Information Security Control Centralization and IT Governance for Enterprises

Rosslin John Robles, Ji-Yeu Park, Tai-hoon Kim
School of Multimedia, Hannam University, Daejeon, Korea
rosslin_john@yahoo.com, taihoonn@hannam.ac.kr

Abstract

Information Technology (IT) governance is important in every Enterprise to ensure the execution of the firm's security policies and procedures. It is a subset discipline of Corporate Governance focused on information technology (IT) systems and their performance and risk management. This paper sights current some problems. It also presents the framework for ensuring that the organization's policies are implemented over time. Since most of these policies require human involvement, the goals are met only if human activities can be influenced and monitored. This is the challenge to IT governance. One issue is to which IT security controls should be centralized or decentralized.

Keywords: IT Governance, IS Centralization, Security Management, IT Security

1. Background

Information system security management goals can only be achieved if the policies and procedures are complete, accurate, available, and ultimately executed or put into action. Organizations must be conscious of the hazards associated with the diffusion of technology throughout the firm and must reflect this awareness through the purposeful creation of policy. The goals of IT security are to ensure the confidentiality, integrity and the availability of data within a system. The data should be accurate and available to the appropriate people, when they need it, and in the appropriate condition. Perfect security is not feasible — instead IT security managers strive to provide a level of assurance consistent with the value of the data they are asked to protect. It is within their structures and governance procedures that organizations are able to solve the issues of responsibility, accountability, and coordination toward the achievement of their purpose and goals.

As organizations evolve to position themselves appropriately within their domains of interest, their governance posture evolves. These changes are reflected in the IT component of the organization as well. Within this mode of flux, however, one thing remains constant — a desire to obtain and maintain a high level of information assurance. In this context, the roles of IT governance and organizational design in fulfilling the security management commitment are presented and presented. Policies-procedures-practice. An organization's information security is only as good as the policies and procedures designed to maintain it, and such policies and procedures must also be put into practice (or executed). If managers, developers, and users are not aware of such policies and procedures, they will not be effectively executed.

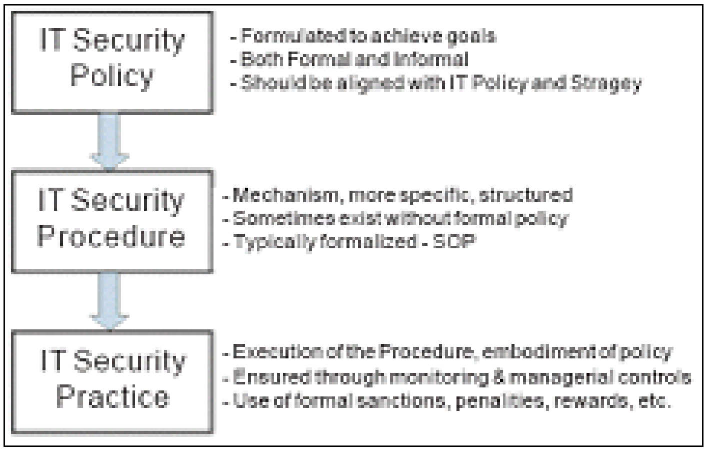

IT Security Policy
- Formulated to achieve goals
- Both Formal and Informal
- Should be aligned with IT Policy and Stragey
IT Security Procedure
- Mechanism, more specific, structured
- Sometimes exist without formal policy
- Typically formalized - SOP
IT Security Practice
- Execution of the Procedure, embodiment of policy
- Ensured through monitoring & managerial controls
- Use of formal sanctions, penalities, rewards, etc.

Fig. 1 Security policy – procedure – practice

2. IT Governance

Information Technology Governance is a subset discipline of Corporate Governance focused on information technology (IT) systems and their performance and risk management. The rising interest in IT governance is partly due to compliance initiatives, for instance Sarbanes-Oxley in the USA and Basel II in Europe, as well as the acknowledgment that IT projects can easily get out of control and profoundly affect the performance of an organization.

A characteristic theme of IT governance discussions is that the IT capability can no longer be a black box. The traditional involvement of board-level executives in IT issues was to defer all key decisions to the company's IT professionals. IT governance implies a system in which all stakeholders, including the board, internal customers, and in particular departments such as finance, have the necessary input into the decision making process. This prevents IT from independently making and later being held solely responsible for poor decisions. It also prevents critical users from later complaining that the system does not behave or perform as expected

IT governance describes the distribution of IT decision-making responsibilities within the firm and focuses on the procedures and practices necessary to create and support strategic IT decisions. The IT Governance Institute (ITGI®) (http://www.itgi.org/) has established the Control Objectives for Information and related Technology (COBIT) to facilitate in conducting all audits. This methodology is especially helpful in establishing thescope and plan for IT audits, and can guide managers in identifying appropriate controls and selecting effective infrastructure processes.

2.1 IT Governance Background

The discipline of information technology governance derives from corporate governance and deals primarily with the connection between business focus and IT management of an organization. It highlights the importance of IT related matters in contemporary organizations and states that strategic IT decisions should be owned by the corporate board, rather than by the chief information officer or other IT managers.

The primary goals for information technology governance are to (1) assure that the investments in IT generate business value, and (2) mitigate the risks that are associated with IT. This can be done by implementing an organizational structure with well-defined roles for the responsibility of information, business processes, applications, infrastructure, etc.

Decision rights are a key concern of IT governance, being the primary topic of the book by that name by Weill and Ross. According to Weill and Ross, depending on the size, business scope, and IT maturity of an organization, either centralized, decentralized or federated models of responsibility for dealing with strategic IT matters are suggested. In this view, the well defined control of IT is the key to success.

After the widely reported collapse of Enron in 2000, and the alleged problems within Arthur Andersen and WorldCom, the duties and responsibilities of the boards of directors for public and privately held corporations were questioned. As a response to this, and to attempt to prevent similar problems from happening again, the US Sarbanes-Oxley Act was written to stress the importance of business control and auditing. Sarbanes-Oxley and Basel-II in Europe have been catalysts for the development of the discipline of information technology governance since the early 2000s. However, the concerns of Sarbanes Oxley (in particular Section 404) have less to do with IT decision rights as discussed by Weill and Ross, and more to do with operational control processes such as Change management.

2.2 Relationship to other IT disciplines

2.2.1 Business Service Management

A strategy and an approach for linking key IT components to the goals of the business. It enables you to understand and predict how technology impacts the business and how business impacts the IT infrastructure.

2.2.2 Business Technology Optimization

An enterprise software product category focused on helping businesses ensure that every dollar invested in information technology, every resource allocated, and every application in development or production meets business goals. BTO is part of an emerging business philosophy to manage IT resources as a business rather than as a service bureau.

2.2.3 Enterprise architecture

Enterprise architecture is the practice of documenting the elements of business strategy, business case, business model and supporting technologies, policies and infrastructures that make up an enterprise. There are multiple architecture frameworks that describe Enterprise Architecture. Enterprise Architecture can be described as 1: documentation describing the structure and behaviour of an enterprise and its information systems, usually in a number of architecture domains. Or 2: a process for describing an enterprise and its information systems and planning changes to improve the integrity and flexibility of the enterprise.

2.2.4 IT asset management

IT asset management (ITAM) is the set of business practices that join financial, contractual and inventory functions to support life cycle management and strategic decision making for the IT environment. Assets include all elements of software and hardware that are found in the business environment.

2.2.5 IT portfolio management

IT portfolio management is the application of systematic management to large classes of items managed by enterprise Information Technology (IT) capabilities. Examples of IT portfolios would be planned initiatives, projects, and ongoing IT services (such as application support). The promise of IT portfolio management is the quantification of previously mysterious IT efforts, enabling measurement and objective evaluation of investment scenarios.

2.2.6 IT security assessment

Information Technology Security Assessment (IT Security Assessment) is an explicit study to locate IT security vulnerabilities and risks.

2.2.7 IT service management

IT Service Management (ITSM) is a discipline for managing information technology (IT) systems, philosophically centered on the *customer's perspective of IT's contribution to the business.* ITSM stands in deliberate contrast to technology-centered approaches to IT management and business interaction.

2.2.8 Project governance

The term Project governance is used in industry, especially in the information technology (IT) sector (see Information technology governance), to describe the processes that need to exist for a successful project. Project Governance is an active rather than just a controlling role. While lack of senior management commitment is a consistent cause of project failure, this still occurs when governance structures are in place and operating. This is because Project Governance is not well understood and even less well executed.

2.2.9 Project management and Program management in the enterprise IT context (including software engineering where appropriate)

Project Management is the discipline of planning, organizing, and managing resources to bring about the successful completion of specific project goals and objectives. Program Management is the process of managing multiple ongoing inter-dependent projects.

2.3 Professional certification

Certified in the Governance of Enterprise Information Technology (CGEIT) is an advanced certification created in 2007 by the Information Systems Audit and Control Association (ISACA). It is designed for experienced professionals, who can demonstrate 5 or more years experience, serving in a managing or advisory role focused on the governance and control of IT at an enterprise level. It also requires passing a 4-hour test, designed to evaluate an applicant's understanding of enterprise IT management.

3. IT Architecture

The Institute of Electrical and Electronic Engineers (IEEE) describes architecture as a dynamic structure of related components, whose design and maturation are governed by an established set of principles and guidelines.

IT governance can be effective only if the enterprise organizes its information technology (hardware, software, procedures) in a manner consistent with its organizational and technical requirements. There are numerous formalized approaches to establishing an appropriate configuration for the organization’s information resources. Such configurations are termed the "IT architecture"and are intended to efficiently and effectively support IT governance mandates as articulated in policy and procedure and enacted in practice.

4. Information Systems Centralization

Information systems deal with the development, use and management of an organization's IT infrastructure.

In the post-industrial information age, the focus of companies has shifted from being product-oriented to knowledge-oriented in the sense that market operators today compete in process and innovation rather than in products: the emphasis has shifted from the quality and quantity of production to the production process itself--and the services that accompany the production process.

The biggest asset of companies today is their information--represented by people, experience, know-how, innovations (patents, copyrights, trade secrets)--and for a market operator to be able to compete, he or she must have a strong information infrastructure, at the heart of which lies the information technology infrastructure. Thus the study of information systems focuses on why and how technology can be put into best use to serve the information flow within an organization.

The degree to which the IS is centralized or decentralized comprises one of the most fundamental characteristics of a firm’s IT architecture or structure. A key role of IT managers is determining the IT architecture for the organization’s information system, and one of the most important aspects of the architecture is the degree of centralization.

4.1 Centralized Information Systems

In centralized information systems, the information resources and decisions regarding their acquisition and control are concentrated in one particular business unit that provides IT services to the whole firm. The main characteristics of a centralized approach include control, efficiency, and economy. Some centralized IS have always been centralized, while others have resulted from a cost-saving regrouping of an organization’s IS to one particular location.

4.2 Decentralized Information Systems

Decentralized systems provide the individual units with autonomy over their own IT resources without regard to other units. The primary advantages of the decentralized approach are the added flexibility and empowerment of individual business units. Response times to business demands are often faster. The proximity to the users and their actual information requirements can lead to closer fit, and the added involvement of end users in system development can lead to superior systems designs.

4.3 Centralization in IT Security Management

There are numerous information assurance mechanisms that may be deployed and managed in manner consistent with a desired level of centralization. For instance, firewall protection can be administered at the enterprise level by one administrator or a single unit within the organization. Alternatively, decentralized firewall protection, in which the individual user maintains a personal firewall solution, may be appropriate for environments characterized by a highly autonomous end user community. Another example of a security technology that can be deployed and managed in either a centralized or decentralized manner is an antivirus solution. While most organizations would probably choose to integrate antivirus protection into their enterprise level protection strategies, it is possible to deploy antivirus protection at the end-user level. In fact, for many organizations that allow mobile computing or remote connectivity, reliance on end users to appropriately manage an antivirus solution is commonplace. The same scenario is repeated for those security technologies that have not yet matured to the level of an enterprise-level solution, such as antispyware technology.

5. Case Study

A comparative case study of two units within one enterprise (Johnston et al., 2004) compares the results of malware exposure under two types of IT security governance. The first, TechUnit, can be characterized as a centralized organization in terms of its IT environment, includingits IT security governance. MedUnit, however, has a highly decentralized structure in which individual users maintain a high degree of control over their IT resources, including the responsibility for security-related activities.

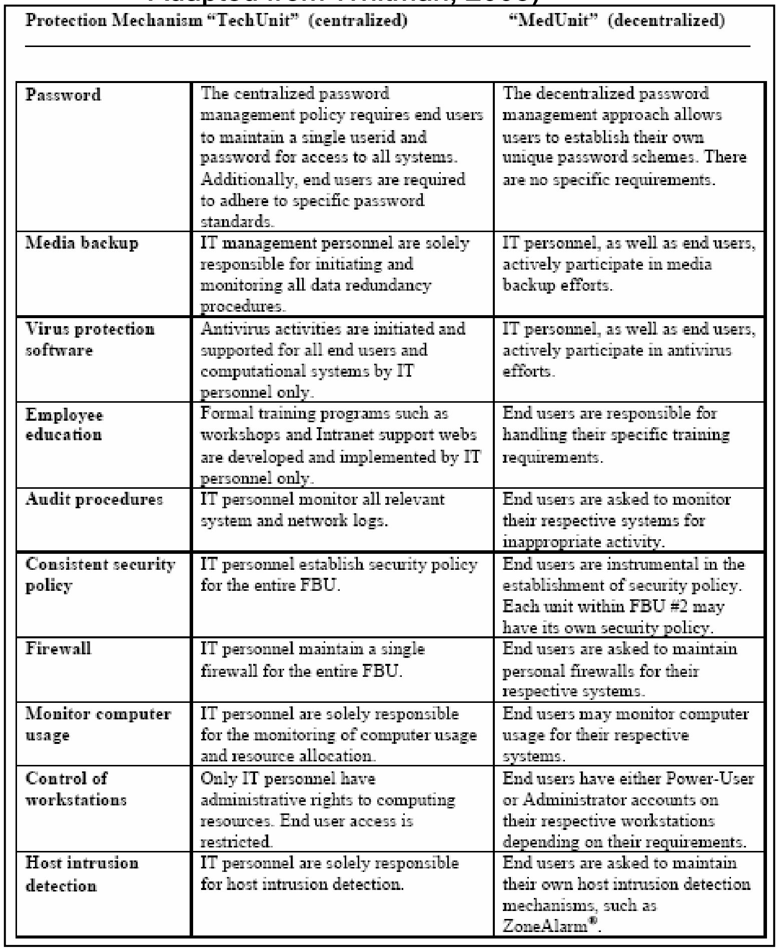
The practice of centralized IT security management provided TechUnit with a highly effective framework from which to address issues specific to the Blaster and Sobig.F worms. As stated by the director of IT, "All of our PCs have antivirus software and multiple layers of protection and, in terms of the worms (Sobig.F and Blaster), it was all hands-off to the users"(Johnston et al., 2004, p. 8). This is a consistent theme among the other IT personnel.

The only actions taken by TechUnit IT personnel to deal with the worms were slight modifications to their firewall and e-mail server filter. There were only a few observations of Blaster or Sobig.F worm activity in TechUnit' s computing environment. These instances were identified and resolved solely by IT personnel with no impact in terms of cost, time, philosophy, or credibility (user confidence).

The IT director noted, "If we have done our job properly, the impact is minimal, if at all felt, to the user community."Perhaps the minimal amount of end-user interaction required by TechUnit' s IT personnel to deal with the worms could help to explain the notable absence of specific knowledge of the worms' functionality. Notably, the level of specific knowledge of the Blaster and Sobig.F worms increased as the level of management decreased and the degree of user interaction increased.

A decentralized approach to IT security management is one in which there is a high level of autonomy for end users in dealing with the security of their respective computing resources. The IT environment of MedUnit is highly reflective of such an approach. Although certain protection mechanisms are deployed in a manner consistent with centralized IT security management, such as the use of virus protection software.

Table 1. Categories of threats to information systems (Source: Johnston et a.l, 2004; Adapted from Whitman, 2003)



Protection Mechanism	"TechUnit" (centralized)	"MedUnit" (decentralized)
Password	The centralized password management policy requires end users to maintain a single userid and password for access to all systems. Additionally, end users are required to adhere to specific password standards.	The decentralized password management approach allows users to establish their own unique password schemes. There are no specific requirements.
Media backup	IT management personnel are solely responsible for initiating and monitoring all data redundancy procedures.	IT personnel, as well as end users, actively participate in media backup efforts.
Virus protection software	Antivirus activities are initiated and supported for all end users and computational systems by IT personnel only.	IT personnel, as well as end users, actively participate in antivirus efforts.
Employee education	Formal training programs such as workshops and Intranet support webs are developed and implemented by IT personnel only.	End users are responsible for handling their specific training requirements.
Audit procedures	IT personnel monitor all relevant system and network logs.	End users are asked to monitor their respective systems for inappropriate activity.
Consistent security policy	IT personnel establish security policy for the entire FBU.	End users are instrumental in the establishment of security policy. Each unit within FBU #2 may have its own security policy.
Firewall	IT personnel maintain a single firewall for the entire FBU.	End users are asked to maintain personal firewalls for their respective systems.
Monitor computer usage	IT personnel are solely responsible for the monitoring of computer usage and resource allocation.	End users may monitor computer usage for their respective systems.
Control of workstations	Only IT personnel have administrative rights to computing resources. End user access is restricted.	End users have either Power-User or Administrator accounts on their respective workstations depending on their requirements.
Host intrusion detection	IT personnel are solely responsible for host intrusion detection.	End users are asked to maintain their own host intrusion detection mechanisms, such as ZoneAlarm®.

6. Conclusion

In these times, the security of information systems needs to be properly managed in order to ensure availability of resources. Organizations planning their IT security management strategies can benefit from the findings of this research. While the decentralized approach and federal governance architecture facilitate meeting end-user requirements, security may need to be increasingly centrally managed. This is not necessarily contradictory to improving functionality for end users, since under the decentralized approach, end users are expected to take an active role in activities such as auditing and intrusion detection. This takes time and effort, and an end user’s failure to practice these functions can potentially compromise the whole network for all users.

References

[1] Warkentin, M & Johnston, A (2006). IT Security Governance and Centralized Security Controls

[2] Hodgkinson, S. (1996). The role of the corporate IT function in the Federal IT organization. In M. Earl, Information management: The organizational dimension. Oxford, UK: Oxford University Press.

[3] IEEE Std. 1471.2000. Recommended practice for architectural description. New York: IEEE.

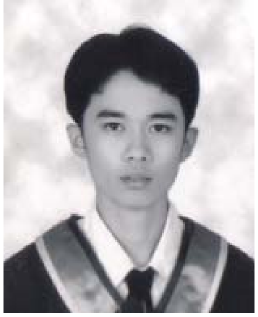
[4] ITGI®- IT Governance Institute. (2003). Board briefing on IT governance. Retrieved September 6, 2004, from www.ITgovernance.org/resources.htm

[5] Information technology governance - Wikipedia Accessed: May 2008 http://en.wikipedia.org/wiki/IT_governance

Acknowledgement

This work was supported by a grant from Security Engineering Research Center of Ministry of Knowledge Economy, Korea

Authors



Rosslin John Robles

He received his B.S. in Information Technology from Western Visayas College of Science and Technology, Philippines. He is currently a Multimedia integrate Masters-Ph.D. Student at Hannam University, Korea. His research interests are Software Engineering and IT Security.

Ji-Yeu Park

She is currently a Multimedia Student at Hannam University, Korea. Her research interests are Network Security and Software Security.

Tai-hoon Kim

He received B.E., M.E., and Ph.D. degrees from Sungkyunkwan University. Now he is a professor, School of Information & Multimedia, Hannam University, Korea. His main research areas are security engineering for IT products, IT systems, development processes, and operational environments.