystroke loggers, and the resultant capacity for system compromise were raised. This concern is extremely valid. Symantec Corporation release their ‘Internet Security Threat Report’ each year. The current report identifies an increase from the previous report in Windows-based virus and worm variants.

The report also identifies emerging trends and indicated that an exponential increase is likely to be seen in the use of botnets (abbreviation for robot and refers to software operating under ‘robotic’ control on the Internet). Also distributed worms and malicious scripts for illegal and financial gain, client side attacks, increased attacks through audio and visual files, increased risks with spyware and adware, and in general an increase in the frequency and sophistication of attacks is likely. This includes modular code that is downloaded in stealth using previously uncommon channels such as Peer to Peer networking (P2P) and Instant Messaging (IM).
Access control was also rated highly, both in terms of account management and use, but also the lack of access control management for workstations, network access control in relation to corporate systems and databases, and authentication. Access control also encompassed a lack of regular firewall auditing. Several participants indicated their concern at the system compromises now widely publicised in American universities, and the potential for this type of attack to be more commonplace in Australian universities. Additionally, poor security applied in systems development, particularly in Web applications, was noted.

**Improving Security Compliance**

Despite security being a recognised issue, many organisations lack a full understanding of what they should be doing and how to go about implementing security. A lack of availability and comprehensiveness of security guidelines and standards is not the issue as these are already available to a large extent.

A critical characteristic of security is that many aspects of security are transparent until a breach occurs (Furnell et al., 2000). Therefore appropriate recognition of security must be brought to the attention of the organisation and acted upon. Security must be viewed as a multi-faceted problem which requires a comprehensive solution to encompass physical, procedural and logical forms of protection. As a result a range of expertise is required to progress appropriate solutions (Furnell et al., 2000). This expertise often resides in the person responsible for the progression of information security. What is needed is a succinct understanding of how to conceptually view a path forward to progressing security implementation.

Improved governance, being adequately funded and resourced, and increased awareness and training rated as the top three areas necessary to make major improvements in compliance with security. Within a structured approach, having the right framework not only applied to management of processes, but also technology controls including standards for systems development, operating standards, best practices and the ‘nuts and bolts’ of tightening security controls. From a technical perspective participants indicated
that their main future focus should include improving network security architectures, particularly in relation to use of virtual firewalling technology, especially for internal corporate systems. Also rated highly was embedding security more effectively in systems development, VPN and encryption methods for wireless, and attempting to gain improved control over the account management process and desktop environment. Participants noted that in the absence of adequate user awareness, increased reliance on technology based controls could often be helpful in ensuring that a transparent process for safeguarding systems was in place. This could help to mitigate the lack of end user awareness.

Other specific directions and goals stated included:

- Improved network architecture (access control, flexibility and robustness),
- Protection of corporate systems behind internal firewalls, and improved regular firewall auditing,
- Better control of the desktop environment, particularly in relation to viruses and malicious threats, remote management and personal firewalls,
- Integration of security into systems development (particularly for Web applications),
- Patch management for workstations and servers,
- Account management (currency of accounts),
- Intrusion Detection/Prevention Systems,
- More secure authentication/identity management,
- Opening up systems in a secure manner (e.g. portals),
- Wireless security.

Measurement of security and aiming for a certain level of compliance was also seen as desirable. Cannon (2006) proposes that ensuring compliance in relation to the federal, state and local regulatory requirements needs to be made succinct. Cannon suggests that
ensuring compliance necessarily revolves around one fundamental concept ‘Are policies being followed the way I expect them to be?’ The approach suggested by Cannon involves a six-step process to ensure that compliance is fundamentally driven by a policy-procedure perspective. The six step process involves:

1) Determine where to focus your compliance efforts – this is primarily driven by understanding the various drivers that affect the bottom line of the organisation in terms of cost and service delivery;

2) Use procedures that validate compliance – procedures for policy need to be scrutinised to ensure that policy is upheld. This can often involve technology based controls providing a reporting mechanism to test this;

3) Consolidate the management of compliance – involves ensuring planning takes place to update new compliance requirements into implemented controls through a centralised, coordinated and structured effort;

4) Create compliance policies using a hierarchical approach – particularly in larger organisations, having high level policies that determine security posture is important so that the various sections within organisations can create complementary and supporting specific policies;

5) Decide to automate compliance policies – systems that provide end-to-end control over business processes are required;

6) Choose compliance enabling technologies – technologies should be selected that are able to aid organisations in automating their compliance needs.

In other research, Kankanhalli et al., (2003) cites a correlation between both active and visible deterrents and preventative measures with the associated likelihood of fewer cases of information security abuse. The researcher proposed that certainty and severity of sanctions are likely to be effective as deterrent measures and that conversely, the absence of deterrents may lead to a misinterpretation of the correct use of IT resources. They cite examples of deterrent efforts as policy statements and clear guidelines on the legitimate use of IT resources. Preventative measures are described as controls that are
in place for when deterrent measures are overridden. Examples include software or physical controls.

An interesting result of their study was that the severity of sanctions contained within deterrents did not seem to increase compliance. A focus therefore on deterrent and preventive efforts rather than severity levels is likely to lead to improve results. These two types of efforts are best combined in an overall strategy for security, which covers all required aspects and includes top management support. Promoting a culture of compliance and achieving even small changes in attitude and behaviour may take years, according to Gaunt (1998), highlighting the necessity for these efforts to be channelled through a security strategy. Cultural compliance therefore needs to be examined from the perspective of having an appropriate security strategy in place.

Obtaining compliance with information security faces a number of challenges that Nosworthy (2000) describes as ‘balancing factors’ between risk and control. In many cases universities have the belief that because it hasn’t happened to them it never will. This type of mindset, unless proven otherwise, makes committing to information security seem an unnecessary expense as was evidenced in the university interviews. Often, information security was associated with IT itself and not back to the business information flows and budgetary allocation process. Therefore a reluctance to release resources occurred, which in turn restricted the level of awareness provided, further exacerbating the situation. Information security is not always funded directly, or if funded inadequately, reflects a lack of prioritisation.

Obtaining a culture of compliance requires a change at the individual, group and organisational level (Vroom and Von Solms, 2004). Vroom and Von Solms (2004) contend that to change the culture in the organisation towards compliance in security, the individual, group and organisational levels requiring change must be identified and understood from a cultural context. These layers and the interaction with the cultural levels are demonstrated in Edgar Schein’s model, presented in Figure 37.
Figure 37 Edgar Schein’s Model of Layered Organisational Culture and Behaviour
In this model, artifacts are the tangible things that any outsider to the organisation would see, espoused values are partially visible and reflect the norms and values of groups, and the basic assumptions are the fundamental underlying beliefs, attitudes and values of individuals. Vroom and Von Solms (2004) contend that changing an organisation towards a ‘culture of compliance’ involves understanding the interrelationship between the layers of culture and the levels of organisational behaviour. The model allows a more in-depth understanding of compliance with security than purely examining deterrents and preventive measures alone. The relevance of such a model is that it highlights that the development of a culture of compliance is required to permeate the organisation at many levels. It also demonstrates that the culture can be observed and assessed from a variety of perspectives.

An argument in support of having a security strategy aimed at developing a culture of compliance at all levels in the organisation is offered by Wright (2003), who suggests that management focus on security tends to be reactive to the perceived level of threats. When a crisis arises, so does lower level management’s attention and the prioritisation on information security. Wright (2003) suggests that this rather limited culture towards information security contributes to poor motivation, resulting in languid compliance activities and reflects a strong need to have information security represented by top level management.

While it is acknowledged that top management support for information security is important, top management concern may be quite low for information security and result in a general lack of commitment throughout the organisation. Kankanhali et al., (2003) offers plausible explanations for low concern by top management, citing three main reasons. There may exist a perception of the information security risks being low, there may be scepticism towards the benefit of controls due to the difficulties in measuring their effectiveness. There may also be a lack of upwards communication about the controls that are available. These factors were all evidenced in the interviews and highlighted the requirement to have security represented as a corporate governance issue.
The problem is often obtaining that support, and the question is asked ‘how can top management be convinced that they in fact have a responsibility towards information security?’ Recent research by May (2003) on adoption rates of BS7799 in the UK indicated that the major stumbling block was that security is still considered the preserve of technical experts by senior management and so has not penetrated the board room. May (2003) suggests that actually changing the corporate culture, which is often at the heart of the matter, and without boardroom acceptance and support, there is likely to be little real progress towards developing a culture of compliance across the entire organisation.

One approach is to link information security more directly with the wider responsibility of good corporate governance (Von Solms, 2001). The concept of information security governance, which currently is not a commonly found term in the board room, should be included as a subset of corporate or enterprise level governance documents. Moulton and Coles (2003) provide a definition of security governance as ‘the establishment and maintenance of the control environment to manage the risks relating to the confidentiality, integrity and availability of information and its supporting processes and systems’. It follows that if security forms a subset of corporate governance then internal controls to comply with legal and regulatory requirements must follow, ensuring that top management in organisations commit to security, with a likely flow on effect throughout the organisation.

In developing a culture of compliance, standards are also likely to provide an important function by fostering a sense of identity, as activities are directed towards achievement of the standard, according to May (2003). The pragmatism that standards embody must however be relevant and be applied appropriately across the organisation from top management down. While top management support for information security is seen as essential, so is cross organisational understanding of security risks and gaps.

Gaining compliance may also be a matter of having external pressure applied to organisations, such as regulatory and legislative requirements specified by government.
For example, in the UK, the Department of Trade and Industry is threatening to make BS7799 a legal requirement, and in the United States several requirements including Putnam and Sarbanes Oxley already exist, positively impacting steps taken in organisations towards information security. It may take this type of externally imposed regulation to ensure that top management complies with, and sets a precedent of, a security culture of compliance.
5.6 CAUDIT

Participants considered that CAUDIT could play a significant role in facilitating the improvement of information security within the university sector. CAUDIT was acknowledged as having potential to contribute to the process of information security management through the areas of developing consistent, Australian-wide university applicable standards, best practices, governance frameworks and policy, and facilitate information sharing, awareness raising and maintain incident statistics. CAUDIT could:

- Assist with the development of template based security policies,
- Assist universities to identify and adopt ‘best practice’, ‘good practice’ and recommended frameworks for operation,
- Provide legal advice or counsel to universities on information security pertaining to compliance requirements and privacy issues,
- Facilitate training days, workshop days and information session/sharing days,
- Establish and maintain a confidential security incident register for universities, to both heighten awareness and to demonstrate the ‘reality of risk’ to universities,
- Provide an auditing service to universities,
- Increase coordination with AusCERT,
- Centralise security product information that universities are currently using,
- Assist with security planning and liaise and influence the AVCC,
- Assist with benchmarking security in the university sector,
- Assist with security awareness resources, such as poster printing, security awareness CDs or Website content, security awareness days or months,
- Assist with security measurement, ROI models and identify value enabling,
- Negotiate licensing with vendors, particularly discounted rates for anti-virus,
- Assist in networking between universities and facilitate meetings.
5.7 Security Practitioner’s Management Model

A detailed analysis of the data collected through the survey resulted in the generation of emerging themes, patterns and theories consistent with the analysis methodology. The proposed security practitioner’s model (Figure 38) represents a synthesis of these emergent themes, patterns and theories. Essentially the model seeks to provide a way to think about the fundamental challenges faced by the security practitioner in progressing security implementation within Australian universities. The major challenges can be thought of as requiring a way of understanding not so much what to implement, but how to think about implementation in order to progress it within the institution.
Figure 38 Security Practitioner’s Management Model.
A Systemic Approach

This model is designed specifically for university information security practitioners in Australian universities, whose role encompasses a responsibility for security implementation at the operational level. The structure of the model takes into account the fact that in many circumstances, universities struggle with a wide range of security best practices, frameworks and standards. What is often missing is a systemic approach to appropriately implementing one or more standards. Key to the model is the challenge that cultural issues in universities often result in resistance to security, unless an effective method is considered and applied consistently with the organisation’s culture. It is recognised that, although the specific application of this model in this thesis is to Australian universities, the model is applicable to a much broader range of applications. The model is therefore generally applicable to most medium to large organisations.

Aims of the Model

The proposed model aims to facilitate security management in the Australian university sector, by linking theories and findings from the study to an improved process for security management at the operational level. The model provides a reference for security practitioners to understand how best to transition the process of security knowledge into implementation.

What is needed is a systemic approach to the management of security in Australian universities, one which integrates and shows the relationships between layered organisational contexts, behavioural aspects and the use of a practical management model. A framework that satisfies two primary goals is needed. The first goal would allow university security practitioners to apply the management of information security in a more structured and cohesive manner. The second goal would be to increase the transparency and effectiveness of the security process towards organisational requirements.
The model is designed to assist security practitioners to progress their institution’s information security management programme. All too often, university security practitioners have an in-depth understanding or instinctive knowledge and feel for what should occur, but meet resistance or barriers to change, or simply encounter a lack of understanding of the need for change. The approach proposed in the model is therefore fundamentally different to simply implementing a set of controls based on a pre-defined standard. The model attempts to describe an end goal of implementation, the ‘how’ to implement rather than ‘what’ to implement.

Despite the importance of information security to Australian universities, existing approaches, standards and guidelines for security do not necessarily integrate well into individual university environments. Therefore existing approaches do not provide a single point of understanding for how the process of information security should be managed. In determining how to achieve this, the model is based on an analysis of the factors and issues that facilitate or impede the management of information security in Australian universities.

From an information security perspective the environment in higher education institutions needs to take into account many contributing factors. Structural issues such as the size of the organisation and the level of decentralization of Information Technology services and associated standards, policies and procedures affect the final security outcome. Business organisational issues such as the real cost of impeding ‘academic freedom’ through stringent security rules and requirements are always a concern. The fact that higher education sectors are a gateway to the Internet used by various stakeholders with conflicting interests affects the very basis of the organisation’s approach to information security.

From the security practitioner’s perspective, an approach needs to provide a meaningful structure for progressing information security in an environment where competing priorities exist. An approach, underpinned by communication and awareness, should be focused on developing the organisation’s culture of compliance. In this way, continuous
security improvements applied through a framework that regulates an aspired culture of compliance can be achieved.

**The Use of Standards in the Model**

An important attribute of this model is the acknowledgement that best practices are recognised as playing an extremely important role in the management of security. In fact, a range of best practices is applicable to information security management within this model. This includes the growing maturity and consequent acceptance of well-regarded frameworks such as AS/NZS ISO 17799, CobiT, ITIL, COSO, ISO9002, Capability Maturity Model (CMM®), Systems and Security Business Architecture (SABSA), Project in Controlled Environments (PRINCE), Managing Successful Programmes (MSP), Management of Risk (M_o_R®), and Project Management Body of Knowledge (PMBOK®) (IT governance Institute, 2005).

The model leverages off the original work in the SABSA (Systems and Security Business Architecture) method (Sherwood et al., 2003) to provide a reference for facilitating the management process of security. Key to the model is the transitioning of knowledge into implementation, towards a culture of compliance. The model is premised on fundamental assumptions well-evidenced in the literature. First, that information security management is most effective when a structured process is aligned across the organisation, from the senior executive down to the daily operational practices of end users. Second, that the use of controls and standards alone are not enough; developing a culture of security is an end goal requiring communication and awareness across all layers of the organisation. Third, that the resultant compliance with security must be continuously monitored and adjusted, through the adoption of a review mechanism such as the ISO 27001 ‘Plan, Do, Check, Act (PDCA)’ model, or another similar audit-based monitoring and corrective action process.

Although a selection of various elements of disparate best practices can be aligned to suit the organisation, invariably the use of best practices needs to be applied in context to organisational needs. The implementation of best practices tends to be costly and
unfocused if treated as a purely technical guide. Implementation of best practices should be consistent with the organisation’s business risk management and control framework (IT governance Institute, 2005). Therefore the most effective approach is to apply best practices starting at the business context.

An important distinction in this model which separates it from other models is the recognition that the application of technical controls is of little use without compliance with policy. Therefore not only is increased awareness required, but a culture of security must be developed to support the security programme. This requires relevant policy with associated work procedures, facilitated by a long term programme in which changes can be introduced in a manner that accounts for both work practices and security requirements (Gaunt, 2000).

**Process Flow Through The Model**

The model begins by feeding knowledge (gained from information security understanding, broader organisational knowledge, information technology expertise, management ability, best practice frameworks, and previous experiences of the individual practitioner) into the institution’s security programme. This knowledge must be channelled into an appropriately designed interface to the organisation in order for security practices to be gradually incorporated into daily processes and procedures. This is necessary as part of developing the culture of the organisation. Inappropriate application of security procedures can result in an expensive or unacceptable overhead (May, 2003). The interface ideally should be a structured and well-accepted information security management programme.

The information security management programme links into a five-level abstracted layered structure which begins at the business strategic level, represented as the contextual level, and is traceable through the organisation finishing at the operational layer. Across the layered structure, the process of communication and awareness facilitates the end by-product, a culture of compliance. The central goal of the model is the required organisational level of a culture of compliance with the depicted external
and internal influences viewed as inter- and intra-organisational factors impacting culture. The resulting compliance levels are then relayed into the knowledge that feeds back into the framework. A continuous loop is thus established that represents the transition of knowledge towards a culture of compliance.

**Channelling Security Practitioner Knowledge**

The findings from this report and other research on information security management support the concept of the security practitioner’s role being one of a knowledge gatherer, with the challenge of implementing knowledge. While the above mentioned frameworks provide guidance on how information security should be implemented, it can be helpful to view information security from the practitioner’s perspective as a challenge of implementing knowledge.

![Figure 39 The Belis and Kiountouzis Structural Model of Security Knowledge](image)

Information security researchers (Belsis and Kiountouzis) from the University of the Agean and the University of Athens propose a structural model (Figure 39) demonstrating how knowledge needs to be applied against policy, guidelines and
The relevance of this model is that in practicality the business units in universities are not necessarily concerned with how systems security is managed (primarily due to a lack of knowledge and understanding), although this scenario is increasingly changing due to growing regulatory requirements.

Contradictory requirements exist when open systems are required on the one hand, and assurance of high protection standards on the other. Appropriate treatment of disparate yet related security issues is not trivial, and requires a wide spectrum of knowledge from technology, organisation and legislation (Trcek, 2003). In many ways, the security practitioner is the glue between the technical components of IT systems, the security of systems and ensuring that the business itself is compliant to security. In reality however the security practitioner can often see what needs to be done, but is challenged by implementation issues including the practicalities of internal skills and resourcing, as well as risk and cost balancing. The key to effectively progressing security management therefore resides in the capacity to skilfully apply security knowledge into implementation.

**Interfacing Through an Information Security Management Programme**

Security practitioners need to transition their information security knowledge into an implementation of security solutions, and should therefore pursue a management model that coordinates an operational, tactical and strategic approach to security. The proposed security practitioner’s model adapts and leverages existing enterprise architecture models for security. The result is an enterprise framework that progresses security knowledge into a culture of compliance.

**Leveraging Zachman, Sherwood and Stephenson Frameworks**

The abstracted layers of the model are well-grounded and leverage off previous enterprise framework concepts originally conceived by Zachman (1987), which were later extended and applied specifically to security architecture by Sherwood et al., (2003). Zachman initially developed the Zachman framework, a six layer abstraction matrix which was later modified by Sherwood into the SABSA methodology (SABSA
being the ‘Systems and Business Security Architecture’). This was then later referenced as the ‘Sherwood Applied Business Security Architecture’. Stephenson (2005) later researched the model and considers the model in a wider context as a ‘Security Architecture Reference Model’ (SARM) and notes its adaptability to security as well as other more generic areas. The primary point of evolution of the model has been away from the SABSA model according to Stephenson (2005), such that the model can be applied effectively to other generic information systems applications.

Sherwood et al., (2003) maintain that very often security solutions for business requirements are responded to through the implementation of ‘point based’ technical controls on a very tactical basis. This finding is also supported by The Butler Group’s findings (Kellet et al., 2005) who concur with the view that security must be driven by the business instead of the often adopted approach of deploying and utilising a range of point based solutions. Often a requirement is identified in terms of a new threat, and a solution sourced without necessarily having regard to the broader implications.

This approach can be inefficient and lack comprehensiveness, thereby leaving systems less protected than a more organised approach. Although this method can provide some security, there can be no certainty that the level of security control is commensurate with the benefit or that it meets other business requirements that are not necessarily security related (Sherwood et al., 2003). This also often results in security being a last minute ‘add-on’ to new business information system design and implementation, when all other design considerations have been decided upon.

The problem associated with this approach is that the point based implementation of security tends to isolate the solutions and render them incapable of integration with other systems or business requirements in general. This leads to a variety of disparate solutions resulting in increased complexity and support issues, additional workloads and increased overheads in administration and management (Sherwood et al., 2003). This can have a significant impact on resourcing.
Establishing Boundaries of Control for Security Domains

The research undertaken in this project found that ‘resourcing’ was consistently cited a major obstacle to improved security management. In many institutions improved levels of resourcing may not be easily achievable, and therefore processes themselves need to be examined. Detert et al., (2000) advocate reviewing processes through identification of cultural configuration and patterns, and within their eight-dimensional framework reference ‘orientation and focus’ as being related to examining and improving processes. The implication is that where resources are not easily increased, processes must be examined for improvement. Those processes should be considered in terms of business requirements as opposed to simple tactical solutions, and the layered abstraction model facilitates this way of thinking.

Often security is approached through a checklist method, by referring to and applying a checklist of technical and procedural controls (Sherwood et al., 2003). The problem with the checklist method is that, while all the components may be checked off, the way they fit together also has to be considered. It is this engineering approach that needs to reflect reality, be accountable and ultimately help develop a culture of compliance. Further complications, according to Sherwood et al., (2003), can arise when the security ‘solution’ can in fact hinder the business operations if it does not support the business’s requirements effectively. This can lead to a worsening of the reputation of security amongst the university community, where security is seen as detrimental to processes rather than facilitating processes. In these circumstances steps are often taken to avoid security by working around it instead of adopting security measures.

Aligning security with the business is therefore fundamental to ensuring the protection of the business from threats in a cost effective way. The traditional, tactical approach needs to be disregarded and instead replaced by a much more strategic, layered approach. This type of approach links the activities of security directly with business needs. The security requirements for an information system imply specific needs and should be traceable to specific needs identified in underlying business drivers.
It is becoming increasingly necessary in a number of environments to trace requirements to a set of standards. Traditionally, approaches to determining security according to a set of standards results in a focus at the component level. For simple systems, this has been acceptable because the boundaries of the systems are clearly definable. Complex systems, comprised of computers, operating systems, networks, communications protocols and applications, are very often approached as a disparate collection of pieces, unless a discrete boundary of control can be applied to the entire system. Without a boundary of control, there is a tendency to evaluate components on an individual level and assume the whole.

This is a difficult approach as there is no unified view of disparate components and therefore security requirements tend to be isolated. Additionally, difficulty in identification of security requirements back to business drivers means that weaknesses in the system can be overlooked, potentially compromising overall security. In order to engineer security requirements for an integrated system, it is necessary to view a complex network as a single entity or at least as a collection of definable domains in the following way:

- Clearly and unambiguously define the business drivers for the system,
- Clearly and unambiguously define the evaluation requirements for the system,
- Clearly and unambiguously define the boundaries for the system.

Focusing on security as a unified whole identifiable by abstracted security domains provides for a key differentiator to traditional approaches to security that consider security from a purely technical or component standpoint. The security model is the core of the approach. Inherent in the model is the fact that security requires an abstraction of basic business requirements into a specific and well-defined approach. By incorporating recognised security standards into the model, an opportunity exists to refine generalised business and security requirements into a set of very specific security function requirements. In other words, by applying the more general requirements from
the use of a security reference model to a set of specific security standards, it is possible to derive a standards-based set of explicit security requirements. The advantages of using this type of approach are supported by Stephenson (2005) who advocates:

- An explicit set of security requirements stated in terms of necessary controls placed at each layer of abstraction,
- Direct traceability to the business, technical and architectural requirements,
- Compliance with governing standards, allowing objective testing and auditing.

The process of applying the model is intended to build a specific set of security requirements that can be applied to a reference model. The end result is a set of standards-based security requirements that are traceable to business requirements. The approach of applying this follows to an extent the approach adopted by Stephenson (2005). This approach includes:

1) **Identify and Document Business Requirements** – this process involves collation of previously stated requirements for systems, interviews, network maps and system documentation, major business initiatives, auditory requirements, extant policy, referenced against each abstraction layer of the model;

2) **Translate the Requirements to a Relevant Standard** – based on the applicable security standard, business requirements can be met by classifying it as a security policy statement, security threat or security assumption in relation to the standard;

3) **Develop a Security Objective** – for each of the applicable standards, an objective should be matched so that a rationale and purpose exists;

4) **Refine Objectives to Controls** – each objective should be defined explicitly to an actual control, process or procedure, identifiable in the applicable abstraction layer. These controls may then break down into further component levels if required.
Abstracted Layers of the Model

Table 13 provides a description of the five layers of the ‘Security Practitioner’s Management Model’.

Table 13 Layers within the Security Practitioner’s Management Model.

<table>
<thead>
<tr>
<th>Layer</th>
<th>Description</th>
<th>Application</th>
</tr>
</thead>
</table>
| Contextual  | The contextual layer is the business context of the organisation, incorporating the core business and organisational environment. It is a description of the business context in which security needs to be managed. Security is driving the business as opposed to the business driving security. Failure to understand and incorporate the business requirements for security can be a common occurrence. At the contextual layer security policy making, information classification, risk analysis process, business requirements collection and specification, organisational and cultural development are considered to be deployed in the lower conceptual level. | This layer essentially ensures that information security management is an enabler of the business by supporting the business and ensuring that security is aligned with the context and culture of the organisation.  
  
  *What?* are you trying to do at this layer? The assets to be protected.  
  
  *Why?* are you doing it? The motivation for wanting to apply security at this layer.  
  
  *How?* are you trying to do it? The functions need to achieve security at this layer.  
  
  *Who?* is involved? The people and organisational aspects of security at this layer.  
  
  *Where?* are you doing it? The locations where you apply security at this layer.  
  
  *When?* are you doing it? The time related aspects of security relevant to this layer. |
<table>
<thead>
<tr>
<th>Conceptual</th>
<th>The concepts and values of information security management are applied in this layer, providing the framework for security in lower layers.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>What? The business and its assets to be protected, as well as the business needs for information security. Security should be treated as an enabler, use of security for secure electronic business, operational continuity and stability, as well as compliance with relevant laws and regulations.</td>
</tr>
<tr>
<td></td>
<td>Why? The business risks in terms of assets, goals and success factors. The threats, impacts and vulnerabilities that place these at risk, as well as the drivers for business security. These may include factors such as reputation, fraud prevention, loss prevention, legal obligations and business continuity.</td>
</tr>
<tr>
<td></td>
<td>How? The different business processes that require security, such as the business interactions and transactions, and the business communications.</td>
</tr>
<tr>
<td></td>
<td>Who? The organisational aspects of security, such as management structures, departments and cost centres, strategic partnerships, contractors and suppliers.</td>
</tr>
<tr>
<td></td>
<td>Where? The business geography and location related aspects of security, such as distribution of campuses and remote access.</td>
</tr>
<tr>
<td></td>
<td>When? The business time dependencies and other time related aspects of business security in terms of performance, sequence and timeliness.</td>
</tr>
<tr>
<td>Logical</td>
<td>The logical layer symbolizes the virtual constructs of security, including logical security domains. This involves the identification and specification of the logical architectural elements of an overall system. This view models the business as a system with system components that are sub-systems themselves. It is essentially logical security architecture. Management of security services, security of service management, negotiation of inter-operable standards for security services, audit trail monitoring and invocation of actions.</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>This is the logical application of security achieved through security design and architecture. What? Business information is a logical representation of the real business. It is this business information that needs to be secured. Why? Specifying in more detail lower level security policy requirements (registration authority policy, certification authority policy, physical domain policy, logical domain policies for securing business information). How? Specifying the logical security constructs and services (entity authentication, confidentiality protection, integrity protection, non-repudiation, system assurance) and how they fit together as common re-usable building blocks into a complex security system that meets the overall business requirements. Who? Specifying the entities (security administrators, auditors etc) and their inter-relationships, attributes, authorised roles, and privilege profiles in the form of a schema. Where? Specifying the security domains and inter-domain relationships (logical security domains, physical security domains and security associations). When? Specifying the security processing cycle (registration, certification, login, session management,)</td>
</tr>
<tr>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td></td>
</tr>
<tr>
<td>The physical layer denotes the actual physical security including infrastructure, devices, hardware and software.</td>
<td></td>
</tr>
<tr>
<td>Products, technology, standards, and tools evaluation and selection, project management implementation.</td>
<td></td>
</tr>
<tr>
<td>Cryptographic key management, communication of security parameters between parties, synchronisation between parties, access control list maintenance and distribution of access control entries, back up management (storing labelling indexing) virus pattern search maintenance, event log file management and archiving.</td>
<td></td>
</tr>
</tbody>
</table>

This is the application of security policy, architecture and design through physical means.

*What?* Specifying the infrastructure, data models and architecture.

*Why?* Specifying rules and controls that drive logical decision making within the system (conditions, practices, procedures and actions).

*How?* Specifying security mechanisms (encryption, access control, digital signatures, virus scanning) and the physical domains these will operate on.

*Who?* Specifying the people dependency in the form of users, the applications they use, and the security user interfaces.

*Where?* Specifying security technology infrastructure (physical layout of the hardware, software and communication lines).

*When?* Specifying the time dependency in the form of execution control structures (sequences, events, lifetime and time intervals).
<table>
<thead>
<tr>
<th>Operational</th>
<th>The operational layer involves people and support mechanisms. Therefore the operational work aspects, procedures, roles, staffing, business continuity and systems maintenance are relevant in this layer.</th>
<th>This is the human and procedural element in support of security functionality.</th>
</tr>
</thead>
<tbody>
<tr>
<td>What?</td>
<td>Assuring the operational continuity of the business systems and information processing and maintaining the security of operational business data and information.</td>
<td></td>
</tr>
<tr>
<td>Why?</td>
<td>To manage operational risks.</td>
<td></td>
</tr>
<tr>
<td>How?</td>
<td>Performing specialised security related operations (user security administration, system security administration, data backups, security monitoring, emergency response procedures, server administration, helpdesk, training, systems development, firewall administration, malicious code management).</td>
<td></td>
</tr>
<tr>
<td>Who?</td>
<td>Providing operational support for the security related needs of all users and their applications (system users, custodians, administrators, owners, developers, IT staff).</td>
<td></td>
</tr>
<tr>
<td>Where?</td>
<td>Maintaining the system integrity and security of all operational platforms and networks by applying operational security standards and auditing the configuration against these standards. Processes and procedures, support.</td>
<td></td>
</tr>
<tr>
<td>When?</td>
<td>Scheduling and executing security related operations.</td>
<td></td>
</tr>
</tbody>
</table>
Communication and Awareness

The use of communication and awareness in the model is so obviously apparent that reference to it is best placed in relation to its role in influencing behaviour. The role of communication and awareness in the model needs to be directed towards a goal of normalising behaviour, in other words developing a culture of compliance. Existing theory agrees that performance is generally related to the interaction of ability, motivation and working conditions (Siponen, 2000).

The two main ways of influencing changes in human belief in order to influence behaviour are thought to occur through both active participation and persuasive communication (Siponen, 2000). Motivation of people towards information security is important and Siponen (2000) describes motivation as dynamic in nature and only lasting from minutes to weeks. This correlates with shorter activity levels, whereas attitudes are of a more static internalised nature, and relate mainly to the quality of actions.

Siponen (2000) references a behavioural science framework for improving information security awareness. The framework is based on existing theory, including theory related to intrinsic motivation, planned behaviour and the Technology Acceptance Model (TAM). Siponen (2000) maintains that certain persuasion strategies based on motivational factors are likely to assist listeners to internalise security guidelines. These strategies should be used in addition to the use of a reward and sanction system, and take into account the aforementioned theories in the behavioural science framework. Siponen (2000) rationalises that a ‘set of persuasive approaches based on morals and ethics, well-being, a feeling of security, rationality, logic and emotions’ should be used where appropriate.
External and Internal Influences

The model takes into account factors that are internal and external to the organisation which are likely to impact on the culture of the organisation and therefore influence behaviour. Although most of these factors will be outside the security practitioner’s control, it is helpful to be able to conceptualise and categorise the types of influences.

Previous work undertaken by Detert et al., (2000) on culture involved a comprehensive review of extant literature in an attempt to synthesise dimensions of organisational culture that have been studied by researchers to date. Detert et al., (2000) advocate the benefits in identification of the cultural configuration and internal patterning within culture relative to the dimensional framework they propose. They suggest than in many frameworks, and in particular those frameworks associated with linking culture and improvement in the organisation, it is necessary to take into account the relationship between an organisation and its internal and external environment as a key aspect of culture.

This relationship includes assumptions about the fundamental orientation of the organisation in terms of control of internal and external factors. Viewing these factors in terms of control means that being aware of them, taking them into account and factoring them into the security management process is an important process towards quality improvements. Detert et al., (2000), note that where organisations concentrate on improvements related to internal factors, the focus will be on improving people and process. Organisations concentrating on improvements related to external factors will look for external sources for new information and look to judge success by external benchmarks. The authors proposed an eight dimensional framework as a result with ideas associated around the dimensions in Table 14.
<table>
<thead>
<tr>
<th>No.</th>
<th>Dimension</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The basis of truth and rationality in the organisation</td>
<td>Within organisations people hold various ideas about what is real and not real and how what is true is ultimately discovered. The key idea is that any system based on cause and effect requires measurement.</td>
</tr>
<tr>
<td>2</td>
<td>The nature of time and time horizon</td>
<td>Ideas about time (short and long term horizons) underlie the orientation of many organisations, ‘ad hoc versus planned’.</td>
</tr>
<tr>
<td>3</td>
<td>Motivation</td>
<td>Beliefs about what motivates people are fundamental to organisational behaviour. Poor systems can lead to misunderstandings about what is required and provide erroneous information upon which to act.</td>
</tr>
<tr>
<td>4</td>
<td>Stability versus change/innovation/personal growth</td>
<td>Individuals have a propensity towards either change or stability. This translates to the organisation having an emphasis on continuous organisational change or conversely on ‘not rocking the boat’. There is potential for quality to improve without additional resources.</td>
</tr>
<tr>
<td>5</td>
<td>Orientation to work, task and co-workers</td>
<td>An individual’s mindset on the balance of work centrality is either as production activity or social activity. This leads to focus either on results improvement or process improvement.</td>
</tr>
<tr>
<td>6</td>
<td>Isolation versus collaboration/cooperation</td>
<td>Organisations may focus on individual effort or group effort. The organisation should benefit from cooperation in the pursuit of quality.</td>
</tr>
<tr>
<td>7</td>
<td>Control, coordination and responsibility</td>
<td>Organisations vary to the degree in which control is concentrated. Loose versus tight control cultures will have different consequences for the work of various individuals, groups and areas.</td>
</tr>
<tr>
<td>8</td>
<td>Orientation and focus – internal and/or external</td>
<td>The relationship between an organisation and its internal and external environment is a key aspect of culture. Organisational improvements related to internal factors will focus on improving people and process. Improvements related to external factors will look for external sources for new information and look to judge success by external benchmarks.</td>
</tr>
</tbody>
</table>
Organisational Culture of Compliance

The security practitioner’s security management model has an end goal of a culture of compliance where behaviour reflects compliance with information security policy and practices. Information security policies are the guidelines that dictate the rules and regulations of the organisation, which in turn govern the security of information (Vroom and Von Solms, 2004) and are therefore significant determinants of culture.

Organisational culture includes the ideas shared by the people within the organisation and communicated between each other. This system of learned behaviour and culture is cited as the single most important factor accounting for success or failure in an organisation (Vroom and Von Solms, 2004). A goal of an organisational culture of compliance therefore seeks to ensure that rules and regulations are normalised as learned behaviour. Recognising an organisation’s culture of compliance towards information security is a major factor in understanding how to manage information security and is a key determinant of the success of information security.

In terms of understanding the culture therefore, it becomes important to recognise the human element in information security and to assess likely compliance when planning protection measures (Guant, 1998). Ultimately, security practitioners will need to evaluate and understand their own personal commitment to security within the organisation to be able to reference the current cultural view towards security (Fitzgerald, 2005). With the human element, understanding what motivates behaviour is intricately tied to understanding likely outcomes. Ryan and Deci (2000) maintain that knowledge concerning the social-contextual factors necessary to encourage and facilitate positive motivation has broad significance.

Recognising Motivation of Behaviour

It is on this basis therefore that the security practitioner can help facilitate a culture of compliance towards security, regardless of senior management support, by endeavouring to understand and apply knowledge surrounding what drives behaviour. Detert et al., (2000) contend that an emphasis is needed on the interplay of enhancing subcultures and
understanding countercultures (those that would oppose cultural change) to create change. An understanding of this is necessary to identify why some cultural changes are effective, and in order to enhance the potential for systemic change. Additionally, understanding the gaps between espoused culture by some organisational members and actual culture as evidenced by artefacts and behaviour is a necessary step to advance systemic change.

Ryan and Deci (2000) assert that the issue of whether people act out of self-interest or are instead driven by external reasons is a significant aspect in all cultural environments. Recognising human beings as generally intrinsically motivated individuals (when the correct external factors are also present) becomes a key consideration for understanding both behaviour and resultant culture. In relation to education and awareness of information security, this is relevant to promoting the assimilation of information and related incorporation of appropriate behaviours through increasing motivation and commitment. By recognition of, and attendance to, the relative presence or absence of supports for basic psychological needs, security managers are better positioned to ‘accurately diagnose sources of alienation versus engagement’ (Ryan and Deci, 2000). Relevant to any of the behavioural theory applied to information security, understanding the concept of a continuum of motivation on behaviour is an extremely helpful aspect.

**Intrinsic and Extrinsic Motivation of Behaviour**

Accumulated research indicates that commitment and authenticity expressed in intrinsic motivation and integrated extrinsic motivation is more likely to be evidenced if certain factors can be met. Further, Ryan and Deci (2000) claim that extrinsically motivated actions can potentially be self-determined as individuals identify with and assimilate their regulation. This may occur, for instance, in circumstances where an appropriate rationale for an action or behaviour is provided with supports for autonomy and relatedness.

Ryan and Deci (2000) propose that Self Determination Theory (SDT) postulates that three conditions, competence, autonomy and relatedness, are necessary to yield
enhanced self-motivation. Encouraging competence (such as through actions including feedback, communications and rewards) can enhance intrinsic motivation for a particular action if a sense of autonomy is present (Ryan and Deci, 2000). A sense of autonomy relates to the perceived locus of causality and therefore the person must experience the behaviour as self-determined for extrinsic motivation to become self-regulated. The third factor, relatedness, is also important, even if only distal according to Ryan and Deci (2000).

Where individuals are not intrinsically motivated towards actions or behaviours, other motivating factors related to extrinsic motivation are important to understand. The goal in this situation becomes one of understanding how to encourage and promote autonomous regulation for extrinsically motivated behaviours. Ryan and Deci (2000) propose that within SDT, the third factor of relatedness becomes more important. Where there is an absence of self-interest for an action or behaviour, a primary facilitator of behaviour is relatedness. Relatedness translates into the equation by virtue that people may be ‘prompted, modelled or valued by significant others to whom they feel (or want to feel) attached or related’ (Ryan and Deci, 2000). This implies that relatedness is highly relevant to internalisation, where internalisation and subsequent behaviour is a desired outcome.

Extrinsic motivation, according to SDT, refers to activities related to a separable outcome and is at variance to intrinsic motivation which relates to an activity for the inherent satisfaction of participating in the activity itself. In other terms, people may be motivated to behave due to factors that are intrinsic or extrinsic, and a self-determination continuum scale can be used to examine this motivation in light of social-contextual factors. Ryan and Deci (2000) theorise that individuals are influenced by the social-contextual conditions that impact where individuals operate on a determination continuum, ranging from a-motivation to intrinsic motivation according to Deci and Ryan (2000) (Figure 40).
Continuum of Motivational Behaviour

SDT describes the far left of the continuum as ‘a-motivation’, or that state of lacking the intention to act. This can result from not valuing an activity, a lack or perceived lack of competence, or not expecting it to produce a desired outcome. To the right of a-motivation, extrinsic motivation contains four subsets, known in SDT as ‘Organismic Integration Theory’ (OIT). These four areas, external regulation, introjected regulation, identified regulation and integrated regulation represent a further continuum within the area of extrinsic motivation. External regulation, the least self-regulation motivation, is characterised by satisfying an external demand or reward contingency.

Behaviour is often experienced as controlled or alienated with a perception of an external locus of causality. Introjected regulation involves behaviours and performing action to reduce feelings of guilt, anxiety or to attain ego enhancement. Behaviour is still motivated by external factors, despite internal feelings affecting intention that results in behaviour. A more autonomous regulation occurs in regulation through identification, where a conscious valuing of a goal or regulation occurs. Integrated regulation is where identified regulations are fully assimilated to the self.

The further along this continuum of extrinsic regulation the more the motivation is integrated to the self and the more autonomous the action. Therefore the goal in achieving a culture of compliance can be facilitated by taking into account an understanding of what factors may impact motivation of behaviour in relation to information security.
Figure 40 Self Determination Continuum Showing Types of Motivation
Plan, Do, Check, Act (PDCA) Process

The PDCA model (ISO/IEC 27001, 2005) is widely referenced in standards as a continuous improvement quality model which can be applied to all processes and involves the following:

- **Plan** – a goal is planned as a series of steps in terms of how to reach the goal and deciding on its implementation.
- **Do** – implement the planned approach involved with resources and actions.
- **Check** - check nominated key activities to ensure that the quality of the output is satisfactory and to identify any new problems as they arise.
- **Act** - to implement changes on a larger scale or to confirm processes.

Conclusion on Security Practitioner’s Model

The model provides an understanding of how to progress information security through an approach that is inclusive of any adopted best practices or standards. In summary, ensuring that security practitioner knowledge can be channelled through an adopted information security management framework is required. This can be applied through a layered model across the enterprise and is fundamental to ensuring a structured, coordinated and comprehensive approach to information security management. This is regardless of which security standards are used. Communication and awareness is essential to the process at all levels, and an understanding of behavioural theory is recognised as having potential to facilitate desired behaviour if taken into account by the security practitioner. The end goal of a culture of compliance is aimed at normalising behaviour, and it is necessary to take into account both the internal and external factors that impact on culture. A monitoring process (the PDCA process) is part of quality control and ensures that the resultant culture of compliance can be monitored and regulated back through the model process.
Security Practitioner’s Model Trial at Southern Cross University

The model is currently being trialled at Southern Cross University and has resulted in several positive outcomes. The model has added to the credibility of the security management program due to the use of a holistic structure. The structure of the model is compatible with the introduction of wider enterprise IT architecture being introduced into the IT department at the university.

Awareness has increased and a noticeable increase in willingness to be involved in security is observable. Another important aspect is that IT management at the university recognise and support the ‘knowledge gathering’ role of the information security manager’s position and, therefore, not only support but expect this role to be involved in security research. This is an extremely valuable outcome as this lends itself to the Harvard Business School recommendation of spending one third time operational, one third tactical and one third strategic. This is to be compared with being swamped by operational demands that leave little time for strategic research and planning, an all too familiar scenario. Measurement of the effectiveness of the model at Southern Cross University is achieved through three main mechanisms:

1) Information to management on the structure and gaining positive feedback.
2) Active participation and feedback from peers in IT is noticeably improving.
3) Observing and assessing the improvements in the appropriate extent of applied technical controls as well as cultural compliance with security.
6 Conclusion

This section provides a conclusion to the study by summarising the research outcomes, providing recommendations, detailing the contributions of this research and highlighting potential for future study.

6.1 Summary of Research Outcomes and Recommendations

As with most things viewed in hindsight, the task of this research project was more onerous than first envisaged. Additionally, the process that was undertaken could now be considerably improved via a more refined and specific approach. This exercise has however demonstrated the valuable potential for surveying and benchmarking security in universities on a more regular basis.

The results of this research indicate that universities face a number of challenges in relation to implementing information security in today’s environment. The response to these challenges is reflected by those institutions that are ‘getting it right’, as being those that have adopted a holistic view of information security within an enterprise business approach. A well-developed information security policy underpinning a structured, formalised information security management program will go a long way towards protecting the value that Australian universities create. Additionally, senior management has an ever increasing mandate to consider information security as part of good corporate governance, and to protect the assets of information, including their reputation and image. Increasingly, universities are recognising and acting on the fact that information is an asset of strategic importance and that the threats are growing and demand a suitable response.

Although many participants indicated areas requiring improvement, it is concerning that a perceived level of complacency towards security exists outside of IT, where security is considered an ‘IT problem’. This is particularly the case where organisations that have not recently experienced a direct and major incident involving a serious business
disruption, appear to retain faith in immunity to information security. The path of least cost and least resistance is sometimes adopted which can have spill over affects into implementation of substandard measures across universities. A large residual responsibility therefore rests with leadership in the ranks of IT to drive security and to be an advocate and leader for security, to ensure that ownership and commitment for security extends outside of IT. Directors of IT in particular are encouraged to lead in security.

Conversely, those organisations that are already well-structured in security, tend to have a more comprehensive and layered view of information security across the enterprise. With sound management practices, and increasing awareness, it is possible that the very people who currently form ‘part of the problem’ can begin to form part of the solution. Finally, the capacity for senior management to set the tone at the top cannot be overestimated. For senior management to view information security as a necessity is expected, however for senior management to view security as an enabler takes the topic to a completely new level. As threats increase, and reliance on information and systems becomes more critical, the need for security can only strengthen. Universities must rise to the challenge.

**Recommendations**

In this section recommendations are provided based on this research project. Specifically, security practitioners should adopt an enterprise approach to the management of security in an effort to harness greater levels of support from senior management and the university community at large so as to facilitate effective security implementation. The discussion on the use of the security practitioner’s management model covers this area in great detail.
The management model is designed to further facilitate these specific recommendations:

1) Increasing senior management awareness and understanding of the role of information security in protecting critical assets and therefore as part of good corporate governance.

2) The use of an enterprise based structured, coordinated and standards-based management approach for security management.

3) Adoption of information security meta-policy using layered abstraction and refinement methods and incorporating international standards-based recommendations for structure and content.

4) Integrating a structured security awareness program that is as automated as possible to ensure increased awareness, education and training amongst the university community and inclusive of a ‘framework and content’ structure.

5) Fostering a culture of compliance towards information security through both behaviour and technology. Behavioural aspects incorporate attempting to normalise behaviour through cultural efforts and technology through technology-based policy enforcement.

**Contributions**

This research work is of significant value to the university sector, as it represents a unique contribution to the security management issues facing Australian universities. It also provides an insightful examination on the current status of play, highlights issues and deficiencies, and provides a realistic recommendation on how improvements in security management can be made.

On a theoretical level this study has, based on the findings, generated a theoretical model as an aid for security practitioners to conceptualise the task before them by way of the security practitioner’s management model. The model, aimed at a ‘how to think’ instead of a ‘what to do’ approach, provides a way for practitioners to focus on transitioning the knowledge they and others possess into security implementation.
On a practical level, this research has provided a detailed articulation of the current status of security management in specific key areas. Additionally, the main issues, barriers and influencing factors that impact the actual implementation of security in Australian universities are provided, with recommendations for addressing those areas. This information in the form of a key findings report was provided to CAUDIT on request. The report was approximately 40,000 words in length including a summary of the questions and answers and recommendations.

This study has also contributed to the general security community through the submission of two conference papers. These include the APIEMS 2004 conference (Lane and May, 2004) and the RNSA 2006 conference (May and Lane, 2006). In addition a paper was provided to the Journal of Theoretical and Applied Electronic Commerce Research (May and Lane, 2006). The study also directly resulted in the creation of a security email forum dedicated to and used by, university security practitioners established by AARNet (Australian Advanced Research Network). This forum is gaining momentum in use, and has extended to other related institutions. It provides a collaborative forum for sharing and discussing security related ideas, problems and solutions. Lastly, this research has brought forward the idea on a wide scale to all involved that security in universities is a growing concern and needs to be elevated to an appropriate level. The study also identified the need for benchmarking security in Australian universities which has the potential as a future research project.

In terms of limitations and unresolved issues, the study found that security is a moving target and therefore the survey was a ‘snapshot in time’. The insights gained from this study are therefore likely to change over time. It is hoped that changes will be positive and that increased maturity in the way universities approach security is adopted. The study focused very much on issues and influencing factors, and therefore examining the technical capacity was outside the scope of this research. It is the firm belief of the researcher, nonetheless, that technology without an appropriate behavioural response towards security from an enterprise perspective is limited.
6.2 Research Learning Outcomes

The learning outcome from undertaking this research project has been significant, not only in terms of understanding the research process but also from a personal level. The main learning outcomes from this project are:

- **Research Scope** - As with many things, scoping a research project properly is a challenging but extremely important aspect. The challenges with scope in this project ranged from the scope being broad and evolving over a longer than expected timeframe. The scope and therefore resultant design took some working out.

- **Data Collection** - Miles and Huberman (1994) helpfully note that the less structured the initial design, the less selective and specific the collection of data will be, as the research is open to all ideas. Initially in this project everything appeared important and so all information seemed pertinent to the formation of key constructs. This experience resulted in large amounts of both data and ideas being obtained, requiring further time to sort through, a common situation according to Miles and Huberman (1994). The learning outcome from this is that it is necessary to take a reality grip on the fact that the world’s problems cannot be solved as a result of the study. Therefore it is essential to be very clear and specific on appropriate data collection in relation to the key research questions connected to the scope.

- **Data Analysis** – It was necessary to include analysis of data from the beginning of the data collection process. There needs to be a process of shuttling between data collection and data analysis, where propositions can be further tested through collection of data as opposed to distinctly collecting data and then analyzing it. This process of collecting-analysing-collecting helped developed an improved understanding of the overall data collection and analysis components of the project. This thought is commented on by Patton (1990) who suggests that there is typically not a point when data collection and analysis begins, and in fact ideas about analysis may form in the course of gathering data.
6.3 Suggestion for Further Study

The study recommends that future research would be well-placed to focus on benchmarking information security management within the university sector. Many university participants expressed a desire to know what other universities where doing, what they were struggling with and what they had succeeded in. It is obvious that universities have an interest in ‘comparing and contrasting’ their efforts against peer institutions. Measurement or benchmarking of security, if developed for the university as a specific industry, or in comparison with another industry, would be a valuable way for Australian universities to rank their efforts towards security. Considering that security is such an intangible concept in the first instance, applying controls in a cost-effective manner is not always easy to understand.

Universities, although increasingly in competition for student numbers, face very unique issues and challenges. Benchmarking has the potential to increase efficiencies for universities by allowing a comparison across the sector in order for institutions to understand their own likely threats and counter-measures. This would facilitate universities in understanding if they are responding appropriately or if they are underweight in areas that will increasingly underscore their competitive advantage.
Appendix A – Survey Instrument

Survey Objective

This objective of this survey is to collect data to help determine key factors impacting the effectiveness of information security management in Australian Universities.

Survey Scope

The survey scope is intended to include all Australian Universities. The participants at each University will be the equivalent of the Directors of IT and/or their Security Coordinators.

Data Collection Process

The survey will be emailed to participants for their review, followed by a scheduled telephone interview with each participant to collect responses.

The phone interview will be digitally recorded to ensure accuracy of responses.

In situations where the IT Directors choose to delegate the interview to their Security Coordinator, it is expected that the Security Coordinator will posses adequate organisational security knowledge so that consistency of responses is maintained. However, it is an aim of the survey to include participation at the Director level as much as possible.

Confidentiality and Privacy

Participants and participating institutions will not be identifiable through this research and are completely assured of anonymity and confidentiality in any publications or other disclosure. All data collected will be securely stored and protected. This project has been submitted to the QUT research ethics committee and has received ethical clearance.
Drafting of the Questionnaire

The questions in this survey have undergone a number of iterations and testing, and have been developed in conjunction with an analysis of leading global information security surveys. The purpose in developing the questions was to help determine key factors that influence effective information security management. The identification of issues and influencing factors impacting the success or otherwise of information security is important in order to better understand how information security management in Australian Universities could be improved.

Part of the theme of this survey is to attempt to obtain a ‘behind the scenes’ look to help understand the current status of information security management. On this basis, the survey provides both quantitative and qualitative aspects, including intentionally open ended questions designed to promote discussion of relevant issues in security management.

Survey Design

The survey questions cover baseline institutional information and the following five areas:

1. Senior Management involvement.
4. Awareness and;
5. Compliance.

Baseline Indicators

1) How many campuses does your institution have?
2) How many central IT staff does your institution have?
3) To what extent is IT centralised or decentralised?
DEST statistics will be separately accessed to determine:

4) How many students your institution has.
5) How many staff your institution has.

Senior Management Involvement

Senior Management is defined as the Executive group, VC, DVC, PVC or Dean positions.

1) Does senior management regularly receive reporting on the status of information security status or on security incidents?
   - Yes
   - No 
   Please provide an explanation

2) Do you consider that senior management has an appropriate understanding of the importance of information security?
   - Agree
   - Somewhat agree
   - Somewhat disagree
   - Disagree 
   Please provide an explanation

3) Does senior management provide the required level of support for information security; if so in what ways has this been demonstrated?
   - Agree
   - Somewhat agree
   - Somewhat disagree
   - Disagree 
   Please provide an explanation
5) If Senior Management involvement in security were to improve, what changes would be required, and how would these changes be reflected in specific senior management actions?

Security Management Approach

1) What is the operational structure for security management and who does the person with security responsibility most directly report to?

2) How would you describe the main approaches that are taken to manage information security?

(please select up to three)

☐ A structured information security management program or strategy exists
☐ Security is managed as part of the IT operational plan
☐ Security is project based
☐ Security is driven by risk management
☐ Security is driven by incident management
☐ Security is primarily guided by security standards
☐ Ad an hoc approach is applied to security
☐ Other method (please specify).

3) Is the current management approach you have adopted proving to be an effective one in terms of achieving security requirements?

☐ Agree
☐ Somewhat agree [Please provide an explanation]
☐ Somewhat disagree
☐ Disagree
4) **What changes would be required to improve the effectiveness of your institution’s information security management approach?**

5) **Do you currently use any security management standards and if so, how have standards been effective in helping with the management of information security?**

6) **What role could CAUDIT play in helping Universities with improving the management of information security?**

---

### Security Policy

1) **Does security policy development and implementation result in the required level of involvement and support from relevant technical stakeholders?**

   - Agree
   - Somewhat agree
   - Somewhat disagree
   - Disagree

   *Please provide an explanation*

2) **Does security policy development and implementation result in the required level of leadership and support from relevant management?**

   - Agree
   - Somewhat agree
   - Somewhat disagree
   - Disagree

   *Please provide an explanation*
3) Is the process for developing and implementing security policies an effective one?

- Agree
- Somewhat agree
- Somewhat disagree
- Disagree

4) Does your institution treat security policies as an essential component of managing information security? (i.e. are security policies and their compliance treated seriously or taken lightly...)

- Agree
- Somewhat agree
- Somewhat disagree
- Disagree

5) How could the policy development and implementation process be improved?

6) Could CAUDIT play a role in assisting Universities with the policy process?

Security Awareness

1) Do you operate a structured and formal security awareness program, or is the process for security awareness more of an ad hoc one?

2) What types of awareness activities are undertaken, to what audience and how often?
3) Is raising security awareness an activity that is given an important priority?
   - Agree
   - Somewhat agree
   - Somewhat disagree
   - Disagree

4) What are the types of activities or events, or situations that have resulted in an outcome that has been very effective in raising security awareness in your institution?

5) Are the existing security activities that are currently undertaken adequately addressing requirements for security awareness?
   - Agree
   - Somewhat agree
   - Somewhat disagree
   - Disagree

6) If security awareness is below the level that it should be, what should be occurring to address this?

7) What are the main barriers to addressing any lack of security awareness?

8) Is there a role that CAUDIT could play in helping Universities with improving security awareness?
1) Does your institution measure compliance or effectiveness of information security either through metrics, key performance indicators, business goals or some other means?

☐ Yes  Please provide an explanation
☐ No

2) Is a ‘culture of compliance’ towards information security reflected through your institution’s work practices and business processes?

☐ Agree  Please provide an explanation
☐ Somewhat agree
☐ Somewhat disagree
☐ Disagree

3) Do you consider your institution to be well-positioned to ‘detect and defend’ against security incidents (including cyber attacks and malicious software)?

☐ Agree  Please provide an explanation
☐ Somewhat agree
☐ Somewhat disagree
☐ Disagree

4) What do you consider to be the top three main causes of security incidents in your institution?
(please select three)

- Viruses and malicious software
- Cyber or internal based attacks
- System or software errors
- System administrator errors or non compliance
- User errors or non compliance
- Hardware failure
- Environmental failure
- Other (please specify)

5) What sort of current security issues (either technology, process or people based) are you most concerned about?

6) What types of either new security technologies or other measures to increase compliance are you considering over the next 1 to 2 years?

7) What percentage of the central IT budget would you estimate is spent on information security?

- Less than 1%
- 1 - 5%
- 5 - 10%
- 10 - 15%
- 15 - 20%
- Greater than 20%
8) What do you consider to be the top three barriers or obstacles to achieving improved security compliance in your institution?

(please select three)

☐ Funding and Resourcing
☐ Awareness and understanding
☐ ‘Culture of Compliance’ (work practices and business processes)
☐ Technology Deficiencies (lack of or inadequate)
☐ Incident detection and response capability
☐ Clear Direction in Security Governance
☐ Organisational Commitment and Support
☐ Inadequate Industry Security Standards
☐ Capacity to measure effectiveness or value of security
☐ Other (please specify)

9) What type of things need to happen for there to be improved compliance to information security at your University?

10) What do you consider to be ‘critical success factors’, for the successful management of information security? (i.e. in your view, what are the key essential factors necessary for ‘getting it right’)?
8 References


Greenwald, M.; Singhal, S.K.; Stone, J.R.; Cheriton, D. Designing an academic firewall: policy, practice and experience with SURF.


Information Security Forum (ISF), (2003), The Standard of Good Practice, Principles and Objectives.


International Information Security Foundation (I2SF), (1999), Generally Accepted System Security Principles (GASSP).


IT Governance Institute (ITGI), (2000), COBIT Framework, COBIT Steering Committee.

IT Governance Institute (ITGI), (2000), COBIT Management Guidelines, COBIT Steering Committee.


Proceedings of the 2003 annual research conference of the South African institute of computer scientists and information technologists on Enablement through technology.


