Information Security Governance: When Compliance Becomes More Important than Security

Terence C.C. Tan [1], Anthonie B. Ruighaver[2], and Atif Ahmad[1]

[1] Department of Information Systems, The University of Melbourne, Melbourne, Australia
[2] School of Information Systems, Deakin University, Melbourne, Australia
terence.tan@defence.gov.au, tobias@deakin.edu.au, atif@unimelb.edu.au

Abstract. Current security governance is often based on a centralized decision making model and still uses an ineffective 20th century risk management approach to security. This approach is relatively simple to manage since it needs almost no security governance below the top enterprise level where most decisions are made. However, while there is a role for more corporate governance, new regulations, and improved codes of best practice to address current weak organizational security practices, this may not be sufficient in the current dynamic security environment. Organizational information security must adapt to changing conditions by extending security governance to middle management as well as system/network administrators. Unfortunately the lack of clear business security objectives and strategies at the business unit level is likely to result in a compliance culture, where those responsible for implementing information security are more interested in complying with organizational standards and policies than improving security itself.

Keywords: Security culture, decentralized decision making, security strategic context, business security strategies.

1 Introduction

In the current dynamic information security environment, simply implementing controls and state-of-the-art security is no longer adequate. Many organizations are still basing their information security on the old ISO 17799 security standard and as a result they are often struggling to cope with the increase in threats and vulnerabilities. The question is whether new security standards introduced over the past decade are likely to change this situation.

While the new 27000 series of standards [1] have introduced a lifecycle model to security management, the emphasis is still on the controls needed in information security. Little information is given about security objectives or on potential strategies to implement these objectives. Neither are there any suggestions, outside of a mention of risk analysis, on how organizations should develop security objectives and strategies as part of their security governance process. While this emphasis on

K. Rannenberg, V. Varadharajan, and C. Weber (Eds.): SEC 2010, IFIP AICT 330, pp. 55–67, 2010.

controls worked well before in a reasonably static security environment, in today's ever changing security environment, organizations will need to encourage and promote innovation in their approach to security management – going beyond what is prescribed in the current standards [2].

Corporate security governance has primarily to do with how the board of directors and executives address security management issues such as "setting the responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly" [3].

Understanding how certain aspects or 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 not wasted. The ability to make well-informed decisions about the many important components of governing for enterprise security, such as adjusting organizational structure, designating roles and responsibilities, allocating resources, managing risks, measuring results, and gauging the adequacy of security audits and reviews is crucial. Our research [4], [5] indicates that efforts to improve decision making in these areas currently is mostly focused on corporate security governance.

Unfortunately, this current 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, we will refer to this level of governance as enterprise-wide security governance, or just security governance, whilst referring to corporate security governance when discussing issues related to board level governance issues.

Hence, while there is some evidence of reasonable efforts to develop corporate security governance guidelines and frameworks, at the moment, there is little known about enterprise-wide security governance. In particular, about how organizations develop their security strategic context, how they decide on security objectives and strategies and how they use these to develop their policies and security infrastructures [6]. The current emphasis at the coal face on implementing policies, without any guidance on what objectives these policies aim to achieve or what strategies the organization aims to implement, means that most organizations are continuing to struggle in their security efforts. Considering this lack of guidance for the key people who have to ensure that the organization's information assets are adequately secured, it is not surprising that our studies have found they will often be more concerned with compliance than with information security itself.

This paper reports on one of several case studies conducted in the area of enterprise-wide security governance. This specific case examines the information security function in a business unit of a large organization with centralized security management - which prescribes what security policies and controls will need to be implemented at the coalface. This paper will discuss several of the major issues related to 'enterprise wide security governance' that we discovered in our in-depth case studies as well as how these issues affect the security strategic context for this particular organization.

2 Historical Background

As the environment an organization operates in changes continuously, threats are changing too. Organizations today face more sophisticated attacks than in the past, both internally and externally. Defenses against such attacks are the bread and butter of security professionals. And yet, high-profile security breaches continue to take place [7], [8]. Experts agree one cause is narrow thinking on the part of security executives [9], [10], [11]. For example, in mid June (2006), New York based AIG acknowledged the theft of the personal data of almost a million people. Firewalls and intrusion detection technology were not the deficiency – thieves simply broke into a regional office and physically carried off a server, along with a laptop.

Previous studies [3], [12] indicate that organizations are now beginning to realize the importance of having to prepare for these increased security risks in an appropriate and effective manner. An interesting discovery from these studies was that despite this renewed emphasis on strategic security planning, the majority of organizations nevertheless are continuing to simply do "what everyone else is doing" [13], [14]. We believe this approach is indicative of a severe problem with an organization's strategic security planning.

2.1 Corporate Governance

The purpose of corporate governance to achieve sustained financial results [15], has been predominantly achieved by means of a focus on financial management, so much so that corporate governance was virtually synonymous with the measuring, monitoring and reporting of the financial condition of the enterprise [16].

However, the landscape upon which business is conducted has changed significantly. Traditionally, corporate governance was the responsibility of the board. In today's complex organizations, where the corporation's "value constellation" is made up of a constantly changing set of entities, governance activities must be extended both down into and outside of the organization to include an expanded role for internal staff at all levels. External entities [15], [17]. IT and security auditors must also be added to the pool of interested parties.

Literatures on Security Governance advocate the idea of incorporating Security Governance as a subset of Corporate Governance. An example is laid out by the Corporate Governance Task Force in their 2004 report entitled "Information Security Governance – A Call To Action": "*…the private sector should incorporate information security into its corporate governance efforts.*" [18].

And again from a statement by eSecure: "*(IT) Security is part of the business and it is imperative to assign responsibility for managing information security to the Board level as information is a valuable and critical corporate asset.*" [19].

The report further argues that if organizations are serious in their efforts to secure their information assets, then "executives must make information security an integral part of core business operations." The report suggests the best way to accomplish this goal is to highlight it as part of the existing internal controls and policies that constitute Corporate Governance. Furthermore, the report provides a number of recommendations and even what they have termed, an "Information Security

Governance Framework," to assist organizations in incorporating Information Security (InfoSec) into their Corporate Governance processes.

From these discussions, two possibilities are revealed. Firstly, what has been done is still not enough to protect organizations. There has been much literature written and much research done on implementing Information Security Policies (ISPs), on cultivating a security culture within organizations, on putting in place technical deterrents and counter measures such as firewalls, password protection and so on. However, these approaches still appear to be insufficient in protecting organizations. Secondly, organizations may have reached a stalemate when considering security and they are simply doing "what everyone else is doing." Organizations are thus baffled, and faced with the question "what must we now do to protect ourselves?

3 Enterprise-Wide Security Governance

The field of InfoSec is a complex and critical component to an organization's success. A strategic approach to InfoSec 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, behaviors, and adaptive solutions that map to business requirements [20]. As such, those responsible are not just senior management but also middle management and others involved with the implementation of security strategies (those at the coalface), and they will need a governance framework for making informed decisions about Information Security. 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 organizational issues, it is plausible to suggest that improving Security Governance throughout the enterprise may be the key to improving the level of security in organizations.

3.1 Frameworks

This study focuses on enterprise-wide security governance to improve decision making at the 'coal face'. It is concerned with the people that implement security and about how they go about making decisions with or without guidance from the organization.

In order for decision makers to make quality decisions, appropriate guidance must be effectively communicated to them in the form of the organization's security strategic context [6], that is through mission statements, objectives, strategies, tactics and so on.

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. [21], [22], argued 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*" Developing security strategic context exclusively at the top management level is likely to result in a lack of diversity across the security strategic context. Good security strategic context needs to be developed by different people/committees at different levels of the organization, similar to the development of IT strategic context [23], [24].

To ensure a comprehensive study of security governance, the authors first developed and tested a security governance research "framework" that identifies five major aspects of security governance, namely, decision making rights, input rights, experience and culture, accountability, and strategic context [12].

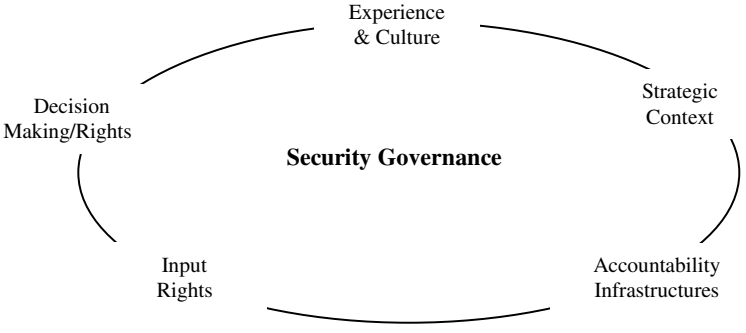

Fig. 1. Security Governance Framework

Exploring each of these aspects of governance in depth is an enormous task therefore a decision was made to focus our research particularly on one aspect of security governance - security strategic context. Strategic context was identified as a key component of successful IT governance [25], thus a decision maker at the coal face is not likely to make good decisions about security without a decent knowledge of the organization's security strategic context either.

To guide our research on how organizations develop their security strategic context we adopted a strategic context model from IT governance [26], [27] and expanded that model into a two-dimensional 'Scope of security strategic context' framework that covers both depth and coverage of the security strategic context.

Dimension 1 – Depth of Security Strategic Context

This dimension aims to clarify how extensive the organization's strategic context is in terms of strategic, tactical and operational aspects by adapting the 5 domains from Broadbent and Weill's [26] original IT strategic context model.

- Security Objectives (mission statements) – High-level statements that inform the organization about how security will be used to create business value and how to protect it. Objectives clarify focus and provide a frame of reference for every important aspect of security activity, from incident handling to disaster recovery, information protection to user functionality.
- Security infrastructure – Strategies employed to build shared and standardized security services/beliefs/ideals across the organization (Strategic Security Policies, etc) and the operationalization (implementation) of those strategies.
- Security architecture – Choices that guide the organization in satisfying security needs (decision/input rights)
- Security application needs – Applications that need to be acquired or built. For example, VPNs, firewalls, etc.

- Security investment and prioritization – Regulates the process of security investment, that is, where it should be focused, the procedures for progressing initiatives, their justification, approval and accountability.

Dimension 2 – Coverage of Security Strategic Context
This dimension was added to the original one-dimensional IT model. It covers how 'broadly defined' an organization's security strategic context is with regard to the different aspects of security.

In constructing this second dimension, an extensive examination of the general literature on Information Security (InfoSec) was performed [5]. This included a review of international standards and guidelines such as the OECD, COSO, ITIL, ISO and COBIT. The resulting security areas currently included in our framework are:

- Network Security – This refers to the controls/actions that secure the corporate network, prevent unauthorized access to systems and data, and ensure data integrity and availability over the network.
- Systems and Data Security – Is about the protection of the information (availability, integrity, confidentiality, authenticity and validity) and handling of information. Includes user account management, monitoring and revocation processes, etc.
- Physical Security – This concerns the protection against human intrusions and natural disasters such as fire, water leakage and other environmental failures.
- Personnel Security – Includes such aspects as hiring policies, termination practices and access controls.
- Operations Security – Is concerned with business continuity, ensuring the integrity and availability of crucial data after a disaster or other disruptions. For example, protecting stored financial reporting data so that business transactions that continue during downtime are properly accounted for.
- Miscellaneous Security aspects. – Acknowledging that there most likely will be other areas organizations will focus their security on that don't fall within the 5 aspects of security above (Eg. a focus on eCrime, and incident handling).

4 The Case Study

The case study reported in this paper took place in an Asian subsidiary of a large international corporation I.T US Inc. For this paper we will call this subsidiary ITUM.

I.T US Inc. (ITU) is a world player in Information Technology. Worldwide ITU operates in over 150 countries. Being part of a large multinational, ITUM's 'security' benefits from high availability of resources and separate funding. As is not unusual in large international organizations, ITU maintains a separate and independent corporate security department. This corporate security department, having been delegated the responsibility of security for ITU and its world wide units, is staffed by *"security specialists"*. Their job is to maintain, develop and distribute security policies, procedures, standards and guidelines for the entire ITU organization.

The main participants involved in the ITUM study were Mr. A the IT Manager, Mr. B the Security Manager and Ms. C the IT Specialist. From a security perspective, all three participants agree that security is key in ITUM's operations.

"Security? Definitely, definitely important." (Mr. A, IT Manager)
"…you must have security in place to protect your interest…."
(Mr. B, Security Manager)
"Security is a mandatory thing..." (Ms. C, IT Specialist)

Overall, Mr. A is responsible for ensuring that the organization's IT unit operates smoothly. Since ITUM relies heavily on IT for many of its business functions, this puts additional pressures on Mr. A to ensure that the organization's systems, networks and so on, are available (up-time of the server), consistent and reliable (integrity). This is how Mr. A describes his responsibilities: -

"…you know how critical information is to us…we have that network connection and it is crucial that it works."

Their operational perspectives reflect an emphasis on compliance, from ensuring that corporate guidelines are followed to compliance with both formal and corporate security standards (mandated from the corporate security department). Mr. A feels that the organization is secure, and he is only concerned about ensuring that his systems, networks and infrastructures meet the required standards set down by Corporate.

For Mr. B, the Security Manager, his portfolios include site security (internal and external security), Occupational Health and Safety (OHS) and Program Security. This makes him responsible for implementing security strategies and tactics within ITUM which includes, *"…counseling the management, to help them, to advice them with respect to the company's security policies"*. Essentially, security awareness and security education.

As Mr. B describes it, his security/awareness programs are to make sure that the security risk for ITUM is manageable and *"…to avoid any untoward situations."*

"I do presentations or at times I will send a memo across the organization about security, about things that happen, about security tips, prevention…"

Mr. B too has a high reliance and confidence in ITUM's corporate security standards and guidelines. His main role is to implement security policies funneled down to him from corporate – a bias for compliance.

Because of ITUM's governance approach, Mr. B has limited involvement in the development of high level security strategies and policies. His exact involvement is confined only to checking that the corporate security policies are valid for the local circumstances and ensuring that ITUM is compliant to the Corporate standards. Hence his understanding of the security strategic context is sorely limited.

Ms. C has an IT background and is involved in project management, asset management and process architecture. On the process side, Ms. C plans, develops and implements IT security processes in ITUM. Similar to Mr. A and Mr. B, she believes that ITUM's security is pretty good.

Although not directly involved with the corporate security group, as a process architect, Ms. C will *"design IT security processes,"* following those corporate guidelines, like Mr. B. It is here that she has picked up her awareness about security.

Ms. C's ability to understand and comprehend the security strategic context is limited too. Her focus is primarily and strictly on adhering to the specified corporate standards, guidelines and policies (i.e. compliance). When asked her thoughts on abiding by standards/audits, Ms. C replied: -

"We cannot afford to fail in any audit. Passing the audit is mandatory for us. Compliance is a very, very high focus for us…all I know is we do adhere to standards"

5 Case Analysis and Discussion

Using the strategic frameworks discussed, an empirical study was conducted investigating Enterprise-wide Security Governance in both large and medium sized organizations. In order to analyze this ITUM case a general discussion of our findings across all participating organizations is needed. The design of the studies involved multiple sources of evidence, collected in a structured manner.

With the Security Governance and Security Strategic Context research frameworks verified for its comprehensiveness in previous studies [4], our current case studies concentrated on Security Governance at the coalface. A number of interesting lessons were learnt and briefly they are:-

1. *Diversity of decision-making is often lacking*. Decision makers were found to be making decisions on their own without inputs from others within or from other business units. For some organizations, even with other inputs, as their governance structure did not encourage it, advice given was never taken on.
2. *Corporate (Executive) Level mission statements are vague and provide little guidance* for those responsible for security at the enterprise wide level. This is particularly evident in ITUM where corporate level guidance did not encourage any understanding of objectives or strategies but unconditional 'replication' of standards – leading to a culture of compliance and limited depth and understanding of security strategic context. However, in another organization, the lack of corporate level mission statements led to good depth in security but limited to only the areas that those responsible for security were familiar with and experienced in. This 'silo effect' resulted in the organization's security context being narrow and lacking coverage.
3. Security Governance and IT Governance although closely related, are separate entities. Security Governance is found to be an add-on to the business and follows an IT Governance approach, that is, a bottoms up approach to security. Instead, it should be a driver.

These three themes will now be discussed independently in detail for ITUM.

5.1 Limited Diversity in Decision Making

At ITUM, almost all decisions about the security strategic context have been decided upon by the corporate security department at the executive level.

"We have globally this dedicated security team who just focuses on doing policies and standards."
(Ms. C, IT Specialist)

The decisions of ITU corporate security are communicated to the enterprise level via policies, procedures and standards, not objectives or strategies. As Mr. B, describes, *"Throughout the whole ITU organization, in every country, we follow the same template, the same procedures, and the same policies."*

This idea of security being a 'template' (i.e. a standardized prescription) that is applied to any and all situations with only slight modifications allowed is likely to cause those involved to perceive security as an A-Z checklist of things that need to be done. As was noticeable during the analysis, very little thought or innovativeness is evident for security at the enterprise wide level. Any decision-making regarding security made at this level are low-level simplistic decisions that revolve predominantly around compliance, controls and passing audits.

"Our audits as well help us make sure people are making the right decisions."
(Mr. A, IT Manager)

Although the strategic decisions are being made at high levels with very little to no communication with other functional levels of the organization, it was hoped that these decisions are made with inputs from various people from affected units of the organization. Unfortunately, this was not the case at ITUM, with all strategic decisions being made by the *"dedicated security team…they're very specialized"* (Ms. C, IT Specialist).

"I get guidelines. I get standards. It's all been prepared by HQ. We get statements from the business to tell us what we should and should not do."
(Mr. A, IT Manager)

At ITUM this situation has led to isolation of the decision makers and therefore reflects a lack of diversity in their decisions.

5.2 Corporate Level Security Mission Statements Provide Little Guidance

It is evident that good coverage of security exists at ITUM (e.g. all areas identified by the ISO Standard are covered). Unfortunately, we found a limited depth in security strategic context in each of these areas

Exploring deeper, we see that most security related activities at ITUM are performed at the 'Security Architecture' and 'Security Application(s) Needed' level with only a few activities being performed at the 'Security Strategies & Infrastructure' level. For instance, at the 'Security Architecture' level, authentication and control of user access, identification and verification of users, monitoring of access control are all performed; security perimeters are defined; user responsibilities are clearly outlined; segregation of duties and routine backup checks are performed;

and so on. At the 'Security Application(s) Needed' level, a diverse range of hardware, software and policies exists such as firewalls, proxy, monitoring software, anti-virus, acceptable use policies, education and training, and so on.

These results are indicative of extremely good coverage of security across the board but have limited depth particularly in the areas of 'Network Security', 'Systems Security' and 'Physical & Environmental Security'.

It is also noted that while some 'Security Objectives' are obvious or known to participants many others are not. However, the objectives known by participants such as "protection from virus attacks" and "protect assets & information in those assets" are of such simplicity and generality in nature that you have to question the quality of those objectives to function as high-level statements that inform the organization about how security will be used to create business value and to protect it.

Furthermore, it is not clear whether those objectives mentioned by the participants were communicated to them by higher management, or just reflect what they believe they are doing. Security Objectives are meant to clarify focus and provide a frame of reference for every important aspect of security activity. It is not clear whether this has been done. From the participant's point of view, when asked the question, "Does your organization have mission statements in place with regards to security?" their responses were:

"Yes we do, I have seen them, I cannot tell you exactly what they are…we do have a mission, I've seen that but I don't really know what they are."
(Ms. C, IT Specialist)

"I believe the Security (dept) at the head office do have mission statements but I'm not aware of that right now but I believe that they have."
(Mr. A, IT Manager)

5.3 A Bottoms Up Approach to Security Strategic Context Development.

Many organizations see Security Governance as just a small part of Corporate Governance. While IT Governance has become a recognized focus area in larger organizations, these organizations often won't give Security Governance the same attention. Hence, organizations still need to realize that just like IT, the field of Information Security is a complex and critical component to their organization'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 coalface), and they will similarly need a governance framework for making informed decisions about Information Security.

At ITUM, apart from the approach of implementing the given standards and requiring business units to 'pass' audits, security is an add-on action, and not a driver at all. As Mr. A the IT Manager describes,

"If I'm putting in any new IT infrastructure I just have to make sure the IT security piece of it is adhered to…"

As ITUM did not receive any information on the organization's security strategies it used a bottoms up approach to develop its own objectives and strategies based on compliance.

This bottoms-up approach in the development of business strategies is common in IT governance where applications needs and the IT architectures necessary to support these applications will lead to the development of objectives and businesses strategies at executive levels to support these lower levels of the IT strategic context. The question arises if a similar bottoms-up approach is really the way to develop a strategic context in security governance. On the other hand, research on possible top-down approaches to develop a security strategic context is still scarce, but an attempt to develop a strategic context from the top-down is described in a recent paper on Ubiquitous security [2].

6 Conclusions

The case study discussed in this paper has revealed a number of interesting and valuable lessons about security governance. In our experience these findings can be generalized to many other large organizations that have a centralized security function.

Most current information and academic papers on security governance at the enterprise wide level unfortunately promote a centralized decision making model based on, in our experience, an ineffective and old-fashioned risk management approach to security. The old-fashioned centralized approach is relatively simple to manage: It needs almost no security governance enterprise wide (business unit or coalface 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 organization's security posture, making it difficult for the organization to respond quickly/timely to changes in its security environment.

Further, the lack of input from people at the coalface in the predominantly centralized security-planning ethos has stifled innovation in security.

More significantly, with the centralized security philosophy, the same employees or committee(s) that decide on security infrastructure and applications also decide on (business) objectives and security strategies. Hence the rationale is that there is no need to communicate those objectives and strategies to the rest of the organization. While it may be unintentional, the organization's security culture now has evolved towards a compliance culture where compliance to corporate guidelines has become more important than improving security.

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.

References

1. Humphreys, T.: How to implement an ISO/IEC 27001 information security management system. ISO Management Systems, 40–44 (2006), http://www.iso.org
2. Ruighaver, A.B.: Organisational Security Requirements: An agile approach to Ubiquitous Information Security. In: Proceedings of the 6th Australian Security management Conference, Australia (2008)
3. IT Governance Institute: Information Security Governance: Guidance for Boards of Directors and Executive Management 2nd edn. (2006), http://www.itgi.org
4. Tan, T.C.C., Ruighaver, A.B., Ahmad, A.: Incident Handling: Where the Need for Planning is often not Recognised. In: Proceedings of the 1st Australian Computer Network, Information & Forensics Conference, Australia (2003)
5. Tan, T.C.C., Ruighaver, A.B.: Understanding the Scope of Strategic Context in Security Governance, In: Proceedings of the 2005 IT Governance Int. Conf., New Zealand (2005)
6. Tan, T.C.C., Ruighaver, A.B.: A Framework for investigating the development of Security Strategic Context in Organisations. In: Proceedings of the 6th Aus Information Warfare & Security Conference: Protecting the Australian Homeland, Australia, pp. 216–226 (2005)
7. Computer Security Institute and FBI Survey, Results of CSI/FBI Computer Crime and Security Survey (2003), http://www.gocsi.com
8. AusCERT, Australian High Tech Crime Centre, AFP, NSW Police, NT Police, Queensland Police, SA Police, Tas Police, Vic Police, WA Police: 2004 Australian Computer Crime and Security Survey. Australian Computer Emergency Response Team (2004)
9. Wright, P.D., Liberatore, M.J., Nydick, R.L.: A survey of operations research models and applications in Homeland Security. Interfaces 36(6), 514–529 (2006)
10. Theunissen, D.: Corporate Incident Handling Guidelines. The SANS Institute (2001), http://rr.sans.org/incident/corp_guide.php
11. Pasikowski, G.T.: Prosecution: A subset of Incident Response Procedures. The SANS Institute (2001), http://rr.sans.org/incident/prosecution.php
12. Tan, T.C.C., Ruighaver, A.B.: Developing a framework for understanding Security Governance. In: Proceedings of the 2nd Australian Information Security Management Conference, Australia (2004)
13. D'Amico, E.: Cyber Crime is on the rise, but let's keep it quiet. Chemical Week 164(17), 24–27 (2002)
14. Braid, M.: Collecting Electronic Evidence after a System Compromise. In: Australian Computer Emergency Response Team, AusCert (2001), http://www.auscert.org.au
15. Pultorak, D: IT Governance: Toward a Unified Framework Linked to and Driven by Corporate Governance. CIO Wisdom II, Prentice Hall Ptr. (2005)
16. Kaplan, R.S., Norton, D.P.: The Balanced Scorecard: Translating Strategy Into Action. Harvard Business School Press (1996)
17. McLane, G: IT Governance and its Impact on IT Mngt. MA dissertation, Sydney (2003)
18. Corporate Governance Task Force: Information Security Governance – A Call to Action. National Cyber Security Summit Task Force, USA (2004)
19. eSecure: Time to elevate IT Security to the Boardroom, South Africa (2000)
20. Proctor, P.: Sarbanes-Oxley security and risk controls: When is enough enough? Infusion: Security & Risk Strategies (2004), http://www.metagroup.com

21. Peterson, R., O'Callaghan, R., Ribbers, P.M.A.: Information Technology Governance by Design: Investigating Hybrid Configurations and Integration Mechanisms. In: Proceedings of the 20th International Conference on Information Systems, Australia (2000)
22. Ribbers, P.M.A., Peterson, R.R., Marylin, M.P.: Designing Information Technology governance processes: Diagnosing contemporary practices and competing theories. In: Proceedings of the 35th Hawaii International Conference on System Sciences, pp. 1–12. IEEE Computer Society, Los Alamitos (2002)
23. Weill, P., Woodham, R.: Don't Just Lead, Govern: Implementing Effective IT Governance, Massachusetts Institute of Technology, Cambridge, Massachusetts (2002)
24. Vitale, M.: The dot.com Legacy: Governing IT on Internet Time. Information Systems Research Center, University of Houston (2001)
25. Weill, P., Ross, J.W.: IT Governance: How Top Performers Manage IT Decision Rights for Superior Results. Harvard Business School Press, Boston
26. Broadbent, M., Weill, P.: Management by Maxim: Creating Business Driven Information Technology Infrastructures. Melbourne Business School, University of Melbourne (1996)
27. Broadbent, M.: CIO Futures – Lead With Effective Governance. ICA 36th Conference, Singapore (2002)