2007

Understanding Factors Affecting Success of Information Security Risk Assessment: The Case of an Australian Higher Educational Institution

Ai Cheo Yeo
Monash University

Md Mahbubur Rahim
Monash University, mahbubur.rahim@infotech.monash.edu.au

Leon Miri
Monash University

Follow this and additional works at: http://aisel.aisnet.org/pacis2007

Recommended Citation
http://aisel.aisnet.org/pacis2007/74

This material is brought to you by the Pacific Asia Conference on Information Systems (PACIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in PACIS 2007 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
Understanding Factors Affecting Success of Information Security Risk Assessment: The Case of an Australian Higher Educational Institution

Ai Cheo Yeo  
Clayton School of Information Technology,  
Monash University

Md Mahbubur Rahim  
Clayton School of Information Technology,  
Monash University  
mahbubur.rahim@infotech.monash.edu.au

Leon Miri  
Clayton School of Information Technology  
Monash University

Abstract

To protect information technology assets, effective risk management strategies need to be implemented. However, there is little empirical evidence on the factors that affect the successful undertaking of risk assessment. It is also not clearly known exactly how various factors affect the different stages of risk assessment and whether all factors are equally important across all stages. This research examines the experience of a large Australian university in implementing information security risk assessment and identifies a set of factors that exert considerable influence on the four stages of risk assessment initiative of the university. Finally, the implications of the findings are discussed.

Keywords: Information security, risk assessment, factors, higher education, Australia

Introduction

Business information which is created and stored in electronic format needs to be protected. This is because inadequate protection of organisational information may result in destruction, distortion, delay, disclosure to unauthorised persons (McCumber, 2004). Losses due to breach of information security and other computer related crimes in Australia and worldwide are profound. The 2006 Global Security Survey conducted by Deloitte found that 72% of participants who experienced a breach estimate that it costs their organization greater than US$1 million (Deloitte 2006). The average annual loss per organisation due to security breaches in Australian companies was reported to be A$241,150 in the year 2005 (AusCert 2006). In order to guard against such a huge loss, effective risk management strategies need to be implemented (Doughty, 2003). Risk management refers to the process of designing, developing, sustaining, and modifying operational processes and systems in consideration of applicable risks to information asset confidentiality, integrity and availability (McCumber 2004). An important component of risk management is risk assessment which takes place in four stages. Despite the significant role that risk assessment plays in the identification and protection of organisational information, little empirical investigations are reported in the scholarly literature about the critical factors that influence the success of risk assessment practices in organisations. Hence, it is not clearly known exactly how various factors affect the different stages of risk assessment and whether all factors are equally important across all stages.

To address this gap in the literature, we therefore make an attempt to identify a set of factors drawing upon a review of the existing literature and explore their relevance in context to the information security risk assessment initiative undertaken by a large Australian university.
The findings of our study suggest that a total of six factors including management commitment, competent staff, tools, plans, information security policies, and awareness among staff/students have influence on risk assessment initiative. These findings are useful as they improve the understanding of IT practitioners and researchers alike by providing them with information on which to form sound decisions about the conditions affecting the operations of introducing risk assessment initiatives in real life settings. The findings also contribute in building a rich empirical foundation for further research in this area.

The rest of the paper is organised as follows. In section 2, we provide a brief overview of the various stages involved in information security risk assessment practice. In section 3, we then identify a set of critical factors that were reported in the existing literature to have influence on the success of risk assessment initiatives. Section 4 describes the research approach. Section 5 provides the background information of the case organisation. Section 6 presents the case findings. Section 7 discusses the case findings, and finally Section 8 draws conclusion and identifies areas for future research.

**Risk Assessment: A Brief Overview**

According to Peitier (2001), risk assessment consists of four distinct stages: asset identification, threat identification, vulnerability identification, and control identification and implementation. The first stage of risk assessment is to identify those assets that need to be protected. In the information security context, assets include those information which are transmitted, stored, and processed by an organisation. Assets further include computer and telecommunications resources used for information transmission, storage and processing (McCumber 2004). In a large organisation, determining what needs to be protected can result in the identification of hundreds of important assets. To secure organisational assets requires many skills and resources that are typically scattered throughout an organisation (Caralli et al., 2006). The second stage is concerned with identifying threats. A threat is a set of circumstances that has the potential to cause loss or harm; it can be a natural or man-made attack (Pfleeger et al. 2003). According to Deloitte’s 2006 Global Security Survey, there continues to be an exponential increase in the sophistication of threats and the criminal profile is shifting from script kiddies and disorganised hackers to well funded organised crime rings. The third stage identifies vulnerabilities. A vulnerability is a weakness in the security system that might be exploited to cause loss or harm (Pfleeger et al. 2003). The number of vulnerabilities reported to CERT has increased over the years. Organisations and their surrounding environment are often changing rapidly. Changes in operational and security software and hardware and even upgrades, improvements, and business-centred changes can create security holes and gaps (Taney et al. 2006). The ever changing threat environment and increasing vulnerabilities pose a great challenge to risk assessment. Nearly half of the 2006 AustCERT Survey respondents cited keeping up-to-date with computer threats and vulnerabilities as problematic. The fourth stage of risk assessment identifies and implements controls. Organisations need to know the extent of the damage that an attack can cause and the possibility of occurrence in order to select appropriate controls to prevent the attack. However, there is a lack of reliable and current data which makes it difficult to determine which information security risks are most significant and which controls are most cost effective (GAO, 1999; Farahmand et al. 2003). There is a tendency of organisations to fight security risks using technical controls. However, technical controls can never be a panacea for information security as security technology can be rendered useless by the actions of computer users. The success of information security thus depends in part upon the effective behaviour of individuals in the use of technology. The Deloitte Survey suggests that although it is becoming more difficult to get at resources using external brute force attacks, it
is becoming easier to get at these resources by exploiting social engineering attacks against the organisation’s people. Combating the threats of social engineering would require education of users. Sixty percent of the AusCERT Survey respondents cited changing users’ attitudes and behaviour regarding computer practices as one of the most challenging aspect of computer security management (AusCert 2006).

**Literature Review: Identifying Relevant Factors**

The scholarly literature on the factors affecting risk assessment practice is sparse and there is a lack of empirical research in the area of security risk management (Kotulic et al. 2004). We have therefore consulted literature on factors affecting information security which helps us to identify a set of factors that may potentially affect the successful undertaking of information security risk assessment practices in organisations. These are listed in Table 1 and are briefly explained below:

Management Support: An often cited success factor affecting information security is the support from management (General Accounting Office 1999; Stoneburner et al. 2002; Information Systems Audit and Control Association 2005; International Standards Organisation 2005; European Network and Information Security Agency 2006; Torres et al. 2006). A study reported by General Accounting Office (1999) presents the practices of four organisations that had institutionalised practical risk assessment methods and finds that senior management support is important to ensure that risk assessments are taken seriously at lower organisational levels. According to this report, management support is also important that resources are available to implement program and to ensure that assessment findings result in implementation of appropriate changes to policy and controls. Support and commitment of management needs to be continuous, unshakeable and visible (ISO 2005; European Network and Information Security Agency 2006).

<table>
<thead>
<tr>
<th>Critical Success Factors</th>
<th>Reference Discipline</th>
<th>Literature Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management support</td>
<td>Risk assessment/</td>
<td>GAO (1999), Stoneburner et al. (2002)</td>
</tr>
<tr>
<td></td>
<td>Risk management</td>
<td></td>
</tr>
<tr>
<td>User security awareness</td>
<td>Risk assessment/</td>
<td>Stoneburner et al. (2002)</td>
</tr>
<tr>
<td></td>
<td>Risk management</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Risk management</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Information security</td>
<td>ISACA (2005), ENISA (2006)</td>
</tr>
<tr>
<td></td>
<td>Risk management</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Information security</td>
<td>Torres et al. (2006)</td>
</tr>
<tr>
<td>Accountabilities</td>
<td>Risk assessment/</td>
<td>GAO (1999), Smith et al. (2001)</td>
</tr>
<tr>
<td></td>
<td>Risk management</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Information security</td>
<td>ISACA (2005), ISO (2005)</td>
</tr>
<tr>
<td>Ongoing assessment</td>
<td>Risk assessment/</td>
<td>Smith et al. (2001), Stoneburner et al. (2002)</td>
</tr>
</tbody>
</table>
Users’ Security Awareness:
A successful risk management program relies on the awareness and cooperation of users who must follow procedures and comply with the implemented controls (Stoneburner et al. 2002). This requires effective marketing of information policy to all users to achieve awareness and providing appropriate and continuous training and education (European Network and Information Security Agency 2006; Information Systems Audit and Control Association 2005; ISO 2005). The use of disciplinary measures should be avoided (European Network and Information Security Agency 2006; Torres et al. 2006).

Business Experts: To ensure that all important risk factors are considered, business experts should participate in the risk assessment process (Chang et al. 2006; European Network and Information Security Agency 2006; General Accounting Office 1999; Information Systems Audit and Control Association 2005). Business experts have understanding of the criticality and sensitivity of individual business operations and of the systems and data that support these operations and they are in the best position to ensure that recommendations for risk reduction techniques are implemented effectively (General Accounting Office 1999).

Technical Experts: The risk assessment team must have the expertise to apply the risk assessment methodology (Stoneburner et al. 2002). Technical experts bring to the risk assessment process an understanding of existing systems designs and vulnerabilities and of the potential benefits, costs and performance impacts associated with new controls being considered (General Accounting Office 1999). According to Torres et al. (2006), a critical success factor for ensuring security management of information systems is having honest, competent, smart and skillful systems administrators.

Accountabilities: Executive and line management should be accountable for implementing, monitoring and reporting on information security (Information Systems Audit and Control Association 2005). Accountabilities and responsibilities should be clearly established for managing risk (Smith et al. 2001). The GAO study found that organisations with strong security programs made their business units responsible for initiating and conducting risk assessments as they are in the best position to determine when an assessment is needed and to ensure that recommendations for risk reduction techniques resulting from the assessment were implemented effectively (General Accounting Office 1999; Smith et al. 2001). The successful implementation of information security requires the implementation of a
measurement system that is used to evaluate performance in information security management (International Standards Organisation, 2005).

On-going Assessment: A successful risk management program relies on an ongoing evaluation and assessment of the IT-related risks (European Network and Information Security Agency 2006; Smith et al. 2001; Stoneburner et al. 2002). Threat sophistication is increasing rapidly and dynamic evaluation of information security has become the only way to keep up with the pace (Torres et al. 2006). Risk assessment will change as more knowledge becomes available, technologies improve and business environment changes (Smith et al. 2001).

Alignment with Organisation’s Objectives: Information security policy, objectives and activities should reflect business objectives (European Network and Information Security Agency 2006; Information Systems Audit and Control Association 2005; International Standards Organisation 2005; Torres et al. 2006). ISACA recommends that each line of business that “owns” information requiring specific levels of confidentiality, integrity and availability should designate a liaison to work with the information security manager to ensure that requirements are properly reflected and prioritised in the information security strategy (Information Systems Audit and Control Association 2005).

Funding: Provision to fund information security management activities is critical to the successful implementation of information security within an organisation (International Standards Organisation 2005; Torres et al. 2006). ISACA suggests that senior management should require that all requests for technology solution expenditure include technology risk identification and risk mitigation requirements as part of cost-benefit analysis (Information Systems Audit and Control Association 2005; Torres et al. 2006).

Balance Risk and Controls: The use of formal controls should always be balanced against the level of risk exposure (Smith et al., 2001). An organisation should only undertake necessary tasks and avoid over-control which leads to a waste of valuable resources (European Network and Information Security Agency, 2006).

The factors identified above which are believed to affect the success of risk assessment practices however need to be evaluated for their influence in empirical settings. In particular, the relevance of these factors in context to the Australian organisations has yet to be examined. We however acknowledge that the set of factors listed in Table 1 are not comprehensive, and it is therefore our intention not only to explore the relevance of these but to find out the existence of any additional factors unique to the Australian context.

**Research Approach**

As this research project is in its early development stage and little is articulated in the scholarly literature about how various factors are likely to affect the practice of information risk assessment, a suitable qualitative approach was selected to address the research concern. Out of two prominent approaches (i.e. exploratory case study and grounded theory), we decided to choose an in-depth exploratory case study approach for two reasons: First, we are not attempting to test any theory rather it is our intention to contribute to theory development by identifying how various factors may potentially influence successful information security risk assessment practices. Second, we argue that information security risk assessment initiatives are more likely to take place in a dynamic environment because of the complex interplay of a diverse range of factors, threats and controls which add to the complexity to the
smooth operation and introduction of security risk assessment practices. Hence, it is critical to capture the experiences of the relevant people and the context of their actions to understand how various factors may exert influence on actual risk assessment practices. Exploratory case studies are particularly suitable for understanding phenomena within their organisational context (Zikmund, 1997; Yin, 2003). The grounded theory approach was not considered to be appropriate because it is more suitable for those situations where the researchers really do not know what process they are going to discover (McAllister, 1999). This is not the case for our research. Moreover, due to time constraints that the researchers had (as this project is part of a postgraduate program), the use of grounded theory was not deemed to be attractive because such an approach is known for being really time consuming (Mellion and Tovin, 2002).

The higher education sector in which the case organisation operates was chosen because information security has become a pressing issue for large universities which often maintain campuses in various countries where information security policies and controls may differ significantly. Higher education industry thus presents a unique situation within which the research concerns can be usefully investigated. The selection of the participating university is guided by the illustrative strategy principle (Veal, 2005) because of our intention to illustrate the effects of factors which could be observed in a large multi-campus organisation that has made a serious attempt to undertake information security risk assessment.

Several rounds of face-to-face in-depth interviews were sought from two key informants who are responsible for the formulation of IT security strategy for the university. They include one IT security manager and a senior IT security analyst. The IT security manager has been with the university for the past ten years in various capacities and is currently the manager responsible for the IT security and risk management of the university. He conducts risk management and generates risk profiles for every divisional unit and faculties of the University. The IT security analyst has been with the university for the past five years. His major responsibilities include ensuring that appropriate continuity and recovery plans are in place for the critical services university-wide as well as for the commercial entities of the university. Each interview lasted for about an hour, was tape recorded, and subsequently transcribed. Interview transcripts were later sent to the interviewees for review and were revised based on their responses. The revised interview transcripts were analysed using the notion of coding scheme (Miles and Huberman, 1994; MacQueen, 1998) based on the interview protocol. Using this coding scheme, each interview script was examined by two members of the research team. Any differences were resolved through mutual discussion. These two interviewees also provided the researcher with some internal documents relating to the policies of risk assessment which helped the researcher in corroborating the information gathered from the interviews.

Reliability was addressed by clearly conceptualizing research variables, using multiple coders and case study protocol (Miles and Huberman, 1994; Yin, 2003). The factors involved in the research project were clearly defined and a summary of these definitions was provided to the interviewees prior to commencing the interviews. This was done in order to ensure that the interviewees were able to interpret the research variables in a consistent manner. Additionally, following Yin’s (2003) guidelines, a case study protocol was developed, which together with a copy of the summary of definition of research variables (i.e. threats, controls, and factors), was sent to the interviewees one week prior to the actual date of the interview. Data collected from the university were analyzed using the pattern matching logic (Trochim,
which enabled the researchers to compare the pattern of outcomes of factors reported in the existing literature with the pattern of outcomes deduced from the case data collected through verbal interviews and other documentary sources of the university.

Case Description
The case organisation is a large and highly reputed university that is located in a state capital city, Australia. It has attracted over fifty thousand students from over 100 countries, and is being served by about five thousand staff. The university has several campuses and maintains its presence in several overseas countries. Due to its diversity and extensive use of the Internet, the threats encountered by the university are very high. Its ITS division consists of about one hundred staff and has employed a wide range of IT-enabled applications in support of the major business processes supporting the core functionalities of the university. The university has a large network consisting of more than 1350 network devices serving 20000 data points in 150 buildings on 20 sites. It has 200 student laboratories housing around 4000 computers. The university relies heavily on the network for the delivery of academic and administrative services. Quality of Service features are being implemented for not only mission-critical enterprise applications, but also delay-sensitive applications such as video and Voice Over IP. There is a wireless network which allows students/staff to connect to the network and the Internet from desktops, laptops and even PDAs. The network is critical to the business of the university and is supported 24 hours a day 7 days a week.

1. Case Study Findings
Empirical evidence has emerged which suggests that risk assessment initiative is influenced by seven critical factors. These include: management commitment, competent staff, tools, funding, plans (resource planning and disaster recovery), information security policies, and awareness among staff and students in the university. It appears that most of the frequently cited factors (shown in Table 1) also affect the risk assessment practice of the university. In addition, a new factor (called presence of software tools) which helped enormously in identifying vulnerability and identifying appropriate controls was deemed important. Many of these factors were found to have contributed to all four stages of the risk assessment process. However, there are some factors which are related to one or more specific stages. This is shown in Table 2.

| Table 2: Relevance of factors affecting various stages of IS security risk assessment |
|-----------------------------------------------|---------------|----------------|-----------------|-----------------|
| Success factors                              | Asset Identification | Threat Identification | Vulnerability Identification | Control Identification |
| Management commitment                        | Yes            | Yes             | Yes             | Yes             |
| Competent staff                              |                | Yes             | Yes             | Yes             |
| Information security policies                 | Yes            | Yes             | Yes             | Yes             |
| Security awareness                           |                |                 | Yes             | Yes             |
| Tools                                        |                |                 | Yes             | Yes             |
| Plans for information security policies       |                |                 | Yes             | Yes             |
Management commitment was found to be important for all the stages of risk assessment in the university. It was reflected in terms of management’s involvement in assigning school managers (known as service managers) in the risk assessment process to identify the critical assets and threats associated with them. Management commitment to risk assessment is also demonstrated by their endorsement of an escalation procedure which is in place to ensure that issues regarding risk assessment can be raised when appropriate actions are not taken at an operational level. A successful risk assessment requires the input of highly qualified staff. ITS ensures that its highly qualified staff keep abreast with current developments in information security. They undergo training and are encouraged to attend conferences. The ITS holds monthly IT Security Forum where knowledge and other issues are shared with faculty representatives. The ITS manager commented:

“Our ITS people are good in what they do and maintaining such a competent team is essential for the successful introduction of risk assessment initiative.”

The use of vulnerability assessment tools was found to be quite useful in the risk assessment process. For instance, assessment tool such as Foundstone has been deployed across all faculties and administrative units to detect vulnerabilities. The deployment of intrusion detection tools helps the ITS division to identify unauthorised access attempts which are potential threats. The IT Security Manager explains:

“The intrusion detection systems give us an indication of which subnet is generating lots and lots of logs. So we can say that that is the most exposed subnet and it has got lots of servers on it. We can go and work that out in terms of priority and all that…”

Effective planning is essential for a successful risk assessment in the university. Planning includes both resource planning and disaster recovery. The ITS division has plans in place for the continuity of operations in the event of personnel taking a vacation or leaving the university. The IT security analyst stresses the importance of shared knowledge:

“If only one person is doing a particular activity, it is a disaster. We share the responsibility. The sharing of responsibilities within the unit reduces the risk of a person leaving. We identify the key persons and their duties within ITS and share the responsibility. We share the knowledge on a regular basis.”

Disaster recovery plans were developed by the university to deal with contingencies. The disaster recovery plan is a proactive measure taken to reduce the impact of a disaster. As the IT security analyst explains:

“Having disaster recovery and other test plans in place is important. We think now so that we don’t need to think when disaster happens. It is more of execution.”

The university has an information security policy in place. An information security policy is important as it provides a framework for best operational practice, so that the university is able to minimise risk and respond effectively to any security incidents which may occur. A security policy also ensures that the university complies with relevant legislation in this area. According to the IT security manager:

“Implementation of security policies has stopped direct inbound access to client computers. It has also prevented copyright issues arising out of unauthorised sharing of music and files from various websites.”

Funding was found to be a major concern affecting risk assessment practice. Funding was needed to introduce the software tools for identifying vulnerability and recommending controls. Management was found to be quite generous when it came to allocate funding to enable the IT managers to conduct the risk assessment properly. The university management also understood the cost of not implementing appropriate control strategies to combat risk and hence funding was also given to training IT staff on security issues.
Awareness and understanding is essential to implement information security policies and to ensure that related controls are working properly. Users cannot be expected to comply with policies they are unaware of or do not understand. The IT security manager describes measures taken by the university to increase security awareness:

“We are planning to have an Information Security Day and presentations will be made to staff and students. From a technical perspective, we have technical representatives at the faculties and departments for end user education. We also have IT Security At Home campaign. We distribute ‘Security at Home’ brochures to staff. The campaign helps in making the staff and students aware of the risks of connecting to the university network from home. We also provide awareness to researches on IT security through various brochures.”

Discussion

The empirical findings emerged from the participating university confirm the importance of key critical success factors reported in the literature (as listed in Table 1). In addition, a new factor (i.e. the use of appropriate software tools) in risk assessment was identified. The important role that management plays by allocating resources and changing necessary university policies and procedures for the smooth conduct of the risk assessment process was recognised. The university management provided necessary funds and adequate resources for implementation of escalation procedures to ensure recommended controls are implemented. This observation is consistent with the existing literature (Eloff, 1988, AUSCERT, 2005, GAO, 1999) which suggests that senior management commitment is important to ensure that risk assessments were taken seriously across all organisational levels.

The involvement of competent individuals from the ITS division in the risk assessment process is considered to be a success factor. Appropriate allocation of responsibilities and knowledge transfer among the individuals in the ITS division has resulted in sound risk assessment. This has ensured that in the extended absence of a particular individual, there is adequate back up within the division. This ensures continuity in function and the assurance of quality in the risk assessment process. Competent staff ensures that the all the security risks are identified and appropriately addressed. This observation is also consistent with the literature which argues that competent individuals must conduct, oversee and guide the risk assessment process (Wood, 1987; GAO, 1999).

There was a great deal of participation from the service owners (i.e. school managers) as well as the technical experts from the ITS division during the risk assessment process in the university. The involvement of business and technical experts is regarded to be a critical factor affecting risk assessments. Their involvement leads to a holistic consideration of issues and better deliverables from the process. This observation is in agreement with the literature which suggests that drawing on the knowledge and expertise from a wide range of sources is essential to ensure that all important risk factors have been considered (GAO, 1999; ENISA, 2006). Business operations and process experts, security operators, information resource management personnel, information technology analysts and even the involvement of internal auditors in the risk assessment process improves the application of risk assessment to a great extent. The right blend of technical and business expertise ensures the robustness of the risk assessment process so that the findings and controls identified through the process, once implemented, would indeed eliminate or at least mitigate the risks.

At the university, the existence of documented policies and procedures was found to be
another important factor. Security policies are an effective control for information security and they have been made available online. Risk assessment deliverables are also documented to a certain extent in the university. This is consistent with the views expressed in the literature which suggests that documented policies and procedures provide a structured approach to risk assessment (GAO, 1999; Von Solms and Von Solms, 2004). The documentation of results of previous risk assessment can act as the starting point for subsequent risk assessments. This would give security members in a team enough material and information to start without reinventing the wheel.

A new factor that affected the risk assessment is the use of appropriate tools. Foundstone and Nmap are software tools which are used by the university to reduce the estimation factor in the risk assessment process and increase the level of surety in the mitigation of risks, especially the technical ones. The role of useful tools in risk assessment has received little attention in the existing literature. Awareness among staff and students was found to be a success factor in the university. Measures like Information security day, brochures for staff and students are initiated to raise the awareness in order to prevent the exploitation of unaware users to compromise the system. An informed user can act as the final layer of defense. There is evidence in literature that awareness amongst the users can prevent lots of unauthorized access to systems. Training is an important tool in raising awareness.

**Conclusion**

This paper has presented the experience of a large Australian university in undertaking its information risk assessment initiative. A set of factors were identified that exerts considerable influence on various stages of the risk assessment initiative. These factors are then discussed in light of the existing literature. Although many of these factors are not new and are already reported in the existing security literature, their relevance in connection to risk assessment has not been empirically discussed. Additionally, a new factor (i.e. use of suitable software tools) was identified that was considered to be a great facilitator of the risk assessment practice. Thus, the principal contribution of this paper is to reinforce the explanatory ability of the factors drawn from the existing literature to satisfactorily describe the undertaking of information risk assessment practices in large organizations. The findings reported in this paper are important because an empirical evaluation of the conditions affecting various stage of risk assessment is not yet widely available.

Finally, this study is not without weaknesses. First, only one case was investigated in this research project and hence future research studies should focus on multiple cases to improve reliability of our findings. Second, our findings should be treated with caution because information was primarily collected based on the views expressed by two stakeholders from the university. We believe that rich insights about risk assessment practice can be obtained when views of service managers (i.e. school managers) could also be collected. Third, there is a need to extend our study by comparing the risk assessment initiatives of universities with large private companies in order to determine the influence of industry context on risk assessment practice. Finally, further studies need to be conducted among educational institutions in developing countries to find the influence of any cultural factors on risk assessment process.

**References**

Information Systems Audit and Control Association, "Critical elements of information security program success." 2005
Peltier, T. Information security risk analysis, Auerbach, Boca Raton