2005

Security governance: Its impact on security culture

K. Koh

A. B. Ruighaver

S. B. Maynard

A. Ahmad

Koh, K., Ruighaver, A. B., Maynard, S. B., & Ahmad, A. (2005). Security governance: Its impact on security culture. In *Proceedings of 3rd Australian Information Security Management Conference* (pp. 47-58). Edith Cowan University. Available here.

Security Governance: Its Impact on Security Culture

K. Koh, A.B. Ruighaver, S. B. Maynard, and A. Ahmad
Department of Information Systems
The University of Melbourne
Australia

ABSTRACT

While there is an overwhelming amount of literature that recognises the need for organisations to create a security culture in order to effectively manage security, little is known about how to create a good security culture or even what constitutes a good security culture. In this paper, we report on one of two case studies performed to examine how security governance influences security culture and in particular, the sense of responsibility and ownership of security. The results indicate that although the structural and functional mechanisms in security governance are influencing factors, it is the extent of social participation that may be the major contributing component in security governance that influences the levels of responsibility and sense of ownership that IT security personnel have over the management of security within an organisation.

Keywords

security governance, security culture, social participation

INTRODUCTION

Background and Rationale

In today's rapidly changing business environment with the evolution of e-technologies, organisations are experiencing increased uncertainty and complexity in their day-to-day operations. Combined with the over-reliance on computer-supported processes, organisations are progressively more vulnerable to security attacks and breaches (Schlienger & Teufel, 2003), emphasising the need and importance of effective security management.

Security, however, is not a one-step, easy-to-identify issue, but rather, requires an in-depth process that must be continually refined, revised and monitored in order to keep up with evolving business strategies and dynamically changing environments (Breidendach, 2000). It is these processes that create security controls to protect an organisation's critical assets against internal and external threats. Without proper monitoring procedures in place these security controls risk becoming obsolete and redundant (Martins & Eloff, 2002). Hence, the challenge becomes understanding security governance and how the security decision making process can aid organisations to effectively adapt and cope with the dynamically changing environment (Peterson et al, 2000; Brown, 1997; Sambamurthy & Zmud, 1999).

Research studies have also acknowledged the importance of users' roles in effective security management, and have argued that contrary to popular perception, the dependent factor for effective security management would not be the technology element, but rather the human element. Researchers have also pointed out that in many organisations, most disregard the human dimension (Adam & Sasse, 1999; Martins & Eloff, 2002). Studies have revealed that the lack of knowledge regarding the behaviour of how users act towards security results in users being forced to comply with security mechanisms incompatible with work. Furthermore socio-cultural practices within the organisation are also often incompatable (Adam & Sasse, 1999). As a result security breaches may occur throughout the organisation. Researchers (von Solms, 2001; Schlienger & Teufel, 2003) propose that in order to institutionalise proper user-behaviour towards information security within an organisation, a security culture has to be created.

A security culture framework was applied by Chia, Ruighaver and Maynard (Chia et. al., 2003) to assess the quality of security culture in organisations using 'eight overarching, descriptive dimensions of culture'. They discovered that the application of the framework was extremely beneficial towards understanding the quality of information security cultures within organisations.

In spite of it being clear that security governance does have underlying influences on organisational security culture, there is still a lack of research linking both together. Henceforth, the rationale and basis behind this research study is to link security governance to security culture. However, to reduce the scope of our research we felt unable to simultaneously address all dimensions of the security culture framework proposed by Chia. As we will discuss in section 2, we choose a single dimension that is most obviously related to security governance, and concentrated our initial investigations on the 'Control, Coordination and Responsibility' aspects of security culture.

Aim and Scope of Research Study

As illustrated previously, the impetus of this study is the dynamic changing environments that organisations need to adapt to, due to the rapid advancement of IT technologies, business strategies and global competition. As a result, organisations need to establish a deeper understanding of how it might be able to better govern its resources to increase its readiness and preparedness against security attacks.

This paper's aim is primarily to explore how security governance can influence information security culture in loose, decentralised decision making contexts so as to allow organisations to better adapt and cope with the dynamic changing environments. Therefore, this study aims to answer two main research questions:

1. **How can security governance influence the sense of responsibility and ownership of security within an organisation?**

Security governance literature states that there is a need to delegate authority and responsibility onto the roles in-charge of implementing security, hence allowing the flexibility for them to design appropriate measures to better protect the organisation's critical assets. This question seeks to explore how security governance can affect the levels of responsibility and sense of ownership that the people implementing security have. Through this question, this study hopes to provide an insight to how security decision making arrangements can improve the organisation's flexibility and adaptability when countering internal and external threats, especially in the nature of security's dynamic changing environments.

2. **How does the degree of social participation in security governance affect the sense of responsibility and ownership within an organisation?**

In order to establish a tighter focus for this research study, a particular aspect of security governance, social participation, will be more thoroughly investigated. Through this question, the influence of the levels of social participation, on the sense of responsibility and ownership that they might have towards security will be investigated. This research question hopes to provide a deeper understanding of the role social participation, in relation to security governance, has on an effective security management in dynamic changing environments.

This study has been designed to examine the importance of security governance and the role it plays in influencing information security culture, in particular, the sense of responsibility and ownership IT security personnel have over managing security in their organisation. Whilst it may be beneficial to assess the levels of security preparedness of the organisations under investigation, it was not the primary objective of this study.

Structure of the Research Study

So far the background and rationale of this research study have been discussed, along with the main research questions. In the next section, security governance and its overlapping relationships with information security culture will be discussed. Two theoretical frameworks the 'IT Governance Framework' (Figure.1) and the 'Security Culture Framework' (Figure 2) will be described in detail to develop a better understanding of how they relate to each other. We will then discuss the lens we developed (Figure 3) to examine how security governance influences the security culture in our case studies.

In section 3 we will describe one of the two case studies we did using the lens described in section 2. This case study was chosen for this paper as it is an excellent example of how extensive and enthusiastic social participation can improve decision making processes as well as improve the security culture in an organisation. The second case study was not included within this paper due to space limitations, although many of the conclusions have been drawn from both case studies.

A brief discussion of this study's main findings is presented in the last section, the discussions and conclusions.

SECURITY GOVERNANCE AND SECURITY CULTURE

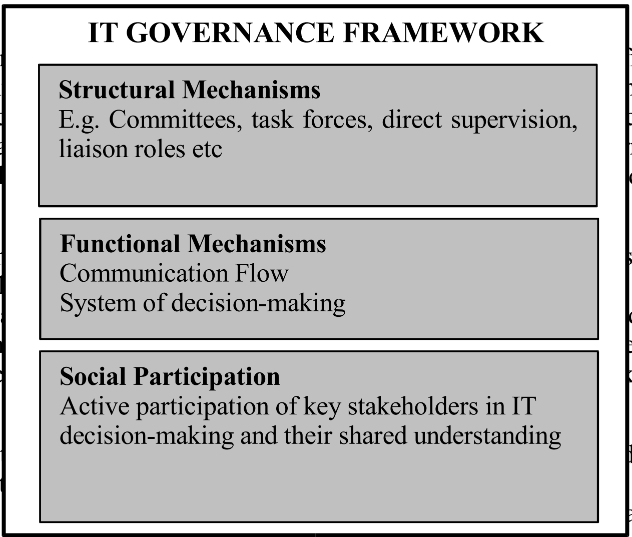
Introduction

The objectives in this section are to allow the reader to gain an overall understanding of the importance of security governance and the key factors that contribute to an effective security governance model. Next, we will identify the need to instil an information security culture within an organisation to enhance security management. After a brief discussion of the similarities and overlapping issues in the two theoretical frameworks for these two areas, an explanation is given about how both frameworks are linked together to develop a lens for our study of how security governance might influence security culture.

Security Governance

Governance is the assignment of decision rights and an accountability framework to encourage desirable behaviour in decision making (Broadbent, 2002). Security governance provides a framework in which the decisions made about security issues are aligned with the overall business strategy and culture of the organisation (Dallas & Bell, 2004). Thus, security governance is about decision making per se and is concerned with setting directions, establishing standards and principles and prioritising investments.

Security governance is different from management. Security governance is about involvement, accountability and decision rights whereas management is about making and implementing specific decisions (Broadbent, 2003). Security governance can be broken up into several domains which include the 'what' decisions to be made, the 'who' being responsible for making key decisions (the authority figures), and the 'how' of decision making (the structures and processes) that foster the decision making process (Dallas, 2002; Weill and Woodham, 2002). Figure 1 shows a model of IT Governance (Peterson et al, 2000). According to Peterson's 'IT Governance Framework', security governance is broken up into primarily three dimensions: structural mechanisms, functional mechanisms and social participation.



IT GOVERNANCE FRAMEWORK

Structural Mechanisms
E.g. Committees, task forces, direct supervision, liaison roles etc

Functional Mechanisms
Communication Flow
System of decision-making

Social Participation
Active participation of key stakeholders in IT decision-making and their shared understanding

Figure 1 – 'IT Governance Framework'

Structural mecha fferent parts, the formal and informal
structures presen nal structures range with increasing
complexity and c ces, and temporal teams, to full-time
integrating roles a mal structural mechanisms in security
governance are t dination and the building of network
relationships.

The functional r system of decision making and the
communication fl level of comprehensiveness in which
decision making d is measured by the formalisation of
which decision m es. The communication flow describes
informal lateral c keholders during the security decision
making process.

Finally social par ders in decision making and the shared
understanding bet characterised by distributed decision
making, require akeholders if they are to coordinate
activities and adapt to changing circumstances. Peterson further adds that social participation is a rich and dynamic mechanism and involves high levels of mutual understanding of business IT objectives and plans by key stakeholders.

In security research there is little research on governance and as a result it is necessary to borrow from the extensive literature on IT governance and to adapt general IT governance frameworks to a security context. Weill and Woodham (2002) observe that through effective IT governance arrangements, organisations not only make better IT decisions, but they also make better IT decisions consistently. This view is further supported by Broadbent's (2002) observation that enterprises achieving above average returns from IT investments deal with the increased complexity by clarifying who is able to make critical decisions and who is accountable for the critical decisions. That is, these successful enterprises have thoughtfully designed their IT governance, rather than focusing only on how IT is managed. Hence, we believe that with the presence of good security governance, it is more likely that good decisions will be made consistently regardless of how complex and extensive the threats the organisation faced during all stages of the security management cycle.

Governance specifies the decision rights and accountability framework to encourage desirable behaviour in the handling and management of security (Dallas & Bell, 2004). As highlighted earlier security governance is not about management, but rather, is about the accountability and responsibility for critical decisions. Hence, effective security governance needs to provide mechanisms that enable managers to allocate responsibilities and accountabilities accordingly (Korac-Kakabadse & Kakabadse, 2001). Dallas also states 'the abandonment of responsibilities in the decision making process will lead to undisciplined decisions made by whoever has sufficient political clout - clearly not the optimal solution'. She further adds that it is critical to clarify stakeholders' roles within the decision making process and for decision makers to be held accountable. For each decision, it should be specified which stakeholder provides input, what activities are required to obtain such input, who is consulted during option deliberations, who makes the final decisions, who communicates the decision and which groups receive news of the decision. Hence a goal to effective security governance is to construct a decision making process and a chain of authority that can be documented and managed.

Another important aspect of security governance, social participation, is defined as the active participation of key stakeholders in decision making and their shared understanding (Peterson et al 2000). In line with this argument, Broadbent (Broadbent, 2002) states that the activities undertaken to gather input during the decision making process is a vital part of governance. However, it is imperative to weigh the participants' input in the decision making process (Dallas & Bell, 2004) to accomplish a successful security governance, The key to achieving this is to enhance the voice of the participants and to provide ownership-like incentives to those participants who contribute or control specialised inputs towards decision making and to align the interests of these critical stakeholders with the interests of the company (Blair, 1995).

Security Culture

Throughout this paper, the term 'Security Culture' will be used extensively as part of its focus and centre of analysis. Therefore, it is important to note that when this study refers to 'security culture', it primarily focuses on the information security culture of organisations. It is not within the objective or scope of this study to investigate or discuss the security culture pertaining to the physical aspects of security such as building access controls, security clearance and surveillance.

A general observation by several researchers (Adam & Sasse 1999; Martins & Eloff 2002) is that information security management in organisations today mostly disregard the human dimension. Organisations tend to focus mainly on technical and procedural measures: Most often the only aspect that takes into account the human element would be security awareness programmes. Breidenbach (Breidenbach, 2000) stresses that there is a need to go beyond awareness and take action. She claims that protection from security breaches requires investment in technology, services, and personnel as well as adjustments in corporate culture. Other researchers (Schlienger & Teufel, 2002; von Solms, 2000; Nosworthy, 2000) claim that in order to institutionalise proper user behaviour towards information security within an organisation, a security culture has to be created.

Although many researchers have identified the importance and the need for an information security culture in organisations, few have established a clear and definitive meaning to the term 'security culture'. Schlienger & Teufel (2002) define information security culture as 'all socio-cultural measures that support technical activity methods, so that information security becomes a natural aspect in the daily activity of every employee'. In addition, they observe that in order for security culture to make a substantial contribution to the field of information security, it is necessary to have a set of methods for studying security culture. However, no unique toolset and method for the study of organisational security culture exists, indicating the need for research in this field.

In light of this, Chia (Chia et al, 2002) applied a generic organisational culture framework, developed by Detert (Detert et al, 2000) to information security, and used it to explore the specific field of security culture within organisations (Figure 2). Detert developed the initial framework by reviewing existing cultural frameworks and using qualitative content analysis to classify them. Based on this prescribed framework, Chia explored the differences in organisational security culture of two organisations, and discovered that the application of the framework was extremely beneficial towards understanding the quality of information security cultures within organisations.

SECURITY CULTURE FRAMEWORK

The Basis of Truth and Rationality
The Nature of Time and Time Horizon
Motivation
Stability Vs Change/Innovation/Personal Growth
Orientation to Work, Task, Co-Workers
Isolation Vs Collaboration/Cooperation

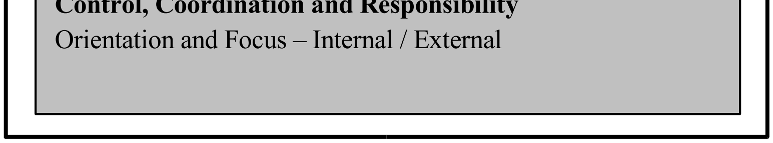

Control, Coordination and Responsibility
Orientation and Focus – Internal / External

Figure 2 – 'Security Culture Framework'

An important issue mentioned by Chia is the need to get more people involved in security. They believe that by increasing the participation levels of employees in security decisions will reinforce the belief that security is of the utmost importance. Consequently this increased participation levels also influences the motivation of employees to be security conscious and take responsibility for their own security. This relates back to security governance, where Peterson (Peterson et al, 2000) refers to this phenomenon as social participation, highlighting its underlying influence towards security culture.

Influencing Security Culture through Effective Security Governance

The main focus of this paper is on how security governance influences the security culture. In the previous sections two frameworks have been identified, one for security governance and one for security culture. Parts of these models can be used to develop a lens for studying how security culture influences security culture within the case study organisation. While security governance should probably have an influence on any of the eight dimensions of this model, the scope of a study using all eight dimensions at the same time is expected to be too large to be manageable. Upon reviewing the culture framework, it is noted that the particular dimension of 'Control, Coordination and Responsibility' draws a strong connection to security governance, and this is where we concentrated our study (Figure 3).

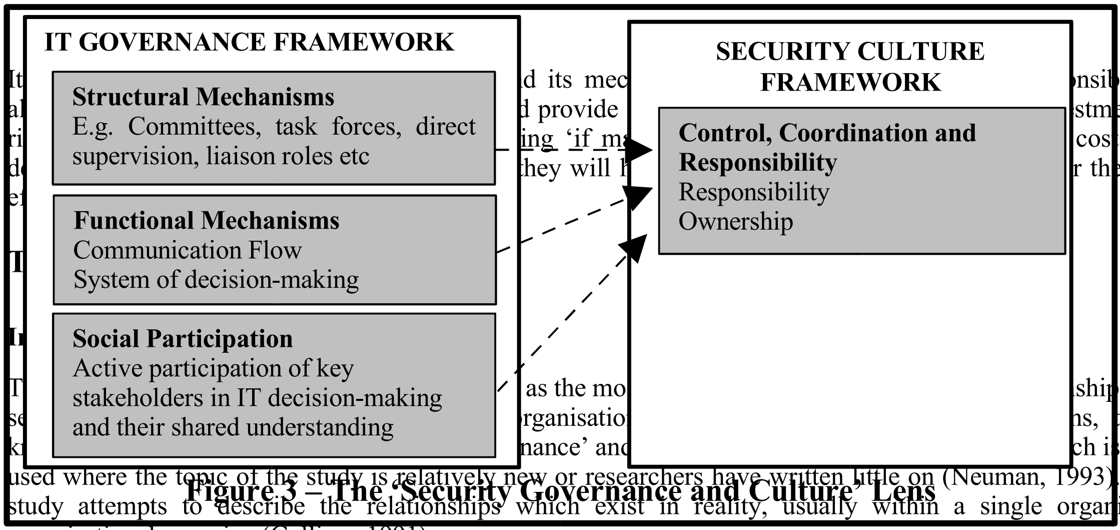

IT GOVERNANCE FRAMEWORK
Structural Mechanisms
E.g. Committees, task forces, direct supervision, liaison roles etc
Functional Mechanisms
Communication Flow
System of decision-making
Social Participation
Active participation of key stakeholders in IT decision-making and their shared understanding
SECURITY CULTURE FRAMEWORK
Control, Coordination and Responsibility
Responsibility
Ownership

Figure 3 – The 'Security Governance and Culture' Lens

It ... d its mec ... nsibilities are a ... d provide ... stments are at ri ... ing 'if ma ... costs of their d ... hey will h ... r their control e

T ... as the mo ... ships between s ... rganisatio ... ns, there is a k ... nance' and ... ch is generally used where the topic of the study is relatively new or researchers have written little on (Neuman, 1993). The case study attempts to describe the relationships which exist in reality, usually within a single organisation or organisational grouping (Galliers, 1991).

The aim of the research is to describe the complexities of the security decision making process and rationalise its impact towards the sense of responsibility and ownership of the people managing security, but not to determine the accuracy of a theory. A case study approach has the ability to extract rich and detailed data from complex case settings (Shanks et al, 1993) through data collection techniques such as interviews, observation, questionnaires, and document and text analysis (Shanks, 2002).

Miles and Huberman (Miles and Huberman, 1984) stated that in order for the findings of the research not to be a result of idiosyncrasies of the research setting, multiple cases should be used. In light of this study's area of research, information security, numerous organisations that were approached during the course of data collection declined to participate. Our initial study is therefore based on only two in-depth cases and for this paper due to space limitations we will describe the rich data we collected in one of these organisations.

The company and participants

The company in this case study, Publishing Company (PC), is a market leader within its own segment of the book-publishing industry. Located in Australia, PC is the headquarters for its global operations. Apart from providing strategic direction to its offices around the world, PC also manages most of the writing, editing, publishing, sales and warehousing functions within Australia.

PC is a relatively young company, expanding rapidly to meet the growing demands of the market. With a staff of approximately 400, its 40-member strong IT team contributes to managing a variety of in-house IT operations such as technical support, applications development, research and development as well as hosting the two corporate web sites. The corporate culture of PC was mentioned by the participants to be considered informal and very casual. Communications within the company is open and crosses functional boundaries. PC's structure is fully decentralised, requiring a strong need for coordination and communications to be in place.

With its increasing dependence on IT to support its day-to-day operations like writing, editing, publishing, accounting, sales, research and development, and customer relationship management, combined with its two corporate websites being a key to their business strategy, it has become progressively more important for PC to protect themselves against security attacks and breaches. It falls under the sole responsibility of the IT department for supporting and managing PC's IT infrastructure, intranet, web-hosting and ensuring effective communications with its other global offices around the world.

IT is not only perceived as a support role in PC but also as a business leader throughout the organisation. This is evident through its continuous IT research and development alliances with leading tertiary institutions to explore new and innovative means of improving business through the use of IT.

"The culture is very informal…its founders are very casual in terms of approach and it is very flat in terms of structure…"

"It's not hard to go and book a meeting with the CEO. It's not that I have ever had one, but if I want to, I'm sure the CEO wouldn't mind having a chat with me… upper managers are approachable"

During the preliminary meeting, three participants were selected to be interviewed: the Chief Information Officer (CIO), the IT Operations Manager and the Network Administrator. They were included in this study to illustrate the three different levels of details involved in the security decision making process: namely the strategic (CIO), operational (Operations Manager) and technical considerations (Network Administrator) levels.

The CIO is in charge of aligning IT and its processes to PC's business's goals. As the head of the IT department, the CIO makes all key decisions relating to IT including security. Although the CIO may have the full authority and responsibility for managing IT security in PC, he delegates the responsibility to the various IT staff in his team. In addition, as a member of the executive committee, he is required to know the business and its needs so that he and his IT department are able to support the business and underpin its success.

Who is responsible for managing security?

"IT security? That's me. But I delegate it to a number of people depending on the job. For example intrusion detection is the administrator's job, accountability come with the job. But from a CEO point of view, I am the one responsible"

[CIO]

The IT Operations Manager is responsible for handling escalations from the other technical services staff around the world, and is responsible for the security of the systems controlled by his department. Under his management, the department and other regional offices drafted and enforced the organisation's IT security policies.

On the IT security policy:

"The IT Operations Manager drafted it. He has the responsibility for enforcing it"

[CIO]

"My department and the regional offices overseas came up with the IT security policy…I am responsible for that"

[IT Operations Manager]

The Network Administrator joined PC three years ago as a systems engineer and is an expert at supporting the Windows environment for the office. Through experience and trial and error, he became adept at administering firewalls and is currently responsible for the management of firewalls and intrusion detection systems at PC.

"The Network Administrator is responsible of the management of firewalls"

[CIO]

Who is responsible for managing security?

"I provide the front-end security…we don't have an IT security officer…I'll be the closest thing to it technically, but then again so are a lot of people who do bits of it as well"

[Network Administrator]

The company's Security Governance Profile

The security governance in PC is structured loosely controlled, allowing regional offices, business units and individuals to have the autonomy to make their own decisions with respect to their own roles and responsibilities. Authority structures are designed so as to align to the individuals' level of responsibility, allowing them to make appropriate decisions pertaining to their own job scope and areas of expertise.

"Each office gets to make its own decision, we do not order them to issue compliance, we rely on them to be responsible for their own systems and inform us if a problem is going on… we want to empower people to make decisions"

"…We are careful when a new person starts on a role…we try to gain a feel of their confidence, when there is true confidence, they later are left to make decisions…"

[IT Operations Manager]

PC has an open communications flowing vertically (within the IT department), laterally (across business units) as well as globally (between regional offices) in their security governance. It is highly important for inter-departmental communication to occur during the decision making process. Hence, formalised meetings, teleconferences and workshops involving all relevant personnel managing security are held from a weekly to monthly basis in order for everyone to be informed of the latest issues and resolve problems occurring in the organisation.

"We [IT Operations team] have weekly meeting with the other departments because we are finding that communications is becoming increasingly important towards the business!"

[Network Administrator]

"We have our regular [IT] meetings with the regional offices conducted fortnightly via teleconference…so if they have thought of anything that is a problem for them and that we haven't considered, they could raise them….."

"This is not an organisation that says 'That shall happen on this day', and they ask 'Why?' And we say 'Shut up and do your job!' that doesn't happen here…we tend to go over and discuss things"

[IT Operations Manager]

Decisions are taken very seriously in PC, and as seen from its communications flow, discussions and input are greatly valued in PC's security governance. Whenever security decisions are made, it involves multiple levels of discussions, starting from the technical staff evaluating the solutions technical feasibility, then onto the departmental managers to factor its cost, compatibility and the impact the solution has to the organisation and finally it get passed onto the Global Leadership Team (GLT) comprising all the chief executives where they consider the solution's appropriateness and its impact towards the entire corporate strategy.

On the IT security policy:

"The IT Operations Manager drafted it…it was rolled out to the management team here [local office], who changed and had comments on it and updated it, then it was sent to the Global Leadership Team for viewing"

[CIO]

On drafting the IT Security Policy:

"I came up with this stuff through great discussions with my team over and over again!"

[IT Operations Manager]

PC experiences high levels of social participation in its security governance. Depending on the context, the seriousness of the problem and the consequence the decision has towards the organisation, inputs and suggestions for security decision making involve people ranging from network administrators to the CEO. At PC, social participation can be observed at three different levels: namely at the Global Leadership Team (GLT), local office and the technical levels.

At the GLT level, prior to making any global deployment decisions, all the senior executives are consulted to seek input and feedback. The various department heads provide their input and sound out their concerns with respect to their own expertise before finalising the decision.

At the local office level, managers from various departments including the IT operations department meet on a regular basis to gather input towards security decisions such as the drafting of the IT security policy, implementing of new security software and new applications development. Suggestions and feedback collected are taken into account prior to any decision being made. Feedback is recorded through the form of minutes taken during meetings and later distributed to the various stakeholders.

At the technical level, the network administrators, database server administrators and application developers interact with one another on an informal basis, attempting to understand what projects that everyone are currently involved in so as to get a feel of how each other's current projects might impact their own task of managing security.

Who provides the inputs for security decision making?

"It could be me or the CIO that drive the idea…more often it is a technical person like a systems engineer…because of their skills they can understand the level of appropriation"

[IT Operations Manager]

"…our manager relies on me and the Unix guys…he relies on our evaluation of products and technologies, and in the end he wouldn't put forward something even if he feels personally strong about it, we wouldn't put forward something unless we all agree on it"

[Network Administrator]

On the drafting of the IT security policy:

"It was done over a period of 3-4 months and we had a meeting once a week. The IT Operations Manager would go and write a section of it or actually sit with us and get our thoughts and then write a section of it"

"We were involved in the technical sections…we were involved fairly strongly in it!"

[Network Administrator]

The company's Security Culture

It is observed that responsibility is delegated together with the job in PC. The participants managing security were given the appropriate level of authority with respect to their responsibilities to act or make decisions, resulting in a strong sense of ownership assumed by the participants. Depending on the level of impact, the decision would be made by the person in charge of that particular area. In addition, PC takes a lot of effort in ensuring that the roles and responsibilities of the stakeholders are scoped in a way that empowers them to make decisions.

Who is responsible for managing security?

"IT Security? Me. But I delegate it to a number of people depending on the job. For example, intrusion detection is the Network Administrator's job…accountability comes with the job"

"But if the administrator thinks that this brand of devices is no longer the right firewall for us, then he would raise it to his manager and his manager would probably make that decision but the responsibility would sit with the administrator to say this is what you should do"

[CIO]

In addition, there was a common notion observed from the participants interviewed within PC to trust and rely on one another for doing their respective tasks of managing security pertaining to their individual job scope.

"There would be multiple levels of responsibility. I am responsible for the areas in my job description, for some of the staff that report to me, I am not aware of the things to the level of detail that they are…I have to rely on them to make certain decisions themselves…it's all a matter of what happens at what level…"

[IT Operations Manager]

Another common notion observed in PC was that the participants interviewed all displayed a strong sense of ownership over security. This was illustrated through the observation that all of participations were instructed to list areas of which they wanted improve with regards to security. At the end of the interview, the list was matched with their individual responsibilities; it was observed in all the participants' responses that their listed areas fell directly under their personal jurisdiction indicating that they felt accountable for managing security.

On are there any security decisions made outside the IT department?

> *"Yes…Finance or HR has access to certain file areas on some servers they set permissions to. So if a finance manager wants to give a freelancer or contractor access to these files, IT will act upon that request, IT will not make the decision that this person should have access or this person should not have access. "*
>
> ***[CIO]***

Lastly, it was a common consensus among all the participants that the managing of security did not fall under the sole responsibility of one person, role or department. It was highlighted in the interviews that there was a common understanding that the responsibility of managing security was shared throughout the organisation.

> *"There is distributed responsibility…IT manages the integrity of the information secure-ness as long as the rules are set properly…if you're not allowed to access this information, IT will ensure that. Now it is up to the business owners to decide whether a not to allow access of the information to you, It's their call!!"*
>
> ***[CIO]***

Who is responsible for managing security?

> *"I think it's a bit of everyone…it's the local tech guys for the file servers, the Linux guys for the Linux accounts, applications development team for the backend code and it's up to me to provide the front-end security…it's really a shared responsibility"*
>
> ***[Network Administrator]***

> *"In terms of responsibility, it is shared; it comes up to each department that has control, knowledge or whatever over that particular resource"*
>
> ***[IT Operations Manager]***

DISCUSSION AND CONCLUSIONS

This study explores the specific elements of security governance that influence the sense of responsibility and ownership IT security personnel possess over security, and further explains how the varying degrees of social participation in security governance might have an impact on their sense of responsibility and ownership over security.

For this study, we used Chia's security culture framework, in particular the dimension of 'control, coordination and responsibility'. This dimension highlights issues relating back to the degree of control which varies in organisations between two extremes, tight and loose control. When control is 'tight', it would be characterised by centralised decision making where the decision making authority concerning strategies, systems development and infrastructure deployment resides primarily with corporate management. This centralised decision making is usually supplemented with strict and formal rules that need to be followed. As a result the tightly controlled environment assists in guiding the behaviour of the majority (Chia et al, 2002), leading to greater efficiencies and standardisation throughout the organisation (Brown & Magill, 1998). When control is 'loose', it would be characterised by decentralised decision making, where the responsibilities and decision making authorities are delegated to the relevant employees, such as employees in the IT divisions or business units (Vitale, 2001). This decentralisation results in flexibility and autonomy of workers (Detert et al, 2000).

In the case reported in this paper, the organisation clearly has a decentralised decision making structure, which should increase the organisations' agility (Brown, 1997; Vitale, 2001) and adaptability to the dynamic changing environment (Peterson et al, 2000). However, as we discussed, it is crucial in a decentralised decision making environment that security governance provides adequate mechanisms to enable managers to allocate responsibilities and accountabilities for security. Our analysis shows that PC successfully delegated sufficient authority to the people implementing and managing information security and has empowered them to make appropriate decisions to protect PC's critical assets.

Chia (Chia et al, 2002) further asserts that, in a good security culture, employees not only feel responsible, but also have a sense of ownership for security. This is particularly important in the context of decentralised decision making, where Peterson refers to this in his discussion of social participation. In security governance, social participation does refer to the degree to which feedback from the people implementing security is valued and taken into account towards decision making in information security. While stringent control processes and centralised decision making may inhibit social participation, it is suggested that in a decentralised environment social participation should increase employees' sense of ownership.

As the quotes in the previous section show, PC's security governance is primarily structured around active social participation and communications. This can be seen through the formalised processes such as weekly meetings, teleconferences, discussions and workshops embedded within the PC's organisational structure which involve a variety of technical staff, managers, business leaders and chief executives during the security decision making process. Inputs and suggestions provided by the people managing security in PC are recorded during the security decision making process and taken into account towards the final decision. As a result, through this active participation and communication between stakeholders in PC's security governance, there is common consensus within PC that managing information security is a shared responsibility throughout the organisation.

Although this study has found social participation to be the major component in security governance to influence the levels of responsibility and sense of ownership that IT security personnel have over the managing of security in their organisation, the presence of social participation activities alone may not be sufficient. Social Participation in PC is heavily supported by formalised processes. Without this support, social participation may not have been that successful in empowering the security staff's decision making. Hence, we believe that there may be a need to formalise the social participation activities into the organisational structure in order to create this increased responsibility and stronger sense of ownership that people have over security.

REFERENCES

Adams, A., and Sasse, M.A. (1999) 'Users are not the enemy' Communications of the ACM, 42(12): 41-46.

Blair, M.M. (1995) 'Ownership and Control: Rethinking Corporate Governance for the Twenty-first Century' Washington DC: Brooking Institute.

Breidenbach, S. (2000) 'How Secure Are You?" InformationWeek, (800):71-78.

Broadbent, M. (2002) 'CIO Futures – Lead with Effective Governance' ICA 36th Conference, Singapore, October 2002.

Broadbent, M. (2003) 'Effective IT Governance by Design' Gartner Inc.

Brown, C.V. (1997) 'Examining the Emergence of Hybrid IS Governance Solutions: Evidence from a Single Case Site' Information Systems Research, 8(1): 69-94.

Brown, C.V, and Magill, S.L. (1998) 'Reconceptualizing the Context-Design Issue for the Information Systems Function' Organisational Science, 9(2): 176-194.

Chia, P. Maynard, S., and Ruighaver, A.B. (2002) 'Understanding Organisational Security Culture' Sixth Pacific Asia Conference on Information Systems, Tokyo, Japan, 2-3 September 2002.

Chia, P. Maynard, S., and Ruighaver, A.B. (2003) 'Understanding Organisational Security Culture' in Information Systems: The Challenges of Theory and Practice, Hunter, M. G. and Dhanda, K. K. (eds), Information Institute, Las Vegas, USA, pages 335 - 365.

Dallas, S. (2002) 'Six IT Governance Rules to Boost IT and User Credibility' Gartner Inc.

Dallas, S. (2004) 'IT Governance Requires Decision making Guidelines' Gartner Inc.

Dallas, S. and Bell, M. (2004) 'The Need for IT Governance: Now More Than Ever' Gartner Inc.

Detert, J., Schroeder, R. and Mauriel J. (2000) 'A framework for linking culture and improvement initiatives in organizations' The academy of management review 25(4): 850-863.

Galliers, R.D. (1991) 'Choosing Information Systems Research Approaches' In: H-E Nissen, H.K. Klein, and R.A. Hirschheim (eds.) Information Systems Research: Contemporary Approaches and Emergent Traditions, Proceedings IFIP TC8/WC8.2 Working Conference, North-Holland.

Korac-Kakabadse, N. and Kakabadse, A. (2001) 'IS/IT Governance: Need For an Integrated Model' Corporate Governance 1(4): 9-11.

Martins, A. and Eloff, J. (2002) 'Information Security Culture' IFIP TC11 International Conference on Information Security, Cairo, Egypt, 7- 9 May 2002.

Miles, M.B. and Huberman, A.M. (1984) 'Qualitative Data Analysis: A Sourcebook of New Methods' Sage Publications.

Neuman, W.L. (2003) 'Social Research Methods – Qualitative and Quantitative Approaches' 5th ed. Allyn and Bacon.

Nosworthy, J. (2000) 'Implementing Information Security in the 21st Century – Do you have the Balancing Factors?' Computers and Security 19(4): 337-347.

Peterson, R. R., O.Callaghan, R., and Ribbers, P. M. A. (2000) 'Information Technology Governance by Design: Investigating Hybrid Configurations and Integration Mechanisms' Proceedings of the 20th International Conference on Information Systems, Brisbane, Australia, 10-13 December 2000.

Peterson, R.R, Parker, M., and Ribbers P. (2002) 'Information Technology Governance Processes under environmental dynamism: Investigating competing theories of decision making and knowledge sharing' 23rd Annual International Conference on Information Systems, Barcelona, Spain, 15-18th December 2002.

Sambamurthy, V., and Zmud, R.W. (1999) 'Arrangements for Information technology governance: a theory of multiple contingencies' MIS Quarterly, 23(2): 261-280.

Schlienger, T. and S. Teufel (2002) 'Information Security Culture - The Socio-Cultural Dimension in Information Security Management.' IFIP TC11 International Conference on Information Security, Cairo, Egypt, 7-9 May 2002.

Schlienger, T. and S. Teufel (2003) 'Analysing Information Security Culture: Increased Trust by an Appropriate Information Security Culture' 14th International Conference on Database and Expert Systems Applications (DEXA 2003), Prague, Czech Republic, September 2003.

Schlienger, T. and S. Teufel (2003) 'Information Security Culture - From Analysis to Change.' Proceedings of ISSA 2003, Johannesburg, South Africa, 9-11 July 2003.

Shanks, G., Rouse, A. and Arnott, D. (1993) 'A Review of Approaches to Research and Scholarship in Information Systems' Proceedings. 4th Australian Conference on Information Systems, Brisbane, Australia, September 1993.

Shanks, G. (2002) 'Guidelines for Conducting Positivist Case Study Research in Information Systems Research' Australian Journal of Information Systems, December, 76-85.

Vitale, M. (2001) 'The dot.com Legacy: Governing IT on Internet Time' Working paper, Information Systems Research Center, University of Houston.

Von Solms, B. (2000) 'Information Security – The Third Wave?' Computers and security 19(7): 615 – 620.

Von Solms, B. (2001). 'Information security – a multidimensional discipline' Computers & Security, 20(6): 504 – 508.

Weill, P. and Woodham, R. (2002) 'Don't Lead, Govern: Implementing effective IT governance' MIT Sloan CISR Working Paper no 326, April 2002.

COPYRIGHT