12-4-2013

Information Security Management: Factors that Influence Security Investments in SMES

Zhi Xian Ng
University of Melbourne, ng.xhixian@gmail.com

Atif Ahmad
University of Melbourne, atif@unimelb.edu.au

Sean B. Maynard
University of Melbourne, seanbm@unimelb.edu.au

DOI: 10.4225/75/57b56667cd8e5
11th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia, 2nd-4th December, 2013

INFORMATION SECURITY MANAGEMENT: FACTORS THAT INFLUENCE SECURITY INVESTMENTS IN SMES

Zhi Xian (Sean) Ng, Atif Ahmad, Sean B. Maynard
Department of Computing and Information Systems
University of Melbourne, Australia
ng.xhixian@gmail.com, atif@unimelb.edu.au, seanbm@unimelb.edu.au

Abstract
In the modern information economy, the security of information is critically important to organizations. Information-security risk assessments (ISRAs) allow organizations to identify key information assets and security risks so security expenditure can be directed cost-effectively. Unfortunately conducting ISRAs requires special expertise and tends to be complex and costly for small to medium sized organizations (SMEs). Therefore, it remains unclear in practice, and unknown in literature, how SMEs address information security imperatives without the benefit of an ISRA process. This research makes a contribution to theory in security management by identifying the factors that influence key decision-makers in SMEs to address information security risks. The study has identified three key motivating factors from a series of case studies. Firstly, the need for sufficient information security to maintain reputation with external clients whilst conforming to the level of information security practices typical in industry culture. Secondly, (mis)perceptions of the existing state of information security and level of exposure to security threats in the organization. Thirdly, the perceived need to focus on higher corporate business priorities rather than on information security.

Keywords
Information Security, Risk Management, Small to Medium Enterprises, SME, Information Security Investment

INTRODUCTION

The security of information systems in organizations has become increasingly important in the modern information intensive environment. In an era of global connectivity and increased use of ICT by organizations, the need to protect information systems from security breaches has become a significant management priority (Ransbotham et al. 2010). This is especially true for small to medium sized enterprises (SME's) where security incidents can be expensive. A Price Waterhouse Coopers (PWC) survey in the UK, reports that incidents can cost £15000 - £30000 per small organization (PWC 2012).

International guidelines on information security 'best practice' advise organizations to conduct risk assessments to determine priorities for security expenditure (ISO/IEC 27002:2005). Given security risk assessments are expensive and complex processes to implement and require specialist expertise, they are more suited to large (resourceful) organizations. SMEs form a large portion of national economies and rely on information systems but with relatively fewer resources than their larger counterparts. Therefore, it remains unclear in practice and unknown in literature, how SMEs are able to address information security risks given minimal resources.

This research is exploratory in nature and is motivated by two factors. Firstly, to determine if SMEs implement a formal security risk assessment process, and if not, how SMEs prioritize expenditure on information security. Secondly, to understand the factors (e.g. technical, social or economic) that influence decisions to invest in information security. These factors will form the basis for future research into security decision-making theory for SMEs.

This research seeks to answer the following research question: What factors influence decision-makers in SMEs to invest in information security?

For the purposes of this study an SME is defined as an organization that has less than 200 employees (Atkins & Lowe 1996). To identify these motivations five case studies of SME security practices were conducted to determine how they undertake information security initiatives. The data collected was analysed using open, axial and selective coding (Neuman 2006).

This research paper is organised as follows. First, the background to the study is discussed including current approaches to risk management, and security standards. Second, the interview research approach is explained. Third, the set of interviews is analysed and discussed leading towards the identification of three main motivations of SME's for investing in information security initiatives. Finally, the paper concludes with a discussion of the main contributions and limitations of the research

INFORMATION SECURITY RISK MANAGEMENT IN SME'S

Information Security

Information security can be thought of as "the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability" (NIST 2009). Essentially, information security is the process of protecting information and information infrastructure (both content and services) from unauthorized access that results in disclosure, modification or destruction of information, and modification or disruption of IT services. These can be accidental or malicious and perpetrated by insiders or outsiders.

Information security management consists of a series of processes by which formal, informal and technical controls are applied to address security risks (Sveen, Torres and Sarriegi 2009). Formal controls include legal mechanisms, risk assessments, audits, and policies and procedures that provide advice to personnel on the one hand and outline punitive measures for non-compliance on the other. Legal mechanisms can be broadly grouped into two main categories namely contractual mechanisms and patents. Non-disclosure agreements (NDA's) are an example of a contractual mechanism that seeks to prohibit the sharing and reuse of specific information or capabilities, and impose penalties in an event of breaches of such agreements (De Faria and Sofka 2010, Norman 2001). Technical controls include firewalls, intrusion detection systems, and other such devices that regulate access to resources. Informal controls such as training and education influence security culture.

Information security management assists organizations in maintaining business continuity, minimising business exposure to damage and maximising investment returns (Chang & Ho 2006). According to the ISO/IEC 27005 standard on the security management code of conduct, security risk assessments are a critical first step to a comprehensive security program as it determines the level of exposure of organizations.

Information Security Risk management

Information security risk management is a staged approach by which organizations can achieve a desired level of security. A risk assessment is conducted by identifying information assets that exist within the purview of an organization. Subsequently, threats and vulnerabilities are identified to generate scenarios that result in a breach of confidentiality, integrity and availability. Quantitative and/or qualitative methodologies are used to estimate the probability of each scenario occurring and its associated impact (Bandyopadhyay et al. 1999; Gerber and Von Solm 2005; Frosdick, 1997). Subsequently, steps are taken to ensure that information assets are protected to the greatest extent possible or to an acceptable level. The prioritized list of scenarios allows security expenditure to be directed towards the highest risks (i.e.

the scenarios that have a relatively high impact and high probability). Organizations may handle the risk by implementing controls to prevent the potential breach from occurring (risk avoidance), reducing the impact after the breach has taken place (risk mitigation), doing nothing at all (risk acceptance) or placing the responsibility on an external party such as obtaining insurance (risk transfer) (Whitman & Mattord 2011; ISO/IEC 27005 2008).

An inadequate risk assessment, or the absence of one, implies that the organization has not used its resources to best advantage in addressing security risk exposure. For example, if certain assets were not considered in the risk assessment, then they may be unprotected. Likewise, if the estimation of probability and impact is inaccurate, not enough consideration has been given to security controls and protective strategy. Ultimately, exposure to security risks can lead to adverse consequences for organizations, such as leakage of sensitive information and interruption or destruction of critical IT services.

There are a number of information-security risk assessment methodologies available in Europe, the US and Australasia. These include FRAP, CRAMM, COBRA, OCTAVE, OCTAVE-S and CORAS (Peltier 2001; Yazar 2002; Alberts & Dorofee 2004; den Braber 2007; Dhillon 2007). Although they differ in their make-up, order and depth of activities, they generally engage in risk identification followed by risk analysis (Whitman & Mattord 2011; Shedden et al. 2006; Dhillon 2007).

Ultimately, the aim of risk management is to reduce information security risk to an acceptable level in the organization (Gerber and von Solms 2005). Performing risk assessment in an organization will allow for the application of systematic methods to identify security risks and guide them on the countermeasures as well as justify their expenditure for security (Spinellis et al. 1999).

Information Security Risk Management in SME's

In practice, information security risk assessments are both complex and costly to implement and require specialist expertise to manage the process (Shedden et al. 2006). Identification of all information assets in an organization requires a dynamic inventory of assets to be created in order to maintain a competent tracking system. Workshops must be conducted to identify possible scenarios where the confidentiality, integrity and availability may be influenced. The probability and impact of each such scenario (for each such asset-threat combination) must be estimated at both user level (those who are familiar with the operationalization of the asset) and management level (those who can better estimate organizational impact). Such a process is time-consuming and costly for organizations and frequently results in over-simplification (to save on resources) and misapplication (due to lack of expertise available) (Shedden et al, 2006).

SMEs are distinguished from their larger counterparts primarily by the number of employees, but also by financial resources and managerial process (Atkins and Lowe, 1996). In most such organizations there may not be a dedicated security resource, therefore they are unlikely to have the expertise necessary to manage an information security risk process. Further, although SMEs may not have as many assets as larger organizations, the number of information assets is likely to run in the thousands, especially if each document is considered a separate asset. Dimopoulos et al. (2004) argues there are three key reasons why SMEs may not be applying formal risk assessments. These are 'restricted budgets', 'lack of expertise' in applying the risk methodologies and 'lack of awareness' of the need to perform risk assessments. However, Dimopoulos et al. (2004) does not conduct a field study to verify these factors. Therefore, in addition to identifying the factors that influence security spending, this research project also seeks to test whether the factors that prevent SMEs from conducting risk assessments can be confirmed in the real world.

RESEARCH METHODOLOGY

This research adopts a multiple case study approach to explore the factors that influence decision-makers in SMEs to invest in information security. The research project being conducted is exploratory in nature. Exploratory research is defined as "research in which the primary purpose is to examine a little understood issue or phenomenon to develop preliminary ideas and move toward refined research questions by focusing on the 'what' question" (Neuman 2006, p33). The multiple case study approach is appropriate as it captures multiple perspectives of the phenomenon and allows for cross case analysis and generalisation to occur.

A total of five case studies were conducted. The case study organizations were selected based on their size (SME's), their willingness to be involved, and the industries in which they operated. Organizations were purposely selected from different industries and ranged in size from 10 to 50 personnel. Due to the size of the organizations selected, there were few people involved with the information security function and in every instance, all of these people made themselves available for this research. Figure 1 shows a summary of the organizations involved in the research.

Organization	Location	Sector	#	Participants
TechCons : A technology consulting and implementation firm that focuses on enterprise content management as well as workflow automation.	Singapore	Technology	20 employees	Principal Consultant / Partner [participant 1] Senior Consultant [participant 2]
GPSComms: A technology production organization focusing on designing high performance integrated GPS and wireless modules.	Singapore	Manufacturing	10 employees	Principal Consultant / Partner [participant 3]
ElectCont: A company that provides electronic control solutions for gas turbines used in the power generation, oil and gas sectors.	Malaysia	Energy	120 employees	Product & Business Development Manager [participant 4]
Consult: A management consultant company, focusing on mapping competencies as well as assessing employee capabilities based on their required competences.	Singapore	Management	10 employees	Chief Technical Officer [participant 5]
Audit: An audit firm. The organization is exposed to internet and computers about 4 years ago and only deployed a full installed network within the organization and utilised a network file server recently.	Singapore	Finance	28 employees	Audit Manager [participant 6]

Figure 1: Summary of Case Study Organizations and Participants

The researchers obtained the contact details of staff from their respective organizations. Only those staff that could provide insight into the research question were interviewed. Interviews were a combination of face-to-face (2 interviews), Skype (3 interviews), and interactive email (1 interview where multiple emails to ask and answer interview questions). In each event a record of the interview was taken for subsequent analysis. The interviews ranged between 45 minutes and an hour and were split into two components. Firstly, open ended questions on information security were asked to determine the interviewee's beliefs about security and risks to the organization. Interviewees were subsequently asked to read, assess and comment upon a number of information security risk scenarios. These were used to determine the participants' perceptions of a range of information security risks. The results from the information security risk scenarios allowed a better understanding of the answers given by the interviewees on the initial part of the interview.

Interviews were transcribed and data analysis was conducted using the open, axial and selective coding technique (Neuman 2006). The coding technique was used by the research team to develop themes and

sub-themes from the collected data through the examination of the transcripts by each team member. This gave inter-rater reliability to the themes and sub-themes identified. After this final process, several distinct themes emerged which will be discussed in the following sections.

THE CASE STUDIES

The analysis of the case study data was conducted in two parts. Firstly the open ended questions on information security were analysed to determine the interviewee's beliefs about security and risks to their organization. This analysis resulted in 6 major themes that are summarised in Figure 2. Evidence for each of the themes from the case organizations is also shown in Figure 2 as links to the Appendix for each organization. For instance an "(A.1)" refers to Appendix A, point 1.

Theme	**TechCons** **Appendix A**	**GPSComms** **Appendix B**	**ElectCont** **Appendix C**	**Consult** **Appendix D**	**Audit** **Appendix E**
What is Information Security - as perceived by SMEs	Securing information from unauthorised access: (A.1, A.2)	Securing information exchange between the organization and clients (*B.1*)	Protecting business information from unauthorised access (*C.1*)	Securing organizational information (*D.1*)	
Perceived need for information security	Need is influenced by industry culture. Risk Management process exists. (A.3, A.4, A.5)	Need based on leakage of Knowledge via Social Media (*B.2, B.3*)	Need based on importance of protecting organizational advantage (*C.2*) – however no security implemented (*C.3*)	Need based on being able to uphold the perceptions of trust customers have for the company (*D.2*) – has security – motivated by client observations of flaws (*D.3*)	
Perceived information security concerns (ranked)	1. Company reputation and credibility at stake	1. Company reputation and credibility at stake	1. Company reputation and credibility at stake	1. Company reputation and credibility at stake	1. Information confidentiality issues
	2. Monetary loss	2. Monetary loss	2. Information Integrity at stake	2. Information Integrity at stake	2. Information integrity at stake
	3. Information integrity at stake	3. Information integrity at stake	3. Monetary loss	3. Information confidentiality issue	3. Company reputation and credibility at stake
	4. Information confidentiality issues	4. Information confidentiality issues	4. Information confidentiality issue	4. Information availability	4. Information availability
	5. Information availability	5. Information availability	5. Information availability (*C.4, C.5*)	5. Monetary loss	5. Monetary loss
Previous Information Security Incidents recognised by SMEs	None in past 3 years	Have had incidents in prior 3 years: Minimal impact as contained internally.	None in past 3-5 years. Security Audit every year (*C.6*)	A number of incidents over the past 3-5 years, all considered low impact	None in past 3 years, can't spend enough to stop a deliberate attack (*E.2*)
Perceived trade-off between Information Security and convenience	Security can be an inconvenience, we need to strike a balance (*A.6*)		Security can be a hindrance. It can't affect work flow (*C.7*)		
Perceived influence of cost and resource limitations on security	Happy with current state of information security (*A.7*)	Cost is a huge factor – if cost is low they implement.	Wait and see approach. (*C.8*)	Resource issues in implementing security (*D.4, D.5, D.6*)	Main priority is making money, not spending it on security (*E.1*)

Figure 2:Themes identified from the cases

Across the cases there was a varied opinion as to what constitutes 'Information Security". Some

organizations focus on the information (content) aspects, whereas others focus on the information exchange (IT services) aspects. Subsequently, what they then consider important to invest in with regards to information security changes. None of the studied organizations exhibited any form of formal or informal risk assessment with regards to information security. Additionally, there is a very narrow view of information security needs. The need for security is greatly influenced by the perceptions of their customers or other external parties and this tends to be a trust building or trust sustaining process. The internal information security needs of the organization, in particular when considering "accidental" incidents are virtually ignored. Most of the organizations don't consider internal incidents such as the inadvertent deletion of a file, or the sharing of a password to be critical security incidents, let alone failure to secure a sensitive document.

As the organizations tend to ignore internal information security issues, the reports of low or no security incidents can be misleading. This can be made worse by, as Tan et al. (2003) suggest, many organizations failing to recognise and report security incidents as there are regulatory implications and the negative impact that an incident report can have on trust with their customers. The question for these organizations is whether or not there were information security issues internally that were not considered as incidents because they a) were internal, or b) would impact their reputation.

Even though the organizations were very concerned about their credibility and the trust that their customers had in them, most organizations ranked "company reputation and credibility at stake" high whilst "information confidentiality issues" was ranked in second last place. This is particularly concerning, as there is an obvious link between information confidentiality (i.e. leakage of sensitive information) and trust in the organization.

Many of the organizations identified the impact that security has on the business processes within the organization as a concern. Most of the organizations have a negative perception on information security and efficiency of processes. However, security experts are aware that information security shouldn't adversely impact the organization productivity and profitability as that is one way to guarantee that the security measures will not be effective. An integrated approach, where information security practices are embedded in the organizational processes and a culture of security is grown in the organization is a better approach (Lim et al. 2012).

TechCons suggested that one of the main things in their favour that meant that information security was less important was the size of the organization. They think that because they are an SME then external attackers would be less likely to target them for an attack. However there is significant evidence that SMEs are being targeted and may well benefit from better information security (PWC 2012).

The second phase of analysis focused on the response to the security risk scenarios. In this phase the ranking of scenarios (from most to least important to SMEs) were determined and supporting evidence of the reasoning behind these rankings was identified. Figure 3 shows a summary of information security rankings.

Risk Scenarios	Participants						Average Rank
	1[1]	2	3	4	5	6	
Risk of unauthorised access by insiders	NA	5	3	5	3	2	1
Risk of deliberate act of sabotage	NA	4	6	1	5	4	2
Risk of deliberate act of information extortion	NA	7	2	2	6	3	2
Risk of compromising to intellectual	NA	8	4	6	2	1	4
Risk of an act of human error or failure	NA	2	1	9	7	6	5
Risk of deliberate software attack	NA	3	10	4	4	5	6
Risk of technical software failure or errors	NA	1	9	10	1	7	7
Risk of deliberate act of theft	NA	6	5	3	9	8	8
Risk of internal network error	NA	9	8	7	8	9	9
Risk of forces of nature (fire, flood, earthquake, etc)	NA	10	7	8	10	10	10

[1] Scenarios were brought into the research after the first interview, therefore data is not available

Figure 3: Risk Scenarios Ranking Results

Whilst organizations tended to ignore the inside risks of security breaches in the first part of the interview, when they were shown scenarios of risks they nominated the risk of unauthorised access by insiders as the number 1 risk, which essentially contradicts the behaviour of the organizations towards information security. It also seems that in the organizations studies that their least concerns dealt with the impact of forces of nature (possibly because of the low probability), internal network errors (possibly because of trust in their network) and the risk of deliberate theft.

FINDINGS AND DISCUSSION

From the analysis of the case study data, three main factors were identified that influence decision-maker actions towards information security within SME's. These will be discussed in this section.

Factor 1 - External Influences

The majority of the decision makers in SMEs stated that they are willing to mitigate information risks. Their motivations for doing so are that external parties, such as their clients or potential customers, rate their organization in terms of their trustworthiness, reputation and quality of products. The decision-makers believe that trust is a key factor and that protecting the confidentiality of their client's data is one way to earn trust from clients. Additionally, SMEs recognised the fact that only consistent delivery of quality products to their clients will increase the level of trust shown towards them. Thus, we can observe that SMEs have made a clear connection between information security and trust. "Because our clients place their trust in us when they place their sensitive data in our database, information security is the basis of trust in our industry." [Participant 5]

One reason for SME's concern on the level of trust may be due to its close relation to the reputation of an organization, which is their main concern. The data shows that 5 out of 6 participants were very concerned with the protection of the organization's reputation. As a result, SMEs clearly understood that without proper information security a major security breach might occur, leading to a reduction in their reputation. Subsequently, when reputation is involved SME's are more likely to invest in information security. "…good information security also enhances our reputation in the market as trustworthy partners." [Participant 1]

Further evidence supporting why SMEs are concerned about their reputation originates in the criticality of an organization's image and reputation in the buying decisions of consumers. Nguyen & Leblanc (2001) suggest that image and reputation are crucial in developing and maintaining the loyalty of

customers. Therefore, if an organization is perceived as "untrustworthy", its reputation would be affected.

Additionally, SMEs are strongly influenced by the standards and culture within their industry sector when it comes to implementing information security. "It's dependent on the organization. Some of the SMEs operate based on the knowledge of a few key personnel and therefore the need for information security is not vital, however, for firms like ours [consulting firms] whereby we are dealing with more employees sharing the information, then this need becomes significantly higher" [Participant 2]. If an organization is in a competitive industry and one of their products is the key to most or all of their organization revenue, then it is crucial for them to secure that valuable piece of confidential information about their product to ensure competiveness. SME's in this study often implemented information security as they were aware that other companies in the same industry were doing so. Therefore, industry culture is definitely one of the key motivating factors to SMEs.

Factor 2 - Misperceptions of Information Security

Much literature has mentioned that perceptions play an important role in the identification of information risks in information security. For instance, Gerber (2005) and Bandyopadhyay (1999) state that risk analysis is subjective as it depends on an individual's opinion, mood and feelings. For example, risks that are perceived to have a high probability and impact are given more consideration and attention than those that are less. This probability and impact are usually estimated by the security managers or key decision makers in SMEs rather than based on hard facts (Shedden 2009). Thus wrong perceptions of information security will lead to inaccurate analysis of the information risks facing an organization. Likewise, a misperception of a security incident may result in a series of escalating effects on an organization's decision to take up information security.

Participants in only two of the cases (GPSComms & Consult) admit that they encountered a security incident in the past three years. The SMEs studied only consider an incident as something major that impacts the organization and involves an external party. Statements such as "I consider security incidents are those that involve external parties eg. accidentally sending confidential information out to a client who is not supposed to know it" [Participant 1] were common in the data. However, literature suggests that incidents are more likely to originate from within an organization, and whilst many are malicious, there are those that are accidental also (Siponen & Vance 2010; Johnston & Warkentin 2010). It is possible, that due to the SME's definition of an incident, that some security events may not have been recognised as incidents. This may also be an indicator of a lack of information security expertise to identify an information security event and to then classify it as an incident. Furthermore the SME's studied did not have a formal incident response plan. This however is typical of SMEs (Briney & Prince 2002) and may lead to a failure to recognize security breaches.

Some SMEs thought that the size of their firms is related to the level of exposure. Consequently they claim that risks could be mitigated more easily within a small firm. "We are already mitigating the risk and since we are a small firm, the impact can be mitigated relatively easier" [Participant 1]. Additionally, they perceived that being small firms implied that they were less likely to be attacked. "We may be lucky or hackers are not interested in small enterprises" [Participant 2]. Such information security mentality begins with SMEs having the wrong perceptions of the definition of a security incident (being an external event), and coupled with the thinking that they are small, they felt that they become less of a target to external threats such as hackers. However, literature has shown that not all security incidents are malicious and hacker related (Whitman, 2003). Threats originate internally as well as externally to an organization. SMEs that lack sufficient information security expertise are too focused on external threats, and subsequently many internal threats are overlooked. Although there is some recognition

regarding human errors and disgruntled employees, majority of the SMEs studied still possessed the misperception that most attacks come from external sources.

The SMEs studied have a negative perception concerning information security. The majority felt that no amount of security will be adequate to protect an information asset if the attack was deliberate. Statements such as: "If the attack is deliberate, it is very hard to prevent it, even if you have the best firewall and anti-virus in place" [Participant 3] and "If someone really want to steal information, no amount of security will prevent it from happening" [Participant 6] are common in the data. Additionally, some of the participants could not be bothered to do anything about some of the breaches because of their high frequencies. "We are quite immune [meaning we ignore them] to this type of risks" [Participant 5]. This negative perception is again led by the misperceptions of SMEs about security threats. As SMEs perceive that security incidents are only triggered by external events and they consider that they can't prevent a determined, deliberate attack, they don't see the worth of information security. However, there are numerous other threats that could have been addressed, such as the many internal ones where a program, such as SETA (Security Education, Training, and Awareness), could be useful for reducing the probabilities of the internal threats. However, due to these misperceptions, other ranges of security threats were completely overlooked.

Factor 3 - Conscious decision not to invest in information Security

Whilst SMEs are aware of the importance of information security, they set it as a low priority, focusing on their core business activities, until they have a security incident. Additionally, the measures they have in place are inadequate to deal with a wide range of security threats. Some SMEs have a false sense of security which subsequently affects their information security investment decisions.

Not surprisingly, for the SMEs studied, information security is not ranked as one of their top priorities. They have a restricted budget, a limited set of information security skills and are much more likely to focus on their core business. Once an SME has some initial security in place, they are unlikely to revisit information security management, unless there is a major security incident. "For our situation now whereby we have already something in place, though it may not be adequate, we will not focus too much into this for now" [Participant 1] "We are aware of the potential problems but we don't see a need to address that problem currently" [Participant 4]. Their tendency to not revisit information security until after an incident may be a result of the misperceptions that the SMEs had about security as already discussed.

Another reason given by the SMEs studied for not investing in information security is the perception that some information security implementations will have an impact on the efficiency of business processes. "While information security is important, we strive to achieve a balance between upholding security policies and not causing inconvenience in our field of work" [Participant 2]. Furthermore, as Participant 1 states "As we are a small organization, too many layers of a system may be a hindrance". Participant 4 agrees stating, "Yes, it can be a hindrance if it does not integrate well into our work flow and processes". Whilst good information security design that is incorporated into the business process and works with the various mind sets of employees is possible, many SMEs, especially those with only small employee numbers, don't have the expertise to implement such a security design. SMEs are reluctant to take the risk on developing an integrated information security programme which they are unfamiliar with and where it is not implemented consistently within the SME's industry sector. This is understandable as a poor implementation of information security may lead to a hindrance of business processes as has been explicitly mentioned by the SMEs studied.

The final reason for SMEs not investing in further information security is that they have a false sense of

security in their current information security practices. The SMEs studied were aware of the importance of protecting their data and systems and used backups and standard high level security measures such as installing a virus-scanner. When this was combined with the fact that four of the six organizations hadn't had a recognised incident in the past three years this tended to provide them with a false sense of security towards their information resources. Additionally, on further discussion with the interviewees it was clear that even though they were performing backups that at no time had these backups been restored to test their viability. Subsequently, the reliability of the backup is questionable and gives the wrong impression that their information is secure. Though the SMEs know that their current measures may be inadequate, they seem to be relying on them (backups) for almost everything. "We are insured against such an event and we have backup system to fall back on" [Participant 5]

CONCLUSION

This research makes a contribution to theory in security management by confirming that formal risk assessments tend not to be implemented in SMEs, and by identifying the key factors that influence security expenditure.

The key factors are, firstly, the motivation for SMEs to have information security is not determined by their security needs, but rather by how their clients perceive their level of security, as it relates to trust and reputation of an organization. In addition, the willingness of SMEs to mitigate information risks is dependent on the industry culture their organization is in.

Secondly, a lack of awareness of security risks to organizations, which is primarily due to the absence of security management expertise. As a result, decision-makers tend not to recognize the full range of security risks and focus on specific concerns that are brought to their attention from a variety of different sources. These can be popular media (hacker attacks etc), the industry (their peers, regulators, etc.) or clients.

Thirdly, in the view of the SMEs participating in this field study, the implementation of information security is complicated, costly, will not deliver immediate results and will impact organizational processes. Furthermore, there are other priorities to focus on, such as business productivity and thus information security is not the utmost priority. Further, some SMEs believe that backing up their data is sufficient protection against the majority of risks. This is clearly a dangerous misperception, as many risks such as those that attack services may not be addressed by backups.

Given the above discussion, the factors identified by Dimopoulos et al.(2004) that relate specifically to the adoption of formal risk assessments (i.e. 'restricted budgets', 'lack of expertise' and 'lack of awareness') are confirmed from this field study.

Of concern to organizations should be the disconnect between what the interviewees thought were important security issues in general discussion versus when given specific scenarios to rank. This study shows that participants had a high level, immature and non-systematic perspective on the range and depth of security issues. However when presented with scenarios their rankings showed a higher and more inclusive level of awareness of information security issues. This may be a symptom of a lack of security awareness and education.

This research also makes contributions to the practice of security management. The results of the field study indicate a need for new risk assessment methodologies that are relatively lower cost and require less expertise than those currently available. Further, this study points to the need for security education, training and awareness for decision-makers in SMEs – this is a concern for business

governance bodies.

Though the factors influencing SMEs have already been identified in this paper as trust, reputation and misperception of information security, they are only useful in providing us with insights into the decision making process of SMEs. A comprehensive study of the financial impact of these influences on organizations is needed.

REFERENCES

Alberts, C., & Dorofee, A. (2004). Security incident response: rethinking risk management. In International Congress Series (Vol. 1268, pp. 141-146). Elsevier.

Atkins, M. H. & Lowe, J. F. (1997). Sizing up the small firm: UK and Australian experience. International Small Business Journal, 15(3), 42-55.

Bandyopadhyay, K; Mykytyn, P; Mykytyn, K (1999) "A framework for integrated risk management in information technology", Management Decision, Vol. 37 Iss: 5, pp.437 - 445

De Faria, P. & W. Sofka (2010) Knowledge protection strategies of mutinational firms - a cross-country comparison. Research Policy, 39, 956-968.

den Braber, F., Hogganvik, I., Lund, M. S., Stølen, K., & Vraalsen, F. (2007). Model-based security analysis in seven steps—a guided tour to the CORAS method. BT Technology Journal, 25(1), 101-117.

Briney, A., & Prince, F. (2002). Does Size Matter. Information Security, 5(9), 36-39.

Chang, S. E., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. Industrial Management & Data Systems, 106(3), 345-361.

Dhillon, G. (2007). Principles of Information Systems Security: Text and Cases. Hoboken, NJ, John Wiley & Sons, Inc.

Dimopoulos, V., Furnell, S., Barlow, I. and Lines, B. (2004), “Factors affecting the adoption of IT risk analysis” in Proceedings of 3rd European Conference on Information Warfare and Security, Royal Holloway, University of London, UK, 28-29 June 2004.

Frosdick, S. (1997). ‘The techniques of risk analysis are insufficient in themselves’, Disaster Prevention and Management: An International Journal, vol.6, no.3, pp.165-177.

Gerber, M. and von Solms, R (2005). "Management of risk in the information age", Computers & Security 24(1): 16-30, http://dx.doi.org/10.1016/j.cose.2004.11.002.

ISO/IEC 27005 (2008) ISO/IEC 27005:2008 Information technology -- Security techniques -- Information security risk management. International Organization for Standardization (ISO) and International Electrotechnical Commission.

ISO/IEC 27002 (2005) ISO/IEC 27002:2005, Information technology - Security techniques - Code of practice for information security management. International Organization for Standardization (ISO) and International Electrotechnical Commission.

Johnston, A.C. & Warkentin, M., 2010. Fear Appeals and Information Security Behaviors: An Empirical Study. Management Information Systems Quarterly, 34(3), pp.549–566. Available at: http://aisel.aisnet.org/misq/vol34/iss3/10/ [Accessed June 23, 2011].

Lim, Joo Soon; Chang, Shanton; Ahmad, Atif; Maynard, Sean (2012) "Towards A Cultural Framework for Information Security Practices". In (Eds.) M. Gupta, J. Walp and R. Sharman, "Strategic and Practical Approaches for Information Security Governance: Technologies and Applied Solutions". IGI Global.

NIST. (2009). "Recommended Security Controls for Federal Information Systems and Organizations." from http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final-errata.pdf.

Neuman, W.L., 2006. Social Research Methods: Qualitative and Quantitative Approaches 6th ., Boston: Allyn and Bacon.

Nguyen, N. & Leblanc, G. (2001), "Corporate image and corporate reputation in customers' retention decisions in services", Journal of Retailing and Consumer Services, Vol. 8, pp. 227-36

Norman, P. M. 2001. "Are your sectrets safe? Knowledge protection in Strategic Alliances," Business Horizons (Nov-Dec), pp 51-60.

Peltier, T. R. (2001). Information Security Risk Analysis. Boca Raton, Auerbach.

PWC (2012) Information Security Breaches Survey: Technical Report, Price Waterhouse Coopers, April 2012, http://www.pwc.co.uk/en_UK/uk/assets/pdf/olpapp/uk-information-security-breaches-survey-technical-report.pdf Accessed Feb 5 2013.

Ransbotham, S., Mitra, S. & Ramsey, J., 2012. Are Markets For Vulnerabilities Effective? Management Information Systems Quarterly, 36(1), pp.43–64.

Siponen, M. & Vance, A.O., 2010. Neutralization: New Insights into the Problem of Employee Systems Security Policy Violations. Management Information Systems Quarterly, 34(3), pp.487–502. Available at: http://aisel.aisnet.org/misq/vol34/iss3/7/ [Accessed June 23, 2011].

Shedden, P., Ruighaver, A.B., Ahmad, A., (2006) Risk Management Standards - The Perception of Ease of Use. 5th Security Conference, April 19-20 2006 Las Vegas, USA.

Shedden, P, Scheepers, R., Smith, M., Ahmad, A. (2009) Towards a Knowledge Perspective in Information Security Risk Assessments – an Illustrative Case Study, Proceedings of the 20th Australasian Conference on Information Systems (pp. 74-84), Melbourne, Australia: Monash University. 2009.

Spinellis, D., Kokolakis, S., & Gritzalis, S. (1999). Security requirements, risks and recommendations for small enterprise and home-office environments. Information Management & Computer Security, 7(3), 121-128.

Sveen, F. O., Torres, J. M., & Sarriegi, J. M. (2009). Blind information security strategy. International Journal of Critical Infrastructure Protection, 2(3), 95-109

Tan, T., Ruighaver, A.B., Ahmad, A., Incident Handling: Where the Need for Planning is often not Recognised, Proceedings of the 1st Australian Computer Network, Information & Forensics Conference, Perth, Nov 24, 2003

Whitman, M.E., 2003. Enemy at the gate: threats to information security. Communications of the ACM, 46(8), 91-95.

Whitman, M.E. and Mattord, H.J. (2011). Principles of Information Security, 4th ed. Centage Learning, Boston, MA, USA.

Yazar, Z. (2002). A qualitative risk analysis and management tool - CRAMM, SANS Institute.

APPENDIX A

1. I believe you are referring to both the securing the information within the organization from unauthorized external access as well as securing the information from internal theft (intellectual property) [Participant 1]
2. It is the need to protect our information systems/intellectual property in the form of internally circulated information, client data as well as our IT products that include software source codes from leak/unauthorized access, use, modification or disclosure [Participant 2]
3. It is dependent on the organization. Some of the SMEs execute based on the knowledge of a few key personnel and therefore the need for information security is not as vital. However, for firms like ours (Consulting Firm), whereby we are dealing with more employees sharing the information, then this need becomes significantly higher. [Participant 1]
4. This is a common practice within our industry so it is something that we learn from our previous firms [Participant 1]
5. Yes, because as with any other running business, security of own information is equivalent to protecting ourselves against competition that may benefit by taking advantages of poor security on our part to protect our own information properly. Good information security also enhances our reputation in the market as trustworthy partners. [Participant 2]
6. We are willing. However as mentioned earlier, we hope to strike a balance between information security and inconvenience to our field of work [Participant 2]
7. For our situation now whereby we have already something in place, though it may be inadequate, we will not focus too much into this for now – meaning we will not spend more. [Participant 1]
8. We are already mitigating the risk and since we are a small firm, the impact can be mitigated relatively easier. [Participant 1]
9. We may be lucky or hackers are not interested in small enterprises. [Participant 2]

APPENDIX B

1. Information security in an organization refers to the security of the data information between the vendors, customer and us through emails and any forms of digital media. [Participant 3]
2. Especially with social media such as Facebook, foursquare and IM chats like Window Massager live, Google voice and Skype. Information such as new product launch or new design can be posted on the web prior to the launch and cause competitors to come out with similar design to market it first. Trojan or Malware can be easily spread via Window message or email if staffs are not aware of what he/she is receiving. This could cripple the staff computer and in turn reduce the effective and manpower need to fix the computer and the important data that is loss. [Participant 3]
3. It was due to a leak of information from another company on social media network that drive us to have information security. [Participant 3]
4. Security incidents will affect the company profit and leaking of company projects with vendors/customer that we had sign NDAs with. [Participant 3]
5. We are willing to improve on information security if it is low cost and affordable by our organization. [Participant 3]

APPENDIX C

1. “Hmm, According to my understanding, I believe it is to protect information relating to the company’s business from non-authorized personnel and within the company’s boundaries” [Participant 4]
2. “It is crucial in a very competitive industry. If what separates you from your competitors is the superiority of your product. You will need to safeguard all confidential information relating to the

technology of your product and all other trade secrets. So it really depended on what industry you are in." [Participant 4]

3. "Yes of course we would want. I believe every organization including us have the need to protect our company's information and resources from outsiders" [Participant 4]
4. "I will say the confidential information and company archives are of the most concern to us" [Participant 4]
5. "Business Continuity. Any disruption to the company's activities will result in a loss of productivity" [Participant 4]
6. "We define a security incident if it has a big impact on our operations or the incident is being done deliberately with the intention of bringing harm to the company. We also do see sending confidential documents to the wrong colleague as being a security incident. This is more so if the document is being sent to outsiders. However we have not come across such cases yet." [Participant 4]
7. "Yes it can be a hindrance if it does not integrate well into our work flow and processes. For example, what can be achieved in 1 or 2 steps needs to go through a couple more steps? However since we have not implemented any form of higher information security as yet, we will make sure that once it is implemented, it will not affect much of our efficiency and productivity." [Participant 4]
8. "Information security is definitely on our radar screen but the implementation will be a wait and see approach … We are willing to have it in place however we need to make sure we can set aside some budget put in place the manpower and infrastructure to look into it … We are aware of the potential problems but we don't see it as a need to address that problem currently. We have assessed the possible threats and none of them we have identified to be high risk" [Participant 4]

APPENDIX D

1. "To me, information security is to secure my clients' data and securing the web tool. We also need to employ encryption as well as SSL to protect sensitive clients data in the database. On top of that, we will also encourage clients to change their password regularly and use stronger passwords. The database will also be purged of client data when they terminate our service" [Participant 5]
2. "Of course, I think it is vital to the success of an SME organization. Because our clients place their trust in us when they place their sensitive data in our database, information security is the basis of trust in our industry" [Participant 5]
3. "We once had feedback from a potential client that they are concern about the information security of our system and they pointed out to us that some of the major issues that they had with our systems. From this incident, this prompted us to conduct a security risk assessment of our system." [Participant 5]
4. "We have identify the security loopholes in our system but the lack of resources is holding us back from implementing the counter measure" [Participant 5]
5. "I hope we will have an information security program within the next 2 years if the resources permits" [Participant 5]
6. "We perform it yearly; we based it on the security related customer support cases that we received. This might not be frequent enough even though we do have security breaches but due to the size of our organization, we do not have the time and resources to commit" [Participant 5]

APPENDIX E

1. "Information Security is important but our priorities go to functionality to make money" [Participant 6]

2. “As experience before, information was leaked through the staff’s unethical approach. If someone really wants to steal information, no amount of security will prevent it from happening” [Participant 6]