Towards a Framework for Strategic Security Context in Information Security Governance

Sean B Maynard
University of Melbourne
sean.maynard@unimelb.edu.au

Terrence Tan
University of Melbourne
t.e.tan80@gmail.com

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

Tobias Ruighaver
University of Melbourne
tobias@ruighaver.net

Abstract

Information security governance influences the quality of strategic decision-making to ensure that investments in security are effective. Security governance involves a range of activities including adjusting organisational structures, designating roles and responsibilities, allocating resources, managing risks, measuring results, and gauging the adequacy of audits and reviews. We identified three security issues in an organisation around strategic context in an in-depth and revelatory case study. These are (1) limited diversity in decision-making; (2) lack of guidance in corporate-level mission statements to security decision-makers; (3) a bottom-up approach to security strategic context development. We further argue that instead of an approach that is based on risk and controls, organisations should address objectives and strategies through developing depth in their security strategic context.

Keywords: Security Culture, Decentralized Decision Making, Security Strategic Context, Business Security Strategies, Information Security Governance.

Citation: Maynard, S. B., Tan, T., Ahmad, A., and Ruighaver, T. (2018). " Towards a Framework for Strategic Security Context in Information Security Governance, " *Pacific Asia Journal of the Association for Information Systems, 10*(4), pp. 65-88.
ISSN 1943-7536(print) / ISSN 1943-7544(online)

DOI: 10.17705/1PAIS.10403

Introduction

Organisational expenditure on IT security solutions is estimated to reach an unprecedented $96 billion US dollars by 2018 (Gartner 2017). However, they still struggle to develop strategies to address increasingly complex security risks such as leakage through Online Social Networking (Abdul Molok et al. 2010; Chong and Tan 2012; Gao et al. 2018; Poggi and Tomaiuolo 2018) and intellectual property theft (Dreibelbis et al. 2018; Shedden et al. 2016). This despite many such organisations drawing their guidance from best-practice security standards such as the ISO 27000 series (Park et al. 2012).

While the ISO 27000 standards introduce a lifecycle model for security management, the emphasis is still on the controls needed in information security. Little information is given about security objectives, potential implementation strategies for these objectives or about the key aspect of accountability arrangements (Siponen and Willison 2009). Also, other than risk assessment, there are few suggestions on how organisations should develop security objectives and strategies as part of their security governance processes (Webb et al. 2014) and develop an incident response and forensic readiness capability (Elyas et al. 2015; Elyas et al. 2014). While this emphasis on controls works well in a reasonably static security environment, in today's dynamic security environment, organisations need to encourage and promote innovation in their approach to security management, moving beyond what is prescribed in the current standards (Shedden et al. 2016).

Love et al. (2010) suggests that corporate security governance "consists of leadership, organisational structure, and processes. Management leadership should be proactive in ensuring that the activities of information security are supported and understood at all organisational levels and aligned with organisational objectives". Understanding how certain characteristics of security governance, at the enterprise level and below, influence the quality of strategic decision-making in information security is an essential step to ensuring that investments in security are used effectively. The ability to make well-informed decisions about the many important components of governing for enterprise security, such as adjusting organisational structures, designating roles and responsibilities, allocating resources, managing risks, measuring results, and gauging the adequacy of security audits and reviews is crucial (De Bruin and Von Solms 2016; Mishra 2015; Veiga and Eloff 2007). Efforts to improve decision making in these areas is mostly focussed on corporate security governance (Carcary et al. 2016).

Unfortunately, this emphasis fails to effectively address the need to ensure that decision making at the lower levels of the enterprise is improved, i.e. the need to establish security governance at the business unit level and below. From this point forward, we will refer to this level of governance as "enterprise-wide security governance", or just "security governance". Further, we will use "corporate security governance" when discussing issues related to board level governance issues. We contend that while there is evidence of reasonable efforts to develop corporate security governance guidelines and frameworks, there is little known about enterprise-wide security governance. In particular, further research is required to study (1) how organisations develop their security strategic context, (2) how they decide on security objectives and strategies, (3) how they use these to develop their policies and security infrastructures, and (4) the role of accountability in ensuring a streamlined and effective process. Therefore, this paper addresses the following research question:

How does information security governance influence the depth of strategic context in enterprise information security?

This paper reports on an in-depth and revelatory case study of an IT service organisation. This case was conducted as part of a larger multiple-case study examining the area of enterprise-wide security governance. Cases were selected on the basis that they were actively

https://aisel.aisnet.org/pajais/vol10/iss4/4
DOI: 10.17705/1pais.10403

undertaking security efforts, were relatively stable, were large enough so that governance was an issue, and had high reliance on their information systems. This particular case examines the information security function in a business unit of a privately owned, Small-to-Medium Enterprise (SME), with security governance decentralized to the IT group. This paper will discuss several of the major issues related to 'enterprise wide security governance' that we identified as well as how these issues affect the security strategic context for the organisation.

Background

Modern organisations are facing an increasingly complex threat environment due to recent emergence of purposive and sophisticated attacks (e.g. Advanced Persistent Threat (APT) and ransomware) (see Verizon's 2018 Data Breach Investigations Report (Lemay et al. 2018; Verizon 2018). This is despite information security professionals being aware of, and engaged in, defending against these complex attacks. We argue that a that a key reason for this consistent trend in incidents is a narrow focus on IT operations and relatively less focus on strategic-level security management activities – a result of compliance culture that focuses on standardized sets of security controls (Dhillon et al. 2018; Maynard et al. 2018; Tan et al. 2010).

Governance

For organisations operating in complex and highly dynamic environments, the importance of effective governance (how decisions are made) and management (what decisions are made) cannot be understated (Chong and Tan 2012; Peppard 2007). The traditional view of corporate governance sees the responsibility falling to the board and senior executives, with the focus being on the financial well-being of the organisation (Shleifer et al. 2000). However, this is not sustainable due to the highly dynamic business environment. Organisations must devolve governance activities down to all levels of the organisation, and even to outside entities (Pultorak 2005; Weill and Ross 2004). From a security perspective, this means that responsibilities for governance fall to all employees of the organisation, and to external stakeholders such as auditors (Bergeron et al. 2015; Pultorak 2005). This devolves responsibility to the lower levels of the organisation as well as to the senior executives.

However, having responsibility and feeling responsible are two different issues. With responsibility comes accountability. Therefore, an important aspect of any effective governance is how the organisation handles accountability for decisions in security management (Borck 2000). A lack of even the simplest accountability processes is a common deficiency in security governance. For example, simple feedback loops in which decisions on security are discussed with higher levels of management, and the focus is on how the decisions are made (Burke 2005; Goodman et al. 2016).

Importantly, the delegation of responsibility to those at the lower levels does not preclude the need for executive level management support. Knapp et al. (2006) found that top management support for information security is a significant predictor of the direction and success of an organisation's information security. Therefore, whereas operational responsibility and accountability primarily lies with those at the middle management and lower levels, top/executive management still has clear responsibility to visibly demonstrate their support and a high prioritization of information security.

Security governance should be viewed as a larger management issue that revolves around understanding how decisions are made and making consistently good decisions in a complex and dynamic environment characterized by distributed decision making (Koh et al. 2005; Ribbers et al. 2002). Decision makers should be given the right information and the right guidance to be able to make quick, decisive and accurate decisions in real time (Dhillon and Torkzadeh 2006).

Summary

From this discussion it is clear that current security practice and compliance with standards is not enough to protect organisations. Much research has been completed in the information security domain in areas such as policy (Alshaikh et al. 2015; Goodman et al. 2016; Ifinedo 2014; Malandrin and de Brito Carvalho 2013; Maynard et al. 2011; Maynard and Ruighaver 2006; Rahimian et al. 2016; Ruighaver et al. 2010; Safa et al. 2015; Sommestad et al. 2014), risk management (Malandrin and de Brito Carvalho 2013; Rahimian et al. 2016; Webb et al. 2014; Webb et al. 2016) security culture (da Veiga and Martins 2015; Karyda 2017; Lim et al. 2010; Okere et al. 2012; Ruighaver et al. 2007), incident response and forensic readiness (Ahmad 2002; Ahmad et al. 2015; Elyas et al. 2015; Elyas et al. 2014; He and Johnson 2017; Shedden et al. 2010; Tsakalidis and Vergidis 2017) and security education (Ahmad and Maynard 2014; Chen et al. 2013; Rezgui and Marks 2008). Additionally, research has been conducted into the regulatory aspects of information security (Appari and Johnson 2010; Carrapico and Farrand 2017; Masrom and Rahimly 2015).Despite this rich body of research, organisations are still suffering from incidents.

As Tan et al. (2010) argues, the practice of information security has become subject to a compliance culture such that the focus is on ensuring the existence of controls recommended by best-practice standards (and industry expectations) rather than measuring their effectiveness in addressing security risks. In the remaining part of the paper we focus on developing the construct of 'strategic security context' as a means of improving information security governance in organisations.

Method

This empirical research has taken an exploratory case study approach using multiple sources of data in a structured manner (Miles and Huberman 1994). A case study approach enables examination of contemporary phenomena within real-life contexts, especially when the boundaries between phenomenon and context are not evident and multiple sources of evidence are required (Miles and Huberman 1994; Yin 2018). Through multiple site visits, the researchers actively explored, observed, verified, discussed and extracted more information (where appropriate), to refine the case. In this way, the information and data gathered provided this research with great depth.

As our case site, we selected MicroComps Limited (MCL), a market leader in supply chain management and business-to-business e-Commerce solutions (see The Case Study for a description of the organisation). We chose MCL for the following reasons: 1) it is information security intensive by the way of the effort involved in securing organisational assets; 2) it employs a variety of different types of professional information workers; and 3) it relies heavily on the functionality, reliability, stability and operability of their information systems.

Following the footsteps of Straub and Welke (1998) who were able to obtain rather detailed information from their two-firm comparative study, this research attributes its success to the well-developed relationship between the researchers and the participants at MCL. The use of signed non-disclosure agreements to protect the identity of participants and MCL and the commitment to give MCL the opportunity to read, discuss and approve written results before submission to academic outlets were useful to allay any fears and allowed the researchers to gain the confidence of the participants and MCL as a whole.

In conducting the case study, we identified that only three personnel within MCL had anything to do with the information security of the organisation: the IT Manager (*ITMngr*), the Systems Administrator (*SysMngr*) and the Network Administrator (*NetMngr*). We were able to interview and observe each of these personnel as part of the case study. As well as the time spent in interviewing participants, we were able to spend one week in the organisation interacting with the participants in their

https://aisel.aisnet.org/pajais/vol10/iss4/4
DOI: 10.17705/1pais.10403

work life. Subsequently, we were able to build a rapport and were able to observe the workplace. This resulted in the participants relaxing around us and giving accounts of explicit and tacit working and social habits.

We used semi-structured interviews, observations and a self-completed survey framework (participants were given the Security Strategic Context Framework and asked to comment) to collect data on the organisation. Our involvement in observing the organisation facilitated follow-up questions, passing back transcripts of interviews to participants for verification, and their active participation in completing a Security Strategic Context Framework for MCL. This served to provide the depth necessary for a successful study. However, since the study dealt with highly sensitive issues dealing with security, MCL was naturally hesitant in releasing formal documentation/policies and were only willing to give the researchers limited access to these within the organisation.

The interview protocol contained three main sections of questions: background information, characterisation of the firm and strategies, and security and corporate governance. A combination of closed questions (to collect facts) and open-ended questions (to explore concepts) were used during the interviews. This provided a rich picture of in-situ professional decision making. This approach provided participants with a greater opportunity to describe the realities of their situation and was further supplemented with field notes taken during the visits to the company and observation of the participants' interactions with each other.

Information collected during the interviews was digitally recorded (with permission) with notes also taken. Immediately following the interviews, notes were transcribed to capture the nature and tone of the interview as accurately as possible. The digital recording was transcribed within a 24-hour period following the interview. Once the data collected had been transcribed, participants were given the opportunity to review the transcribed interview scripts for accuracy and completeness. Revisiting the interviewees on multiple occasions was also necessary with follow-up questions and to extract more information in an attempt to further clarify points that a participant may have made during the initial interview and/or to ask further questions that the researcher may not have thought of initially during the interview.

Observation is an effective way of gathering data by watching behaviour, events or noting physical characteristics in their natural setting (Jorgensen 2015). In this study, overt, direct observation as a data collection strategy was employed. Direct observation was used as it allowed this researcher to watch interactions, processes and behaviours as they occur in situ (Waxer 1985). Through employing this technique, the researchers were able to observe the security environment in MCL. Overall, the data collection was undertaken over a two-month period. The observations made within MCL proved enlightening and in several instances allowed for corroboration of the responses from interviews.

The analysis was conducted in line with Miles and Huberman (1994) strategy of: data reduction, data display and the drawing and verification of conclusions. Interviews were coded using open coding with following codes developed from the literature: security strategic context, decision-making rights, accountability infrastructures, input rights, and experience and culture. Subsequently, detailed codes for each data source were developed to describe how the participant was involved in security decision making, in strategy development and with other stakeholders. This approach was used to sharpen, sort, focus (at the same time discard) and analyse data so that final conclusions can be drawn and verified (Tesch 2013). Once the open coding was completed, axial coding was used to further analyse the data using codes developed from the governance and strategic context frameworks at a lower level of abstraction. At this stage, data were tabulated to show the interactions of governance activities, its impact on decision making and its impacts on the development of security strategies.

Data display then encompasses further organising and compressing of the information into an assembly that permits conclusion drawing and action (Miles and Huberman 1994). Once organised, the data were then structured into a matrix displaying the complex links among the five constructs of security governance. In this third stream of analysis we aimed to uncover the real meaning behind the information gathered, taking note of similarities, irregularities and any inconsistent patterns (Miles and Huberman 1994). After the analysis process was complete, it was possible to illustrate the research themes and identify which governance practices were relevant and influential to participants at the various stages of the decision-making process.

Enterprise-wide Security Governance

For this case study, it is important to make a clear distinction between corporate security governance and enterprise-wide security governance as introduced in this paper. From the previous section, it can be appreciated that corporate security governance can be understood as governance at a board or executive level (Brown and Nasuti 2005) with its main aims to ensure that security governance is promoted and controlled enterprise-wide. Its focus is ensuring controls and reducing or avoiding risks. Enterprise-wide security governance as discussed in this paper refers to the controls, arrangements, processes or structures that are exercised over the organisation's security. Specifically, these controls, arrangements, processes and structures are focused on improving decision making through providing decision makers at all levels with the right information and the right guidance, at the right time, to make good decisions about security (deMaine 2016).

The field of Information Security is a complex and critical component to an organisation's success. A strategic approach to Information Security aims to transform the IT security function from a set of ad-hoc activities with an emphasis on technology, to a coordinated approach of principles, behaviours, and adaptive solutions that map to business requirements (Whitman and Mattord 2017). As such, those responsible are not just senior management but also middle management and others involved with the implementation of security strategies. As the practices and methodologies behind Corporate Governance and IT Governance are somewhat reliable and time tested and seen to be successful in dealing with various organisational issues, it is plausible to suggest that improving Security Governance throughout the enterprise may be the key to improving the level of security in organisations.

Frameworks

The focus of this study is to improve information security decision-making through enterprise-wide security governance. The execution of security strategies and timely decisions around these strategies occurs at the operations level of the organisation. Subsequently this study is interested in how people that implement security perform decision making, with or without organisational guidance. Tan and Ruighaver (2005b) and (Chong and Tan 2012) point out however, that for decision makers to make quality decisions, guidance must be effectively communicated to them in the form of the organisation's *security strategic context*, which is contained within artefacts such as security objectives, strategies, tactics and mission statements.

These artefacts are crucial as they outline for decision makers the intent or motivation behind what the organisation is trying to achieve with security and the desired end state. For instance, soldiers in battle, given a mission, need to understand their commander's intent. In the military context, the commander's intent is understood as *'a concise expression of the purpose of the operation and the desired end state that serves as the initial impetus for the planning process'* (Shattuck 2000). With this understanding soldiers can be proactive, innovative, flexible and aggressive in their decisions to achieve

https://aisel.aisnet.org/pajais/vol10/iss4/4
DOI: 10.17705/1pais.10403

mission success. With these artefacts effectively developed, it is then vital that they be communicated enterprise-wide, as far down to even the lowest levels. Consequently, this will encourage and allow better, more concise and effective decisions to be made.

Trying to quantify what a good security strategic context is and how one can improve it is a complex problem that cannot be adequately answered in a single study. Importantly, however, Peterson et al. (2000) and Ribbers et al. (2002) argue that good security strategic context *"requires active participation and a shared understanding among stakeholders if they are to coordinate activities and adapt to changing circumstances"*. By developing security strategic context exclusively at the top management level, it is likely to result in a lack of diversity. Hence, good security strategic context needs to be developed by different people/committees at different levels of the organisation, similar to the development of IT strategic context (Weill and Woodham 2002).

In this case study we specifically focus on a key aspect of security governance, strategic context (see Tan and Ruighaver (2004). Notably, strategic context is identified as a key component of successful IT governance (Broadbent 2002; Broadbent and Weill 1997; Weill and Ross 2004). We adopt and expand upon the strategic context model of Broadbent (2002) and subsequently Weill and Ross (2004) to look at both the depth and coverage of the security strategic context. We chose this model as it is the most utilised governance framework to our knowledge with a strategic context component. Depth focuses on the extensiveness of the organisation's strategic context and encompasses 5 domains (adapted from Broadbent and Weill (1997) and Weill and Ross (2004): Security Objectives (mission statements), Security infrastructure, Security architecture, Security application needs, and Security investment and prioritization. Coverage focuses on the comprehensiveness of the organisational strategic context and includes the security areas defined by (Tan and Ruighaver 2005a): Network Security, Systems and Data Security, Physical Security, Personnel Security, Operations Security, and Miscellaneous Security aspects (Eg. a focus on eCrime, and incident handling).

A matrix of the depth and coverage dimensions helps to determine the strategic context in which an organisation is operating in. In the analysis of the case data we use this matrix to assess the scope of the organisation's security strategic context (see Appendix 1 for the analysis).

The Case Study

This case study reports on an Australian organisation: MicroComps Limited (MCL). MCL is a commercially successful organisation who are market leaders in supply chain management and business-to-business e-Commerce solutions. Privately owned, the management structure within MCL consists of a management group that reports to a private ownership board (see Figure 1).

This board has the final say on the operations of the organisation. In the early days of operating, the management group consisted wholly of the ownership board, with the CEO of the organisation being the primary owner. Over time, and as the organisation grew, it became necessary to set up a management committee that answers to the board. At this time, the ownership board of MCL took on a supervisory role. The CEO, the CFO and senior leadership from each department within the organisation together comprise the management committee.

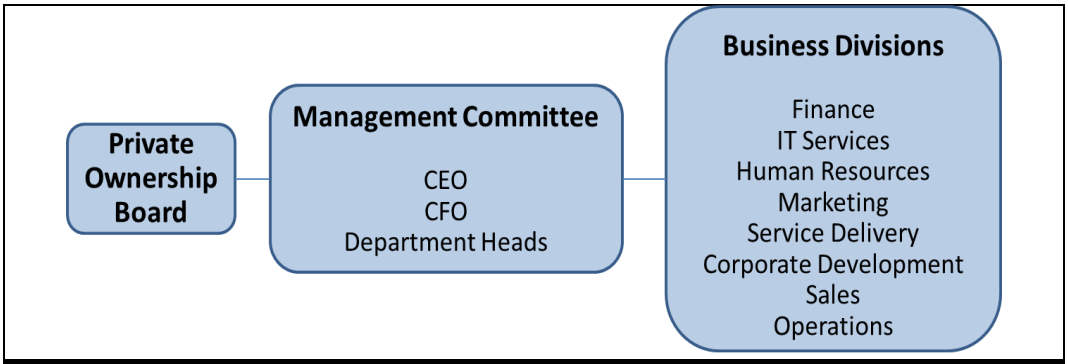

Figure 1: MCL's Organisational Structure

Department heads report to the ownership board through the CEO and CFO. With regards to the day-to-day operations of the business, the ownership board has a hands-off approach. However, the board still maintains and is actively involved with influencing the strategic direction of the organisation. From a governance perspective, the decision-making structures at MCL delegates decision making to the division level, allowing each head to formulate and develop their own strategy, as long as it is within the organisation's strategic context (strategic plan). Thus, the responsibility for all security in the organisation falls to the IT Manager, who is responsible for the security governance in the organisation.

Dealing largely with the transaction, processing and ordering systems of other businesses, MCL's role is to receive files (such as orders and payments), translate them into an understandable, common language, then deliver the order (as many businesses operate their own backend systems and generally not one backend system can talk with every other backend system). A simple way of thinking about this process is to visualise what is involved, think the Postal system: receiving, sorting (translating), storage and delivery.

The participants targeted in this case were specifically selected due to their likely involvement in the development of security strategies, decision making and in providing input to security decisions. As MCL is a SME, the three selected participants were the only personnel within MCL that have security responsibilities. The participants were the IT Manager (*ITMngr*), the Systems Administrator (*SysMngr*) and the Network Administrator (*NetMngr*). The participants experience in the IT field ranges from 5 years (*NetMngr*) to 13 years (*ITMngr*). These personnel were intimately involved with the implementation of security controls and highly relied upon to make decisions about security and to react to security incidents. Of the three, one respondent held the most senior position in the IT and information security area while the others reported directly to them. In addition to gaining data form the participants the researchers sought documents (such as policies, security strategy etc) and were able to observe members of the organisation across a one-week period with respect to security. The main reason for this was to triangulate data for the research.

From a security perspective, none of the participants had any exposure or formal training on security standards because security had never been something pushed strongly by the organisation. Therefore, inconsistencies are evident from the participants' views on the importance of security to the operations of MCL, with some participants stating that security was not important apart from being able to cover vulnerabilities, whilst others stated that security was extremely important to the ongoing running of the organisation. In MCL security was set up and managed by *ITMngr* and *SysMngr* and has a technical focus.

Overall, *ITMngr*'s responsibilities are to provide a functional and robust infrastructure, equipment and framework for the organisation to enable employees to do their jobs and to allow customers to receive their services. *ITMngr*, like the rest

https://aisel.aisnet.org/pajais/vol10/iss4/4
DOI: 10.17705/1pais.10403

of the organisation is incredibly customer focused, and only on very few occasions (and when probed) did he discuss the importance of security and threats to his organisations, rather talking about the importance of the customer. Security initiatives at MCL have been 'organically' grown and ad hoc. Without formal standards or guidance from the organisation on how and what to do about security, *ITMngr* had to formulate his own strategies and his objectives (security strategic context), based largely on the wider objectives of availability and reliability of systems given to him by the organisation.

ITMngr acknowledges that security to him (and the organisation) is not so much a priority but a necessity and that his approach to security in many ways is reactive. He addresses security through the implementation of technical controls and adjusts these in response to security threats and incidents.

NetMngr, is new to the job and has had security delegated to him by *ITMngr*. Having only just joined the organisation, *NetMngr* is representative of the problem that could arise from the organisation's lack of corporate governance and focus on security. The consequence of a lack of organisational guidance on security on the participants is clearly demonstrated in *NetMngr*. Not only does he have little experience with security, he does little regarding security and views security to be less important compared to other business functions. Similarly, he is unaware of what goes on concerning security in general at MCL. Without formal standards, guidelines, documents, mandates or guidance from the corporate governance to inform *NetMngr* of his responsibilities relating to security, like *ITMngr*, he is left to his own devices.

Fortunately for *NetMngr*, although the organisation has not provided much, if any, formal guidance, *NetMngr* receives sufficient on-the-job guidance from *ITMngr*, within the team. This ad hoc training, is analogous with someone working as an apprentice through a hands-on, learn from experience, on-the-job mentoring process. *NetMngr* looks after the local network. Accordingly, he monitors the network performance and services, making sure that everything is working as it should and that all resources are running at optimum levels.

MCL has its data centre and all its data, servers and backups outsourced and located off-site. Responsibility for that data centre and all external business centres lies with *SysMngr*. Coming from a strong technical background and with previous experience in technological support, administrative roles and limited security, *SysMngr* possesses a great deal of technical knowledge. Like the other participants, *SysMngr* too does not receive much, if any, formal guidance from the organisation on what to do, what to secure or how to prioritise security. Like *NetMngr*, *SysMngr* gets direction from *ITMngr*, supplemented by his past experiences.

However, relying on past experiences as a guide for future actions and decisions can also be dangerous. In the first place, most people do not recognise the underlying reasons for their mistakes or failures. In the second place, the lessons of experience may be inapplicable to the new problems. This is where effective security governance to understand how decisions are made and to improve decision making is very important. Good decisions must be evaluated against future events, while experience belongs to the past (Harold and Heinz 2008) .

Case Analysis and Discussion

As stated earlier, the analysis of the case data produced a matrix to assess the scope of the organisation's security strategic context (see Appendix 1 for the analysis). From the analysis three main themes were identified. These are discussed in this section.

Diversity in Decision Making is Limited

At MCL, security does not follow any single security standard, rather security initiatives were improvised and ad hoc, and almost all decisions about the security strategic context are made by the IT Manager. Little or no formal guidance on decision-making rights have ever been explicitly expressed or delegated by the organisation. According to participants, the organisation is not concerned about what decisions are made, nor about how participants went about their jobs, as long as they achieved the availability and reliability of systems and networks. Whilst *SysMngr* and *NetMngr* had unwritten guidelines around security there were no formal policies provided. *"We [referring to Mr Sys and Mr Net] have unwritten guidelines that we work by with security…there is no overarching policy or paper that connects them all together" (ITMngr).*

At MCL, security governance is mostly delegated to the IT group by default. Almost all decisions and input into decisions, from almost every level of security strategic context is developed and decided by the IT Manager with input coming from his team. *"Yes, I have inputs to security - I have meetings with Mr IT and we discuss things" (SysMngr).* Unfortunately, inputs are only from his team, thus creating an environment of limited social participation and limited diversity in decision-making. *"They'll tell me what they want to do and the outcomes they expect, and we'll talk about it" (ITMngr).*

These settings then create the situation where participants rely heavily on their own ingenuity, particularly that of the IT Manager to drive security initiatives and to develop security strategies. Interestingly, all these actions and initiatives are undertaken without the knowledge and understanding that they are actually developing security strategic context. Unfortunately, with the lack of formal guidance from executive levels and from other functional areas, any discussions, dialogues or consultations, including feedback loops, are internalised within the IT department. The input given and received is very insular within the IT department and is limited to the experiences of the team members (mainly in systems and networks) and does not adequately cover the wider range of security concerns and imperatives. For instance, from our case observations, areas such as physical and environmental security and personnel security are lacking in strategies and attention.

Depth in the technological aspects of security (in network security, systems security and data security) is excellent. This has been the main focus of security in the organisation: "*…it's maintaining the availability and reliability of the system. I'll do it through setting up digital certificates, network security, encryption and so on" (SysMngr).* All levels of depth in the security strategic context matrix (see appendix 1) are adequately addressed. This implies that participants at MCL would have good diversity in decision making for these specific areas. Our analysis of MCL's security strategic context identifies that the objectives, strategies and certain controls developed, employed and actioned at MCL, differ from those recommended by security standards such as the ISO 27002 standard. Whereas the ISO 27002 Standard recommends strategies such as:

- Control access to critical data and/or servers to ensure availability and reliability
- Monitor access to directories
- Real time protection
- Up-to-date anti-virus software

MCL has customized these recommendations and developed strategies such as:

- Maintain a flexible approach to security. Adjust and move in response to things
- Automatically delete all .exe files on mail server
- Alerts to be sent when any inconsistencies are noticed

https://aisel.aisnet.org/pajais/vol10/iss4/4
DOI: 10.17705/1pais.10403

- Maintain tight and dedicated roles for every server, machine and process so that redundancy can be achieved (double up on everything)
- Training and mentoring.

Although performed on an ad hoc basis and not through any formal instruction or direction, these strategies are specific, customised and flexible to the needs and functions of MCL allowing the organisation to view security "*not as an individual, quantified item but because we deal with it all the time and all the time it's part of what we do, it's built into everything by necessity"* (*ITMngr*). In this sense, as security objectives clarify focus and provide a frame of reference for every important aspect of security activity, these objectives and strategies become appropriate as high-level statements that would inform the organisation about how security will be used to create business value.

Little Guidance Provided By Corporate Level Security Mission Statements

The initial setup of security at MCL was ad hoc, fragmented and unplanned with the executive management paying scant attention to security and lacking a holistic perspective of their security governance posture. Security is not regarded as being an issue of executive management, until something goes wrong. *"Security is not regarded as being an issue apart from they [referring to executive management] understand it has to be…it's not on their radar. Until something goes wrong" (ITMngr).* However, even without acceptable levels of formal guidance and assistance, participants were delegated the responsibility for security and security decision-making, hence a culture of accountability was evident. Participants *SysMngr* and *NetMngr*, both stated that their decisions around security are based on their own experiences; *"Currently everything is based on our experiences"* (*SysMngr*). Consequently, the participants, with the understanding that they are held accountable, are in a sense, driven to develop their own security strategic context based on their own experiences and always looking to the IT Manager for guidance, which as explained earlier has its own pitfalls.

Further, the participants at MCL were held responsible not only for what decisions were made but also on how they made those decisions. For instance, did they seek advice? Participants at MCL were not held accountable for compliance to security or of a specific implementation of security. Instead, they were held accountable for the effectiveness of security. This is particularly so for *ITMngr*. In their words "if you want to lose your job, lose data". As such, *ITMngr* takes full ownership of security, and in a sense, controls security in an almost authoritarian fashion. Given their own inadequacies, the other participants accommodate this dictatorship: "*We set the rules and working with ITMngr is good, he sets all these rules and I agree with him entirely"* (*SysMngr*) & *"I do what I've been told by ITMngr"* (*NetMngr*).

Without appropriate formal guidance, this scenario could potentially result in many 'catastrophic' decisions being made by the participants. The serious question to consider is whether the organisation can ultimately hold the participants responsible if something goes wrong bearing in mind that the organisation, due to the lack of formal guidance and attention to security, has never told the participants as to how to make good decisions? Or for that matter, what good decisions are. For instance, *NetMngr* mentions *"Not that I'm aware of…we might have them, but I haven't seen them before [referring to corporate security policies and guidelines]*".

However, the participants knew they were held accountable by the company's director for their role in information security. "*They [referring to executive management] don't have much interest or understanding of why I do what I do. Just that my uptime is good, and everything is working*" (*ITMngr*). Although there was only one accountability loop between the IT Manager and the CEO with active discussions on the state of the company's security and on how to improve it, a secondary feedback and accountability

loop existed between the IT Manager and the other participants. These accountability and feedback loops, although existent, are about what decisions are being made and not about how the decisions are made. Essentially, we believe that the participants were afraid of losing their jobs, which can be considered more as a 'motivational influence' than an accountability aspect.

Security Strategic Context Development From The Bottom Up

Many organisations see Security Governance as a (minor) subset of Corporate Governance. While IT Governance has become a recognized focus area in larger organisations, these organisations often do not give Security Governance the same attention. Hence, organisations still need to realize that just like IT, the field of Information Security is a complex and critical component to their organisation's success. As such, those responsible for security are not just senior management but also middle management and others involved with the implementation of security strategies (those at the operations level of the organisation), and they will similarly need a governance framework for making informed decisions about Information Security.

At MCL, culturally, the focus of security is on the physical systems and network security, an environment traditionally conducive to bottom-up participation. Participants did not have a framework to work with and their experiences were limited. However, whether due to the 'motivational' fear of potentially losing their jobs, or due to their positive disposition towards security, the participants have (unintentionally) developed their own security strategic context as they were forced to come up with their own objectives and controls. Whilst discussing security objectives and controls, *NetMngr* stated "*I just started writing up my own documentation. So basically, I'm starting from scratch here"*. Their experiences being limited to mainly the technical areas drove them to a narrow focus. Thus, frivolity about certain risks and controls exist with certain areas having a heavier focus than others do. Areas such as personnel security and physical and environmental security are missing in MCL's security strategy context. However, other areas such as network and systems security have a heavy focus. This is indicative of a highly IT-driven, porous security with the security focus and initiatives purely on the technical aspects.

At MCL, due to limited corporate governance support and understanding of the importance of security, the participants regarded security as "*totally unplanned and ad hoc*" (*ITMngr*). This attitude was inherent across all levels in the organisation, be it at the executive or middle management, business unit or lower levels. Coupled with the second imperative of an emphasis on executive controls, the significant lack of strategic direction imparted by the organisation has led to a mediocre effort in its security strategy development. We submit that this then results in deficiencies in their depth of security strategic context.

Conclusions

Previous research in Information Security Management highlighted the need for security governance as a means to guide decision-making at the level of middle-management and below (Mishra 2015; Posthumus and von Solms 2004; Veiga and Eloff 2007). This paper presents a revelatory case study that identifies three significant shortcomings in the security governance of SMEs. These are limited diversity in decision-making, lack of guidance in corporate-level mission statements to security decision-makers, and a bottom-up approach to security strategic context development.

Contributions

The rise of external attacks on organisations exposes the inadequacies of a compliance-driven and inward-looking view of security management that relies on a technological 'shield' for protection against generic threats. Instead,

https://aisel.aisnet.org/pajais/vol10/iss4/4
DOI: 10.17705/1pais.10403

organisations must develop a keen situation awareness of the threat environment and the capability to address the complex and evolving security threats therein. Our primary theoretical contribution is to introduce the important (dependent) construct of 'security strategic context'. This construct concerns the participation and shared understanding of stakeholders that enables them to coordinate their activities and adapt to a dynamic security environment. This study explored the phenomenon of strategic security context to explain the variables that affects its existence in organisations. We suggest that the centralization of decision-making structures negatively varies with security strategic context. Further, that diversity of participation in decision-making processes positively varies with security strategic context.

Most current information and academic papers on security governance at the enterprise wide level promote a centralized decision making model based on, in our experience, an ineffective and old-fashioned risk management approach to security (Mishra 2015; Posthumus and von Solms 2004; Veiga and Eloff 2007). The old-fashioned centralized approach is relatively simple to manage: It needs almost no security governance enterprise wide (business unit or operations levels) as most decisions are made at the corporate level.

In the current dynamic security environment, this centralized approach does have a major drawback. Centralized decision-making will reduce the flexibility and adaptability of an organisation's security posture, making it difficult for the organisation to respond quickly/timely to changes in its security environment.

Further, the lack of a formal process by which strategic context is developed with participation from middle and low management results in the creation of a vacuum. In this vacuum middle and lower management are forced to make decisions, a consequence of which is the inadvertent development of a bottom-up strategic context. The lack of a deliberate and conscious development of strategic context due to a predominantly centralized security-planning ethos stifles innovation in security. Our study suggests that organisations should empower decision makers at the middle and lower management levels and improve the timeliness and effectiveness of security decisions by ensuring that all the governance practices identified in the security governance framework are effectively addressed.

From a practice perspective our primary contribution is a precise definition of the breadth and depth of strategic security context as a useful tool for organisations to transform their approach to security. Instead of an approach that is based on compliance and technological controls, we advocate for organisations to address objectives and strategies through developing their security strategic context. With this alternative approach, it is expected that security policies and guidelines developed will enable decision makers to understand the rationale for controls, rather than simply performing the function of security controls. Further, unlike current studies that focus primarily on oversight, our emphasis is to understand how decisions are made and not focus on what decisions are made.

To create a dynamic, flexible and agile security posture, a more decentralized approach to security decision-making is needed. A decentralized approach will need good security governance at all levels. To attain this, it is important that the necessary enterprise-wide security governance structures and processes are developed and put in place. This ensures that adequate security objectives and security strategies are developed and effectively communicated to the decision makers. This, in itself, is expected to promote innovation and effective security.

Future Work

The study of information security governance is fertile for considerable and sustained focus in Information Systems research. The construct of strategic security context requires further study starting of which there can be varied

approaches. A large-scale survey of small-to-medium as well as large organisations across a broad range of industry sectors and regulatory environments requires further exploratory studies to identify a full set of theoretical constructs (independent variables). Other studies may look more closely at the specific best-practice standard implemented in the organisation to better understand how various standards affect the strategic security context of the organisation (e.g. COBIT).

Our study did not look at the role of power distance between senior managers and the lower echelons of the management structure. In countries like Malaysia with a high power-distance index (Hofstede Insights 2018), the typical gap in communications and trust is significantly widened (see Mackenzie (2010) for a US-based study). When this gap is compounded by the perception that IT security is a technical problem best handled by operational staff, strategic security context will suffer on account of the diversity in decision-making, lack of guidance from senior managers, and a firm bottom-up approach to making critical security decisions that affect the firm.

References

Abdul Molok, N.N., Ahmad, A., and Chang, S. 2010. "Understanding the Factors of Information Leakage through Online Social Networking to Safeguard Organizational Information," *Proceedings of the 21st Australasian Conference on Information Systems*.

Ahmad, A. 2002. "The Forensic Chain of Evidence Model: Improving the Process of Evidence Collection in Incident Handling Procedures," *The 6th Pacific Asia Conference on Information Systems*.

Ahmad, A., Maynard, S., and Shanks, G. 2015. "A Case Analysis of Information Systems and Security Incident Responses," *International Journal of Information Management*).

Ahmad, A., and Maynard, S.B. 2014. "Teaching Information Security Management: Reflections and Experiences," *Information Management & Computer Security* (22:5), pp 513-536.

Alshaikh, M., Maynard, S.B., and Ahmad, A. 2015. "Information Security Policy: A Management Practice Perspective," in: *The 26th Australasian Conference on Information Systems,*. Adelaide, Australia.

Appari, A., and Johnson, M.E. 2010. "Information Security and Privacy in Healthcare: Current State of Research," *International journal of Internet and enterprise management* (6:4), pp 279-314.

Bergeron, F., Croteau, A.-M., Uwizeyemungu, S., and Raymond, L. 2015. "It Governance Theories and the Reality of Smes: Bridging the Gap," *System Sciences (HICSS), 2015 48th Hawaii International Conference on*: IEEE, pp. 4544-4553.

Borck, J. 2000. "Advice for a Secure Enterprise: Implement the Basics and See That Everyone Uses Them," *InfoWorld* (22:46), pp 90-90.

Broadbent, M. 2002. "Cio Futures–Lead with Effective Governance," *ICA 36th Conference, Singapore*.

Broadbent, M., and Weill, P. 1997. "Management by Maxim: How Business and It Managers Can Create It Infrastructures," *Sloan management review* (38), pp 77-92.

Brown, W., and Nasuti, F. 2005. "What Erp Systems Can Tell Us About Sarbanes-Oxley," *Information Management & Computer Security* (13:4), pp 311-327.

Burke, J.C. 2005. "Closing the Accountability Gap for Public Universities: Putting Academic Departments in the Performance Loop," *Planning for higher education* (34:1), pp 19-28.

https://aisel.aisnet.org/pajais/vol10/iss4/4
DOI: 10.17705/1pais.10403

Carcary, M., Renaud, K., McLaughlin, S., and O'Brien, C. 2016. "A Framework for Information Security Governance and Management," *IT Professional* (18:2), pp 22-30.

Carrapico, H., and Farrand, B. 2017. "'Dialogue, Partnership and Empowerment for Network and Information Security': The Changing Role of the Private Sector from Objects of Regulation to Regulation Shapers," *Crime, Law and Social Change* (67:3), pp 245-263.

Chen, H., Maynard, S.B., and Ahmad, A. 2013. "A Comparison of Information Security Curricula in China and the USA," in: *11th Australian Information Security Management Conference*. Churchlands, Australia: Edith Cowan University.

Chong, J.L., and Tan, F.B. 2012. "It Governance in Collaborative Networks: A Socio-Technical Perspective," *Pacific Asia Journal of the Association for Information Systems* (4:2).

da Veiga, A., and Martins, N. 2015. "Improving the Information Security Culture through Monitoring and Implementation Actions Illustrated through a Case Study," *Computers & Security* (49), pp 162-176.

De Bruin, R., and Von Solms, S. 2016. "Cybersecurity Governance: How Can We Measure It?," *IST-Africa Week Conference, 2016*: IEEE, pp. 1-9.

deMaine, S.D. 2016. "Preparing Law Students for Information Governance," *Legal Reference Services Quarterly* (35:2), pp 101-123.

Dhillon, G., and Torkzadeh, G. 2006. "Value - Focused Assessment of Information System Security in Organizations," *Information Systems Journal* (16:3), pp 293-314.

Dhillon, G., Torkzadeh, G., and Chang, J. 2018. "Strategic Planning for Is Security: Designing Objectives," *International Conference on Design Science Research in Information Systems and Technology*: Springer, pp. 285-299.

Dreibelbis, R.C., Martin, J., Coovert, M.D., and Dorsey, D.W. 2018. "The Looming Cybersecurity Crisis and What It Means for the Practice of Industrial and Organizational Psychology," *Industrial and Organizational Psychology* (11:2), pp 346-365.

Elyas, M., Ahmad, A., Maynard, S.B., and Lonie, A. 2015. "Digital Forensic Readiness: Expert Perspectives on a Theoretical Framework," *Computers and Security* (52), pp 70-89.

Elyas, M., Maynard, S.B., Ahmad, A., and Lonie, A. 2014. "Towards a Systematic Framework for Digital Forensic Readiness," *Journal of Computer Information Systems*).

Gao, W., Liu, Z., Guo, Q., and Li, X. 2018. "The Dark Side of Ubiquitous Connectivity in Smartphone-Based Sns: An Integrated Model from Information Perspective," *Computers in Human Behavior* (84), pp 185-193.

Gartner. 2017. "Gartner Forecasts Worldwide Security Spending Will Reach $96 Billion in 2018, up 8 Percent from 2017." Retrieved 7/8/18, from https://www.gartner.com/newsroom/id/3836563

Goodman, S., Straub, D.W., and Baskerville, R. 2016. *Information Security: Policy, Processes, and Practices*. Routledge.

Harold, K., and Heinz, W. 2008. "Essentials of Management: An International Perspective." McGraw, New Delhi, India.

He, Y., and Johnson, C. 2017. "Challenges of Information Security Incident Learning: An Industrial Case Study in a Chinese Healthcare Organization," *Informatics For Health & Social Care* (42), pp 1-16.

Hofstede Insights. 2018. "What About Malaysia?" Retrieved 20/8/18, from https://www.hofstede-insights.com/country-comparison/malaysia/

Ifinedo, P. 2014. "Information Systems Security Policy Compliance: An Empirical Study of the Effects of Socialisation, Influence, and Cognition," *Information & Management* (51:1), pp 69-79.

Jorgensen, D.L. 2015. "Participant Observation," *Emerging trends in the social and behavioral sciences: An interdisciplinary, searchable, and linkable resource*), pp 1-15.

Karyda, M. 2017. "Fostering Information Security Culture in Organizations: A Research Agenda," in: *MCIS 2017 Proceedings*. p. 28.

Knapp, K.J., Marshall, T.E., Rainer, R.K., and Ford, F.N. 2006. "Information Security: Management's Effect on Culture and Policy," *Information Management & Computer Security* (14:1), pp 24-36.

Koh, K., Ruighaver, A.B., Maynard, S.B., and Ahmad, A. 2005. "Security Governance: Its Impact on Security Culture," *Proceedings of the 3rd Australian Information Security Management Conference*, Perth.

Lemay, A., Calvet, J., Menet, F., and Fernandez, J.M. 2018. "Survey of Publicly Available Reports on Advanced Persistent Threat Actors," *Computers & Security* (72), pp 26-59.

Lim, J.S., Ahmad, A., Chang, S., and Maynard, S.B. 2010. "Embedding Information Security Culture Emerging Concerns and Challenges," in: *PACIS 2010 Proceedings*. Brisbane, Australia: pp. 463-474.

Love, P., Reinhard, J., Schwab, A.J., and Spafford, G. 2010. "Gtag 15: Information Security Governance," The Institute of Internal Auditors, p. 134.

Mackenzie, M.L. 2010. "Manager Communication and Workplace Trust: Understanding Manager and Employee Perceptions in the E-World. ," *International Journal of Information Management* (30:6), pp 529-541.

Malandrin, L.J.A.A., and de Brito Carvalho, T.C.M. 2013. "Maintaining Information Security in the New Technological Scenario," *Pacific Asia Journal of the Association for Information Systems* (5:3).

Masrom, M., and Rahimly, A. 2015. "Overview of Data Security Issues in Hospital Information Systems," *Pacific Asia Journal of the Association for Information Systems* (7:4).

Maynard, S., Ruighaver, A., and Ahmad, A. 2011. "Stakeholders in Security Policy Development," *9th Australian Information Security Management Conference*.

Maynard, S.B., Onibere, M., and Ahmad, A. 2018. "Defining the Strategic Role of the Chief Information Security Officer," *Pacific Asia Journal of the Association for Information Systems* (10:3).

Maynard, S.B., and Ruighaver, A.B. 2006. "What Makes a Good Information Security Policy: A Preliminary Framework for Evaluating Security Policy Quality," *Proceedings of the Fifth Annual Security Conference*, Las Vegas, Nevada USA.

Miles, M.B., and Huberman, A.M. 1994. *Quantitative Data Analysis*.

Mishra, S. 2015. "Organizational Objectives for Information Security Governance: A Value Focused Assessment," *Information & Computer Security* (23:2), pp 122-144.

Okere, I., Van Niekerk, J., and Carroll, M. 2012. "Assessing Information Security Culture: A Critical Analysis of Current Approaches," *Information Security for South Africa (ISSA), 2012*: IEEE, pp. 1-8.

https://aisel.aisnet.org/pajais/vol10/iss4/4
DOI: 10.17705/1pais.10403

Park, S., Ruighaver, A.B., Maynard, S.B., and Ahmad, A. 2012. "Towards Understanding Deterrence: Information Security Managers' Perspective," in: *Proceedings of the International Conference on IT Convergence and Security*. Suwon, Korea.

Peppard, J. 2007. "The Conundrum of It Management," *European Journal of Information Systems* (16), pp 336-345.

Peterson, R.R., O'Callaghan, R., and Ribbers, P. 2000. "Information Technology Governance by Design: Investigating Hybrid Configurations and Integration Mechanisms," *Proceedings of the twenty first international conference on Information systems*: Association for Information Systems, pp. 435-452.

Poggi, A., and Tomaiuolo, M. 2018. "Information Attacks and Defenses on the Social Web," in: *Global Implications of Emerging Technology Trends*. IGI Global, pp. 216-235.

Posthumus, S., and von Solms, R. 2004. "A Framework for the Governance of Information Security," *Computers & Security* (23:8), pp 638-646.

Pultorak, D. 2005. "It Governance: Toward a Unified Framework Linked to and Driven by Corporate Governance," *CIO Wisdom II, Prentice Hall Ptr*).

Rahimian, F., Bajaj, A., and Bradley, W. 2016. "Estimation of Deficiency Risk and Prioritization of Information Security Controls: A Data-Centric Approach," *International Journal of Accounting Information Systems* (20), 4//, pp 38-64.

Rezgui, Y., and Marks, A. 2008. "Information Security Awareness in Higher Education: An Exploratory Study," *Computers & Security* (27), pp 241-253.

Ribbers, P.M., Peterson, R.R., and Parker, M.M. 2002. "Designing Information Technology Governance Processes: Diagnosing Contemporary Practices and Competing Theories," *System Sciences, 2002. HICSS. Proceedings of the 35th Annual Hawaii International Conference on*: IEEE, pp. 3143-3154.

Ruighaver, A.B., Maynard, S.B., and Chang, S. 2007. "Organisational Security Culture: Extending the End-User Perspective," *Computers & Security* (26:1), pp 56-62.

Ruighaver, A.B., Maynard, S.B., and Warren, M. 2010. "Ethical Decision Making: Improving the Quality of Acceptable Use Policies," *Computers and Security* (29:7), pp 731-736.

Safa, N.S., Von Solms, R., and Furnell, S. 2015. "Information Security Policy Compliance Model in Organizations," *Computers & Security*).

Shattuck, L.G. 2000. "Communicating Intent and Imparting Presence," ARMY COMBINED ARMS CENTER FORT LEAVENWORTH KS MILITARY REVIEW.

Shedden, P., Ahmad, A., and Ruighaver, A.B. 2010. "Organisational Learning and Incident Response: Promoting Effective Learning through the Incident Response Process," in: *Proceedings of the 8th Australian Information Security Management Conference*. Perth, Australia: Edith Cowan University, pp. 139-150.

Shedden, P., Ahmad, A., Smith, W., Tscherning, H., and Scheepers, R. 2016. "Asset Identification in Information Security Risk Assessment: A Business Practice Approach," *CAIS* (39), p 15.

Shleifer, A., Vishny, R.W., Porta, R., and Lopez-de-Silanes, F. 2000. "Investor Protection and Corporate Governance," *Journal of financial economics* (58:1-2), pp 3-27.

Siponen, M., and Willison, R. 2009. "Information Security Management Standards: Problems and Solutions," *Information & Management* (46:5), pp 267-270.

Sommestad, T., Hallberg, J., Lundholm, K., and Bengtsson, J. 2014. "Variables Influencing Information Security Policy Compliance: A Systematic Review of Quantitative Studies," *Information Management & Computer Security* (22:1), pp 42-75.

Straub, D.W., and Welke, R.J. 1998. "Coping with Systems Risk: Security Planning Models for Management Decision Making," *MIS Quarterly*), December.

Tan, T., and Ruighaver, A. 2005a. "A Framework for Investigating the Development of Security Strategic Context in Organisations," *Proceedings of the 6th Aus Information Warfare & Security Conference: Protecting the Australian Homeland*, pp. 216-226.

Tan, T., and Ruighaver, A. 2005b. "Understanding the Scope of Strategic Context in Security Governance," *IT Audit: A Strategic Foundation for Corporate Governance*), pp 65-77.

Tan, T., Ruighaver, A.B., and Ahmad, A. 2010. "Information Security Governance: When Compliance Becomes More Important Than Security," in: *Security and Privacy–Silver Linings in the Cloud*. Springer, pp. 55-67.

Tan, T.C., and Ruighaver, A. 2004. "Developing a Framework for Understanding Security Governance," *2nd Australian Information Security Management Conference*: Citeseer, p. 37.

Tesch, R. 2013. *Qualitative Research: Analysis Types and Software*. Routledge.

Tsakalidis, G., and Vergidis, K. 2017. "A Systematic Approach toward Description and Classification of Cybercrime Incidents," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*:99), pp 1-20.

Veiga, A.D., and Eloff, J.H. 2007. "An Information Security Governance Framework," *Information Systems Management* (24:4), pp 361-372.

Verizon. 2018. "2018 Data Breach Investigations Report."

Waxer, P.H. 1985. "Video Ethology: Television as a Data Base for Cross-Cultural Studies in Nonverbal Displays," *Journal of Nonverbal Behavior* (9:2), pp 111-120.

Webb, J., Ahmad, A., Maynard, S.B., and Shanks, G. 2014. "A Situation Awareness Model for Information Security Risk Management," *Computers & Security* (44), pp 391-404.

Webb, J., Ahmad, A., Maynard, S.B., and Shanks, G. 2016. "Foundations for an Intelligence-Driven Information Security Risk-Management System," *Journal of Information Technology Theory and Application (JITTA)* (17:3), pp 25-51.

Weill, P., and Ross, J.W. 2004. *It Governance: How Top Performers Manage It Decision Rights for Superior Results*. Harvard Business Press.

Weill, P., and Woodham, R. 2002. "Don't Just Lead, Govern: Implementing Effective It Governance,").

Whitman, M.E., and Mattord, H.J. 2017. *Management of Information Security*, (5th ed.). Boston, Mass.: Centage.

Yin, R.K. 2018. *Case Study Research and Applications: Design and Methods.* . Sage publications.

https://aisel.aisnet.org/pajais/vol10/iss4/4
DOI: 10.17705/1pais.10403

Appendix 1: Detailed Analysis of the Breadth and Coverage of The Strategic Context

green and italicized text = activities performed by participants at MCL in accordance with suggestions from ISO 27002.
red and bolded text = activities performed by participants additional to those activities suggested in the ISO 27002 Security Standard.
black underlined text = activities proposed by ISO 27002, but no evidence was found that would indicate MCL was performing these activities.

		Depth	
		Security Objectives	**Security Strategies & Infrastructure**
Coverage	Network Security	• *Ensure availability and reliability of network services (general access, authentication and access to information systems).* • **Compartmentalise and define roles.**	• *Control access to critical data and/or servers to ensure availability and reliability.* • *Manage incoming files.* • **Maintain a flexible approach. Adjust and move in response to events.** • **Lockdown of servers via tightening of roles.**
	Systems Security	• *Prevent unauthorized activities.* • *Detect unauthorized activities.* • **Compartmentalise and define roles.**	• Regular monitoring of sys and events. • Define a security policy outlining unauthorised activities. • Implement organisational wide use of company approved encryption. • *Provide means for authentication.* • **Maintain a flexible approach.** • **Adjust in response to things.** • **Ad hoc monitoring of network, processes and systems.** • **Informal control of access rights.** • **Lockdown servers, tighter roles.**
	Physical & Environ-mental Security	• Prevent damage and interference to business premises and information. • Prevent loss, damage or compromise of assets and interruption to business activities. • **Outsourced to third party.**	• Defined security perimeter erected. • Security related hardware and software should at all times be protected against tampering to maintain their integrity and against disclosure of secret keys. • Computer and information equipment are secured to reduce unauthorised physical access.
	Personnel Security	• Reduce risks of human error, theft, fraud or misuse by employees. • Ensure users are aware of security threats & concerns. • *Minimise damage, monitor & learn from incidents (limited).*	• Ensure that incidents affecting security be reported. • Define and establish formal disciplinary processes. • Ensure that employees are aware of security threats. • *Address security responsibilities at the recruitment stage.*

		Depth	
		Security Objectives	**Security Strategies & Infrastructure**
Coverage	Communi-cations & Operations Security	• Define procedures for securing communications and operations facilities. • *Ensure correct & secure operation of information processing facilities.* • *Minimize risk of systems failure.* • *Maintain integrity & availability of info processing & communication.*	• Establish strategy for advanced planning and preparation to ensure availability. • Establish routine procedures for housekeeping. • Establish responsibilities & (informal) procedures for management on of all information processing facilities. • **Maintain a flexible approach. Adjust and move in response to things.** • **Ensure systems have redundancy in event of failure.**
	Data Security	• *Maintain appropriate protection of organisational assets.* • *Ensure that information assets receive an appropriate level of protection.*	• Identify areas of risk in processing cycle. • Define protection of company records. • *All major info assets should be accounted for and have an owner.* • *Owners should be identified for all major assets and the responsibility for the maintenance of appropriate controls should be assigned. This accountability ensures appropriate protection.* • **Maintain a flexible approach. Adjust and move in response to events.**
	Miscellan-eous Security	• Comply with legal requirements. • Ensure compliance of systems with security policies and standards. • *Business continuity management to counteract interruptions to business activities and to protect critical processes from the effects of major failures or disasters.*	• Ensure that the design, operation, use & management of systems be within statutory, regulatory and contractual requirements. • Ensure regular review of Information Systems security. • *Implement a business continuity management process to reduce disruption to an acceptable level.*

https://aisel.aisnet.org/pajais/vol10/iss4/4
DOI: 10.17705/1pais.10403

		Depth	
		Security Architecture	**Security Application(s) Needed**
Coverage	Network Security	• Evaluate policies for information dissemination & authorisation. • *Authentication mechanisms.* • *Control of user access to information.* • *Alerts sent when monitoring software flags anything.* • **Monitor unauthorised access.** • **Automatic deletion of .exe files on mail server.** • **Dedicated role for each server and machine.**	• *Encryption and certificates.* • *Monitor access to directories.* • *Firewalls.* • *Proxy servers.* • *Home grown monitoring software.* • *Up-to-date anti-virus software.* • **Controls to delete .exe files on mail server automatically.** • **SMS and Email alerts.** • **Informal policy determining role for every server/machine.**
	Systems Security	• Security and Acceptable use policies to be disseminated organisation wide. • Systems should be monitored to detect deviation from access control policy and record monitor able events to provide evidence in case of incidents. • *Identify & verify identity of users.* • **Monitor access to directories by unauthorised software/programs.** • **Home-grown monitoring but only of things that would disrupt services (predominantly software or programs, not users).** • **Alerts sent when monitoring software flags anything.**	• Monitoring software to monitor employee activity on system. • *Access Control Software (password managers & policies to ensure complex passwords).* • *Up-to-date anti-virus software.* • *Real time protection.* • *Monitor access files.* • **Monitoring software to monitor system and processing health.** • **SMS and email alerts.** • **Informal policy determining role for every server/machine.**

		Depth	
		Security Architecture	**Security Application(s) Needed**
	Physical & Environ-mental Security	• Secure areas need to be protected by a defined security perimeter, with appropriate security barriers and entry controls. • Special controls may be required to protect against hazards or unauthorised access & to safeguard support facilities. • *Protection equipment to reduce the risk of unauthorised access to data and to protect against loss or damage.*	• Surveillance Technology. • *Access Control (door entry technology, proximity card access, photo identification, and biometrics).* • *Monitoring Software with reviewable access control logs.* • *Data centre provides redundant power supply, air conditioning, secure environment.*
	Personnel Security	• Any breach of security policies will cause an initiation of formal disciplinary action. • Users should be informed in security procedures and correct use of information processing facilities. • *Users made aware of their responsibilities at recruitment (security in job responsibilities, personnel screening and terms of employment).*	• Personnel security policies. • Disciplinary policies. • Accepted Use Policies. • Character Checks. • Maintaining personnel security files. • Security education & training. • Visitor Control. • **Regular emails sent out to employees about laptop security, updating antivirus definitions, etc.** • **Personal, hands on, 1 to 1 mentoring programs.**
Coverage	Communic-ations & Operations Security	• Develop appropriate operating instructions and incident response procedures. Disseminated organisation wide. • Segregation of duties established to reduce risk of negligence or misuse. • Users should be made aware of dangers of unauthorised/malicious software. • *Routine checks on back-up strategy (take back-up copies of data & rehearse timely restoration, logging events and faults).* • **Routine checks to make sure all security updates are installed.**	• Monitoring software to flag errors or procedural breeches. • Security education & training. • *All servers and systems have redundancy.* • *Secure backup facilities.* • **Hourly Online backups.**

https://aisel.aisnet.org/pajais/vol10/iss4/4
DOI: 10.17705/1pais.10403

		Depth	
		Security Architecture	**Security Application(s) Needed**
	Data Security	• Important records are identified. • Controls are allocated depending on nature of application and business impact of any corruption of data. • Delegate specific responsibilities for developing and implementing security controls. • *Responsibilities for the protection of individual assets is clearly defined.*	• *Disk Encryption.* • *Security Tokens and PINs.* • *Backups.* • *Data Masking.* • *Copy protection.* • *Single sign-on.* • **User groups set.** • **File management processes.** • **Informal policy on data security set.**
	Miscellan-eous Security	• Reviews performed against appropriate security policies & technical platforms. • Information systems should be audited for compliance with security implementation standards and legal requirements. • *Business continuity management process must be implemented to deal with disruption through a combination of preventative and recovery controls.*	• *Security audits and assessments (limited and ad hoc).* • *Backup strategies.* • *Monitoring strategies.*

A note on Security Investment & Prioritisation

As an SME, resource allocation for security initiatives is scarce and limited. MCL does not have an individually allocated budget for security. Security initiatives are drawn out of the IT Budget. Security is not prioritised but is seen as an aspect of things that need to be done. Suggestions for investments can be made any one of the members of the Managed Services Team as they are responsible for security. However, the decision is made by the IT Manager. Although in certain circumstances, the IT Manager brings these suggestions up to higher management, this is in no means an attempt to get verification. Rather it is more about communication and an effort to keep the executive levels of the organisation involved in what is happening.

About the Authors

Sean B. Maynard is an academic based at the School of Computing and Information Systems, University of Melbourne, Australia. His research interests are in the management of information security specifically relating to security policy, security culture, security governance, security strategy, security analytics, and incident response. He has over 50 publications on these and other areas. His research has been published in high-impact journals such as Computers & Security and the International Journal of Information Management as well as leading conferences such as the International Conference on Information Systems.

Terrence Tan completed his PhD in 2012 at the University of Melbourne. His research looked at improving the process of decision-making in information security governance and strategy development. Terence has had a long standing relationship with the security world. He has a number of security qualifications stemming from his background in physical security operations including close personal protection and investigations.

Atif Ahmad is a senior academic at the University of Melbourne's School of Computing & Information Systems. His main areas of expertise are in the strategy, risk and incident response aspects of Information Security Management (ISM). He has authored over seventy scholarly articles in ISM and received over $3M in grant funding. His research has been published in high-impact journals such as Computers & Security and the International Journal of Information Management as well as leading conferences such as the International Conference on Information Systems. Atif has previously served as a cybersecurity consultant for WorleyParsons, Pinkerton and SinclairKnightMerz. He is a Certified Protection Professional with the American Society for Industrial Security.

A.B. (Tobias) Ruighaver is a retired academic, who still maintains a website on security governance and security culture at www.securitygovernance.net. Before his retirement Dr. Ruighaver was the head of the Organisational Information Security Group at the University of Melbourne and supervised in depth case study research in over 30 Australian and Singaporean organisations to investigate their security culture, security governance and/or risk assessment practices.

https://aisel.aisnet.org/pajais/vol10/iss4/4
DOI: 10.17705/1pais.10403