IT Security Governance for e-Business

Rosslin John Robles, Na-Yun Kim, Tai-hoon Kim
School of Multimedia, Hannam University, Daejeon, Korea
rosslin_john@yahoo.com, bijou0318@nate.com, taihoonn@hannam.ac.kr

Abstract

Information Security is very important in e-Business. Previous IT governance frameworks have not given the connection between IT governance and e-business security sufficient attention. This paper identifies various levels of governance followed by a focus in the roles of information technology (IT) governance with reference to information security for today's electronic business (e-business) environment. The emergence of and dependence on new technologies, like the Internet, have increased exposure of businesses to technology-originated threats and have created new requirements for security management and governance. We proposed a model achieves the necessary integration through risk management in which the tensions between threat reduction and value generation activities have to be balanced.

Keyword : Information Security, IT Governance, e-Business Management, Secure System

1. Background

Information Security Governance gained attention due to failures of big companies. The concept of corporate governance is much quoted as "the system by which companies are directed and controlled". Corporate governance includes concerns for information technology governance because without effective information management, those charged with corporate responsibilities would not be able to perform effectively. Corporate governance includes concerns for information technology governance because without effective information management, those charged with corporate responsibilities would not be able to perform effectively. eWeek (2004) make the case for IT professionals to take a leading role in corporate governance since they have control over the processes underpinning governance activities. They mention the example of the human resource database providing information about employees’ compensation which, if the information is properly monitored, could provide an early indication of malpractice.

This means that IT functions need to be secure so that “business data is not altered by unscrupulous hands”. With business increasingly utilising modern digital technology in a variety of ways, effective information security governance has, therefore, become a key part of corporate governance.
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 the scope 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 interdependent 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. Architecture and design of secure systems

![Diagram of IT governance and enterprise governance](image)

Fig. 1 IT governance and enterprise governance

3.1 IT Governance Model

Perspectives on IT governance from three significant institutions in this field are examined below: they are the IT Governance Institute, Standards Australia (SA), and National Cyber Security Partnership. The analysis focuses on the activities of IT governance and the integration of IT security in the respective frameworks in order to synthesis these views later into a model of information security governance.

3.2 e-Business Security Management

E-business has been defined as "a business that creatively and intelligently utilizes and exploits the capabilities of IT and Internet technologies to create efficiencies, to achieve effectiveness gains such as flexibility and responsiveness, and to create strategic opportunities through competitive uses of IT to alter markets and industry structures."

3.3 Risk Management

As observed in the preceding discussions, effective risk management is a key objective of IT governance (ITGI®, 2004; Standards Australia, 2004) and is required to minimize the IT risks associated with operating an e-business. In the proposed model, it can furthermore be seen as an integrating force, linking IT governance processes with e-business security management.

The elements of the traditional risk management life cycle are important for e-business, but due to e-business’ inherent needs for flexibility and responsiveness (e.g., to react to emerging customer demands), an ongoing and more dynamic risk management approach is required (Mann, 2004).

Fink (2004) reviewed existing risk management methodologies as to their suitability for the Internet environment and found significant shortcomings among some well-known products. He recommended that an effective methodology should be able to meet the following criteria: Comprehensive, Inclusive, Flexible and Relevant.
4. Implementation Guide

Here are some guidelines for the organization on how such a model can best be implemented.

A clear understanding needs to exist within the organization on the responsibilities of governance at the enterprise level and how IT governance integrates into this.

- For an e-business, information security has become an important consideration. The organization has to understand the nature and significance of current and possible future threats and risks as well as the counter measures that are available to an e-business.

- Risk management plays the key role in balancing what appears to be conflicting objectives when applying ICT, namely, value realization and security.

- A program of education to raise competence and awareness should be implemented across all levels of management to ensure that the requirements for effective information security governance are well understood.

- It is recommended that an adaptable and flexible attitude be adopted during implementation in that the model needs to integrate into the existing ICT, and organizational and management structures.

- Lastly, implementation progress should be reviewed and monitored on a regular basis applying the well accepted feedback loop.

5. Conclusion

This paper has shown the need for governance and suggested a concept for the integration of IT governance with enterprise governance. It then identified three major approaches to IT governance and their management of IT security. The latter was shown to be critical for the operation of an e-business. Hence, a framework was developed in which IT governance and e-business security operate together in an integrated, structured, yet holistic manner. The proposed model recognizes that IT governance aims to optimize the value delivery of ICT while e-business security ensures that identified risks are controlled in an efficient manner. This model emphasizes the importance of risk management as the method that links IT governance
and e-business security and thereby resolves the often conflicting objectives of security and value delivery.

References


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.

Na-yun Kim

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.