Chapter V
A Holistic Approach to Information Security Assurance and Risk Management in an Enterprise

Roy Ng
Ryerson University, Canada

ABSTRACT

The hypergrowth of computing and communications technologies increases security vulnerabilities to organizations. The lack of resources training, the complexity of new technologies, and the slow legislation process to deter the breach of security all constitute to the trends of increasing security risk in an enterprise. Traditional approaches to risk assessment focusing on either the departmental or branch level lacks an enterprise perspective. Many organizations assess and mitigate security risks from a technology perspective and deploy technology solutions. This approach ignores the importance of assessing security risk in policy and execution. This chapter discusses a systematic and holistic approach to managing security risk. An approach that utilizes the information life cycle and information assurance (IA) assessment points for the creation of policy, monitoring, auditing of security performance, regulate, and initiate corrective action to minimize vulnerabilities. An “information life cycle” is being proposed with its stage value and the underlying security operatives (gate-points) to protect the information. An information assurance framework and its functions to audit the information security implemented in an enterprise are proposed. Organization must assess the value and the business impact of the information, so that optimal and effective security system and security assurance can be designed.

INTRODUCTION

The exponential growth of the powerful, feature-rich computing and communications technology give rise to two contradicting influences to business. On one hand, it answers the business survival needs to hypercompetition (Burton, 2001), which constantly shrinks the business cycles and time to market. On the other hand, it gives rise to security vulnerabilities and attack, due to the user’s ignorance and company’s limited resources in the management especially disasters recovery of the new and complex technology. Enterprise is at risk in maintaining an effective level of information assurance due to the hypergrowth in technology and the lagging behind of resources training and legal ramifications in the deterrence of security hacking and cracking. From a practitioner’s point of view, many organizations still treat information security as a technological issue which requires only a technology solution. Others companies miti-
A Holistic Approach to Information Security Assurance and Risk Management in an Enterprise

gate security risk in a silo manner of departmental or branch-level solution. Security risk distributed across the enterprise, and the weakest security protection on one part, is the weakest link of the whole security protection system within the enterprise.

Security, by nature, requires a comprehensive and a total-system approach. Effective security implementation demands a holistic and systematic design and implementation. Information security and assurance should be a proactive process by design, rather than a reactive implementation as an after-effect patch tool. Security metrics should be used to measure the performance of the information security systems (Jaquith, 2007). A well-defined metrics will not only benchmark the security system enables a systematic and holistic approach to improve the existing system continually.

BACKGROUND

Information Assurance (IA) is a risk management tool. It reduces the probability of security vulnerability and minimizes the effects should a security incident occurs. IA provides the guiding principles and audit to the underlying information security (InfoSec) process across an enterprise. IA affirms the stakeholders’ trust, confidence, and the quality of information in areas of confidentiality, integrity, and authenticity of the information being processed.

Various risk assessment models have been proposed, such as the Risk Level Matrix, Business Impact Analysis and the Annualized Loss Exposure (ALE) (Krutz & Vines, 2001; Stonebumber et al., 2002; Tipton & Krasuse, 2000). These are very useful models dealing with a specific assessment of risk within a risk scenario. On the contrary, the standard “17799 common information security architecture” from the Committee of Sponsoring Organizations of the Treadway Commission’s (COSO’s) enterprise risk management architecture and Zachman’s information systems architecture provide an enterprise level and a comprehensive approach. These models and frameworks, when applied in the context of information assurance, increase the trust and confidence level in the performance of the information security. Security policy, procedure, and the execution of the information security process should include the assessment of security risks and the defined metrics should be evaluated to form an integrated approach in an enterprise.

BUSINESS DRIVERS THAT INCREASE SECURITY EXPOSURE

Every organization exists to fulfill its mission. A for-profit organization strives to increase revenue and shareholders’ profits. A nonprofit organization endeavors to provide more services within the allocated grants and funding. In order to maximize the goals to achieve their mission, both types of organizations make every effort to increase efficiency and effectiveness with cost reduction or savings. The ability to outreach to clients or customers will enjoy a better return on investment. It also increases the “service to funding” ratio for nonprofit organization. It is believed that by providing the right information to clients helps the increase of sales or services. Information is now believed to be an asset, and helps organizations to gain competitive advantage over other organizations. The followings are some of the many business drivers that increase the efficiency and effectiveness, but also create the propensity of increasing security vulnerabilities and attacks.

Driver 1: Competition drives efficiency and effectiveness. Three factors have made possible the increase of efficiency and perhaps effectiveness of an organization. They are (1) the continuing of lower cost of computing equipment such as desktops, laptops and handheld devices, (2) the feature-rich multimedia applications that allow for portability of “anywhere, any time, any systems” connections, (3) acceptance of the use and the growth of the Internet. Organizations take advantage of these three factors and outreach to more customers in order to increase the market share. However, information security to protect the services, process, and procedure of computing environment has been lagging behind in the research and development of solution.

Driver 2: Customer choices of a better purchase experience. As early as 2001, the awareness of hypercompetition (Burlton, 2001) has been recognized as a new business driver that shrinks business cycles. Ever since, it has been observed that over the years, customers demand a better purchase experience by expecting better product information to be available for product selection and purchase decisions, and more convenience to shop both with time (7/24) and the use of handheld or laptop devices over the Internet for purchase.

With the availability of competitive product information, the customer also expects a better price
Related Content

Laws and Regulations Dealing with Information Security and Privacy: An Investigative Study
[www.igi-global.com/article/laws-regulations-dealing-information-security/2482?camid=4v1a](www.igi-global.com/article/laws-regulations-dealing-information-security/2482?camid=4v1a)

Synchronization in Integer and Fractional Order Chaotic Systems
[www.igi-global.com/chapter/synchronization-integer-fractional-order-chaotic/43288?camid=4v1a](www.igi-global.com/chapter/synchronization-integer-fractional-order-chaotic/43288?camid=4v1a)

Evaluating Security Mechanisms in Different Protocol Layers for Bluetooth Connections
[www.igi-global.com/chapter/evaluating-security-mechanisms-different-protocol/22076?camid=4v1a](www.igi-global.com/chapter/evaluating-security-mechanisms-different-protocol/22076?camid=4v1a)

Insider Perceptions of Insider Trading and Corporate Governance at Nigerian Banks
[www.igi-global.com/article/insider-perceptions-insider-trading-corporate/67371?camid=4v1a](www.igi-global.com/article/insider-perceptions-insider-trading-corporate/67371?camid=4v1a)