Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 1 / ISSUE 2 / AUGUST 2006 / 90 – 96

This paper is Available online at
www.jtaer.com

A Model for Improving e-Security in Australian Universities

Lauren May[1] and Tim Lane[2]

[1] Queensland University of Technology, Information Security Institute, l.may@qut.edu.au
[2] Queensland University of Technology, Information Security Institute, tlane@scu.edu.au

Received 04 December 2005; received in revised form 13 May 2006; accepted 26 June 2006

Abstract

As universities seek to adopt increased e-business, e-commerce and e-learning initiates, the overall approach taken for security management within the organisation plays an increasingly relevant role. In many cases security in universities is approached through the addition of tactical solutions. Often systems security is added on as a final consideration instead of during early design stages. This approach can be incomprehensive and inefficient. Although this approach can provide limited security, there is no guarantee that business requirements for security are incorporated and integrated effectively. This situation is partly due to security management in Australian universities being challenged by the complexity of both university culture and diverse operating environments. In many circumstances the champion for security in universities tends to be relegated to an officer in the IT department, hidden away from the business itself. Often this person with operational responsibility for security will have a detailed understanding of what should occur in security, but faces difficulties in determining exactly how to go about achieving this on an enterprise level. In order to assist in securing university IT systems and thereby improving e-business security, this research proposes a security practitioner's management model. This model is aimed at facilitating the transition of security knowledge into actual implementation across the enterprise, with an end goal of an improved culture of compliance towards security practices in the university sector. This work is of significant value as it results from a study into specific security management issues facing Australian universities. This study highlights that future research would be well-placed to focus on benchmarking information security management within the university sector.

Key words: security framework, security management, Australian universities, culture of compliance, information model, e-security

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 1 / ISSUE 2 / AUGUST 2006 / 90 – 96

This paper is Available online at
www.jtaer.com

1 Introduction

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. Australia is an active player in this global village, with the government openly working to promote and accelerate the uptake of electronic business initiatives to increase productivity [2]. Consequently, maintaining continuity in modern organisations ultimately relies on the preservation of information. This process is increasingly achieved through securing the information infrastructures that e-business, e-commerce and e-learning initiatives rely upon.

All Australian industry sectors are dependent on infrastructure that they do not own or control [9]. The intention of this paper is to highlight issues with respect to maintaining the quality of the information in these infrastructures, focusing on the Australian tertiary sector. As a priority of national interest, the Commonwealth Government acknowledges the need to create a culture of security across all industry sectors, and acknowledges the need for a greater focus on IT security in companies, including in outsourcing contracts, and for better communication within companies on security issues. In this context such a culture needs to be nurtured and practiced. Additionally, the government advocates developing a culture of compliance towards security as its number one top 10 security essentials and recognises that "businesses need to not only have e-security measures and programs in place, but also make sure staff are aware of and follow Internet security policy" [2].

The research interests of universities are fundamental to contemporary knowledge. As business organizations, universities are in a unique position to operate and contribute to the development of major e-security IT infrastructures, use and research. Further, universities provide the main source of our future leaders, innovators and technical workforce through their core business of teaching, learning and research [7]. This activity places university communities in a strong supportive and leadership role for the nation in general with respect to ensuring e-security in its information systems.

2 e-Security in Universities

For any modern organization, effective operational control and strategic direction are dependent on the effective management of high quality information. In today's environment, universities are increasingly reliant on information to support their core activities and e-business operations. Universities depend on activities associated with creating, using and sharing information for teaching, learning and research functions. The increase in e-learning and e-commerce is growing dramatically. Typically, e-business initiatives cover three domains of e-business, as is the case with Queensland University of Technology [2]. These include: in the back office, for functions such as administration; in the front office for services such as the provision of online learning and other student services; and with external suppliers, for instance, for e-Procurement and for transmitting data to Department of Education, Science and Training (DEST). Add to this the extensive amount of intellectual property generated by universities, and the organisational importance of information means the significance of security to universities is clearly evident.

It is therefore important to protect information in universities, a function achieved through effective information security practices. Information security ensures a high "quality of service" of information infrastructures and technologies, which support and complement the business goals of the organization. Having appropriate and effective information security control mechanisms in place to ensure the availability, confidentiality and integrity of information is both integral and critical to the process of security management [3]. The essential goals of information security then are much more than just "making sure nothing bad happens"- information security is increasingly associated with enabling the business function.

2.1 Threats in the Tertiary Sector

Universities constitute an important aspect in protecting e-business initiatives from several perspectives. At the institution level, three tangible issues predominate. First, universities host a large number of diverse systems, and act as Internet gateways for large numbers of systems. The approach to securing these systems is not always a structured or consistent process, particularly where Information Technology services are decentralised. This situation can provide a target rich environment for malicious code, as systems are often left ripe for exploitation and recruitment for cyber crime or targeted attacks on other systems. Large scale targeted attacks are growing, involving increased sophistication and organizations known as "bot" networks. Bot (short for robot) networks are "armies" of workstations that have been left exposed to vulnerabilities, then "recruited" by hackers through mass dissemination and exploitation of malicious code. The compromised machines are controlled to carry out synchronized attacks and other malicious activity at the will of the attacker.

Second, university environments characterise a fertile "breeding ground" for IT exploration and research, attracting the interest of Internet hackers and even hackers from within the university community. An unmanaged environment can indirectly promote further development of hacking skills, tools and underground networks. Hacking incidents in American universities are well documented, with identify theft a prime target due to the use of social security

numbers for student identification. In Australian universities, although the student identification numbers are not as useful for identify theft, targets can include a university's finance, student, human resources and payroll systems, as well as any Internet facing systems.

Third, universities from an industry perspective are often a main source for future innovators and leaders [7]. From a community standing perspective, universities are in part reflected through their practices, customs and processes. This includes the extent to which safe computing is promoted and reflected within the security culture of the university, and the security culture that flows from the university sector to industry. Successful security implementations in higher education can also serve as guideposts or standards for related developments in the nation at large [7]. Any successful national response to the threat of cyber security needs to ensure that university networks and their information resources are protected. It also needs to ensure that their computing facilities are not used to launch attacks on critical infrastructure beyond the campus. The values of universities therefore ultimately reflect the values of the nation [7].

2.2 Information Security in the Tertiary Environment

Universities represent an eclectic environment containing an interesting challenge of cultures and technologies. The need to ensure academia is not impeded must be balanced against corporate and business requirements, against a backdrop of a transient and at times explorative student base. This is often mixed in with a residential base, a research environment, broad core values, and a technology base consisting of multiple high bandwidth links to the Internet. Frequently a disparate mix of technologies, systems, operating environments and requirements is involved. The research environments in universities often have values including tolerance, individual autonomy and experimentation. These values contribute ultimately to developments in security, but paradoxically do not necessarily go hand-in-hand with fostering a culture of maintaining operational security [7].

The function of information security management in universities operates necessarily between the corporate mandates associated with the business of providing education, and the cultural and pedagogical pursuit of academic teaching, learning and research. Dealing effectively with threats to information involves the process of information security management to ensure that overall risks, costs and efforts are properly balanced within the organisation.

Within the university sector, there is increasing acknowledgement of the importance of information security and its role in maintaining business continuity and social responsibility. Despite the growing acceptance of the need for security, university members understandably differ in opinion on the application of specific practices and are therefore challenged with adopting the right balance between developing effective security measures and maintaining the fundamental principles of academia [7].

Although information security in universities is a function that is often recognised as important, the priority allocated to security is not consistently commensurate with its perceived importance. This leads to difficulties and conflicts in understanding and agreeing on how security should be implemented and managed. Further, the often cited lack of a coordinated security approach tends to exacerbate the problem of gaining acceptance of security in a diversified and priority competing environment.

Few authors have recognized the fact that organisations not only have disparate security requirements, but that the dynamic business environments in which they operate are important factors that need to be taken into account [13]. The issue of why information security in the tertiary sector is any different to any other sector naturally arises. Higher education sectors in particular are unique in their semi privatized quasi government mode suggesting that establishment and implementation of stringent controls that would otherwise provide appropriate protection of information can in fact prove politically and technically difficult.

In the Educause book, 'Computer Network Security in Higher Education', Luker and Petersen [7] discuss the principals of academic freedom in relation to strategies employable by universities for successful information security awareness and compliance. They also note the difficulties and challenges in this area. These authors 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 [7]. It is necessary to carefully balance work practices with security control to make any headway, and in doing so to foster a culture of compliance.

3 A Culture of Compliance Towards Security

The American Heritage Dictionary [11] provides a definition of *culture* as "the predominating attitudes and behavior that characterize the functioning of a group or organization". A *culture of compliance*, therefore, implies a culture whose participants harmonise towards a particular outcome. From a university perspective, a culture of compliance is inclusive of an awareness and understanding of, followed by compliance to, information security policies, processes and guidelines as part of the norms and values.

In this paper, compliance is based on the relationship between the university's security posture and the levels of compliance reflected at all levels of the university community through its culture. For universities to effectively

incorporate information security into the routine of employees, it is necessary to change the information security culture of universities. In order to change the information security culture, each level of the organisation's behaviour needs to be considered to see how it affects the organization [12]. This involves considering the organization from a layered and systemic approach for the purposes of cultural compliance.

3.1 The Need for a Systemic Approach to Managing Security

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

From an information security perspective the relatively unregulated environment in higher education institutions needs to take into account many contributing factors. Structural issues such as the size of the organization 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.

What is lacking in the literature is a systemic approach to the management of security in Australian universities; one which integrates and shows the relationship between the organisational context, behavioural aspects and 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 organizational requirements. The research undertaken involves an exploratory analysis of key issues, some of which have been discussed previously in this paper. The main final objective of this research is to propose an integrated framework for information security management in Australian universities, an outline of which is given towards the latter part of this paper.

From the security practitioner's perspective, an approach is required that provides 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 the desired culture of compliance can be achieved.

Our 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. The model provides a reference for security practitioners to understand how the process of security knowledge should be transitioned into implementation. Our proposed model is the culmination of our research in this area and the results of an exploratory survey of all Australian universities.

4 The Survey

In order to improve on the current approach that universities adopt for information security management, a survey instrument was administered to all 38 Australian Vice Chancellor listed universities. The survey was aimed at gathering data central to the following three research questions:

1. What is the current status of information security management?
2. What are the key issues surrounding information security management?
3. How could information security management be improved?

4.1 Security Practitioner's Management Model

A detailed analysis of the survey results gave rise to a proposal for a security practitioner's management model (see Figure 1). 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.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 1 / ISSUE 2 / AUGUST 2006 / 90 – 96

This paper is Available online at
www.jtaer.com

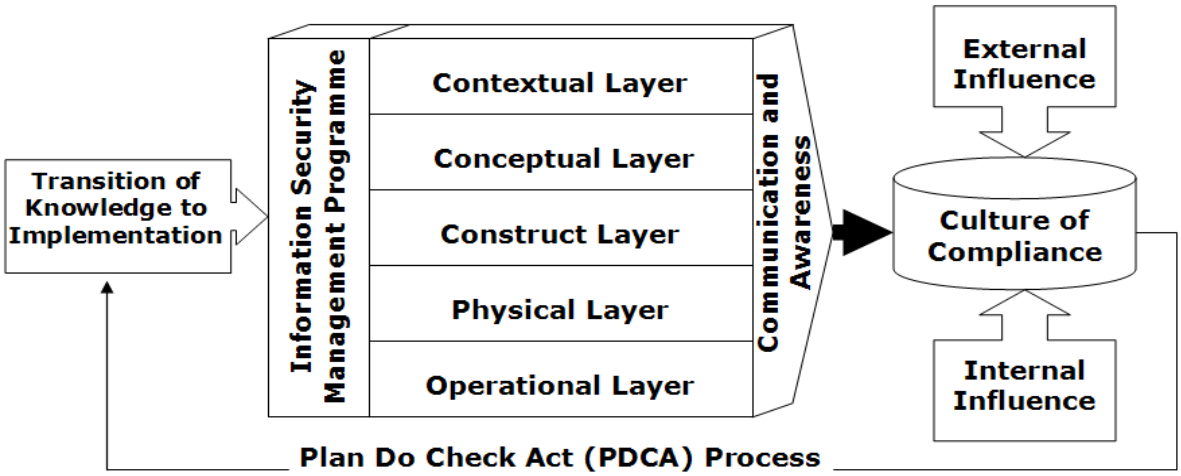

Figure 1: Security Practitioner's Management Model

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 our model is therefore fundamentally different to simply implementing a set of controls based on a pre-defined standard. Our model attempts to describe an end goal of implementation; the "how" to implement rather than "what" to implement.

An important attribute of this model is the acknowledgement that best practices are recognized 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).

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 organizational 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 [6]. 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 to policy. Therefore not only is increased awareness required, but a culture of security must be developed to support the security programme. This requires clear policy with relevant 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 [4].

The model leverages both the SABSA (Systems and Security Business Architecture) method and the Zachman framework [10] 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 is 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 to security must be continuously monitored and adjusted, through the adoption of a review mechanism such as the ISO 17799 "Plan, Do, Check, Act (PDCA)" model, or another similar audit-based monitoring and corrective action process.

4.2 Process Flow Through the Model

The model begins by feeding knowledge (gained from information security understanding, broader organizational 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 channeled 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 organization. Inappropriate application of security procedures can result in an expensive or unacceptable overhead

[8]. Therefore the interface ideally should be a structured and well accepted information security management programme.

The information security management programme then links into a layered structure which begins at the business strategic level, represented as the contextual level, and permeates throughout the organisation finishing at the operational layer (see Table 1). Across the layered structure, the process of communication and awareness facilitates the end byproduct, a culture of compliance. Within each layer, six key questions are asked to determine solutions:

- What needs to be achieved at this level, what assets require protection at this layer
- Why is this being done, i.e. the motivation for wanting to apply security at this layer
- How is this being achieved i.e. the functions need to achieve security at this layer
- Who is involved i.e. the people and organisational aspects of security at this layer
- Where is security needed or applied i.e. the locations where you apply security at this layer
- When is security needed i.e. the time related aspects of security relevant to this layer.

Layer	Description	Application
Contextual Layer	This layer represents the business of the organisation, incorporating the core business drivers and environment.	This layer needs to ensure that information security management is an enabler of the business by supporting the needs of the business. Security must be aligned with the context and culture of the organisation.
Conceptual Layer	The conceptual layer represents the security posture of the organisation, reflected through the risk management approach and supporting policy and stategies.	The concepts and values of information security management are applied in this layer, providing the framework for security in lower layers. Strategies for lower layers are derived from this layer.
Construct Layer	The construct layer symbolizes the virtual constructs of security, including logical security domains.	This is the logical application of security achieved through security design and architecture.
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 represented in products, tools, hardware and software, etc.
Operational Layer	The operational layer involves people and support mechanisms.	This is the human and procedural element, in support of security functionality and ensuring the continuity of the business.

Table 1: Layers in the Security Practitioner's Management Model

The central goal of the model is the required organizational level of a culture of compliance with the depicted external and internal influences viewed as inter- and intra-organizational 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.

4.3 Application of the Model

This model is being applied at Southern Cross University in order to validate its applicability and usefulness. The model is core to the existing information security management programme in operation. (The existing programme predominantly uses the AS/NZS 7799.2:2000 standard "Information Security Management: Part 2: Specification for Information Security Management Systems" [5] and uses the model to progress implementation).

5 Conclusion

Universities increasingly rely on e-business models to facilitate business processes. Security in universities is critical to safeguarding information, however many challenges exists due to university culture and diverse operating system environments. Often ensuring security remains the operational responsibility of officers isolated from the business environment in universities. The proposed model provides an understanding of how to progress information security through an approach that is inclusive of any adopted best practices or standards on an enterprise level. 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 information security management. This is regardless of which security standards are used.

This research work is of significant value to the university sector, as it represents a specific study into 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. The study recommends that future research would be well-placed to focus on benchmarking information security management within the university sector.

References

[1] D. Hickman. (2006, June.) Adoption of e-business. Department of Communications, Information Technology and Arts Website. [Online]. Available: http://www.dcita.gov.au/ie/ebusiness
[2] D. Hickman. (2002, June.) E-business in Education: Section 1 - Case Studies. Department of Communications, Information Technology and Arts, eBusiness in Education Case Studies. [Online]. Available: http://www.dcita.gov.au/__data/assets/pdf_file/21353/eBusiness_Education_3-38.pdf
[3] H. Fulford and N. Doherty, The Application of Information Security Policies in Large UK Based Organisations: An Exploratory Investigation. Information Management and Computer Security. Vol. 11, No. 3, pp. 106-114, 2003.
[4] N. Gaunt, Practical Approaches to Creating a Security Culture, International Journal of Medical Informatics, vol. 6, pp.151-157, 1982.
[5] Joint Technical Committee IT/12, Information Systems, Security and Identification Technology, 2003.
[6] IT Governance Institute and Office of Government Commerce, Aligning CobiT, ITIL and ISO 17799 for Business Benefit, 2005.
[7] M. Luker and R. Petersen, Computer and Network Security in Higher Education. San Francisco: Jossey-Bass, 2005.
[8] C. May, Dynamic Corporate Culture Lies at the Heart of Effective Security Strategy, Computer Fraud and Security, Vol. 5, pp. 10-13, 2003.
[9] National Office for information Economy. (2002, March) Information Security Awareness for Managers: What Do They Really Need to Know? [Online]. Available: http://www.ag.gov.au/agd/WWW/rwpattach.nsf/VAP/(930C12A9101F61D43493D44C70E84EAA)~NOIE+2.PDF/$file/NOIE+2.PDF
[10] J. Sherwood, A. Clark and D. Lynas. (2003, September) Systems and Business Security Architecture. [Online]. Available: http://www.sabsa-institute.org/publications.aspx
[11] The American Heritage® Dictionary of the English Language: Fourth Edition. (2000) [Online] Available: http://www.bartleby.com/61/11/C0801100.html
[12] C. Vroom and R. Von Solms, Towards Information Security Behavioural Compliance, Computers and Security, vol. 23, pp.191-198, 2004.
[13] C. Wood, Information Security Policies Made Easy. West Houston US: Pentasafe Security Technologies Inc., 2002.