STRATEGIC, TACTICAL, & OPERATIONAL MANAGEMENT SECURITY MODEL

GARRY WHITE
Texas State University
San Marcos, TX 78666

ABSTRACT

Information security can be viewed as being different, at different levels of management. Strategic management involves creating security policies, dealing with people issues, and evaluating threats and risks. Tactical management involves how the security systems are developed and implemented to meet policy requirements. Operational management involves maintaining and monitoring the enforcement of information security policies. This paper presents and explains information security from a managerial level perspective and how curriculum supports the model of the different information security needs of strategic (why), tactical (how), and operational (what) management.

Keywords: security, management, strategic, tactical, operational, curriculum.

INTRODUCTION

Overview

Organizations are urging top executives to make information security a priority. Therefore, quality and trustworthiness of information are becoming key business issues (Ezingeard et al, 2005). To better accomplish information security in an organization, a management level infrastructure approach is needed. Just as information and data characteristics are different at the different levels of management, information security has different characteristics at the different levels of management.

These levels of management are strategic, tactical, and operational. At the operations level, transaction data is produced and serves as input to create information. Maintaining and monitoring of integrity, confidentiality, and availability of the transaction data are primary objectives which are supported by organizational procedures and guidelines. At the tactical level, information is interpreted and utilized in decision making. Implementations of preventative, detective, and responsive controls are a primary objective which is supported by organizational standards. Further analysis/aggregation of the information creates knowledge to help make strategic level decisions.

Information security can also be viewed as being different at the different levels of management. Such a view makes it easier to resolve needs. These needs are to pay attention to the security issues in information technology and to cope with the different information security problems (Surendran et. al., 2002). Organizations and academia currently lack sufficient awareness of the different information security needs at different management levels.

Purpose

This paper presents and explains information security from a managerial level model, and how curriculum fulfills the different information security needs of strategic (why), tactical (how), and operational (what) management levels. This view of corporate security structure in terms of this model will better address business security issues.

Background

Information security is orientated towards information technology (Nosworthy, J., 2000). However, information security is more of a people problem than a technological problem (Rainer et al, 2007). Many of the common job titles and descriptions associated with information security do not incorporate people-oriented objectives or experiences. For example, business managers are generally concerned with the managerial aspects of information security, and information security professionals are more concerned with the technical aspects of information security (Rainer et al, 2007). Most information security groups retain central control over policy and standards development, but leave implementation to the operation groups (Rangaswami, 2005).

Rather than build a technological fortress, companies must assess their information assets from a business standpoint and manage the threats to each asset in a way that reflects its importance (Lohmeyer et al, 2002); a tactical and strategic approach. However, companies are still struggling to integrate security into a strategic approach (Rangaswami, 2005). This issue is not reaching top managers (Ezingeard et al, 2004). Generally, a senior manager's attention is with operational incidents (Ezingeard et al, 2004), rather than strategic assets and threat assessments.

It is unclear how information security integrates management with technology at the different management levels. Distinguishing differences between tactical and strategic approaches will enable organizations to respond to short-term business drivers without interrupting strategic projects (Purser, 2004). Companies must look at operational and strategic factors; know the value of their information; and take an integrated approach to information security (Lohmeyer et al, 2002). This paper address such issues in terms of a security management model.

MANAGEMENT SECURITY LEVELS DEFINED

Strategic Management — Why do security problems exist?

Strategic management answers the question "why do security enterprise problems exist?" This question of security leads to developing security policies that deal with people issues, and evaluates internal/external risks.

Policies: Information security policy provides a framework to ensure that systems are developed and operated in a secure manner. Such policies must consider internal and external threats and risks. They must address issues such as privacy and be current to changing technologies. Additionally, policies must complement and be compatible with federal, state, and local laws. Zhang & Suhong (2006) indicated the need for secure information sharing policies in Internet-based supply chain management. Such policies enhance the competitive advantage by promoting trust with partners, a strategic goal. However, the literature, with regard to the formulation of the information security policy, has generally tended to ignore the important relationship with the strategic information systems plan (Misra et al, 2007).

People issues: Strategic management is not focused on technologies, but on higher-level issues of functionality for all stakeholders. Stakeholders in information security include government regulators, shareholders, customers, employees and business partners. (Vijayan, 2005). Additionally, laws, ethical principles, codes of conduct, and society-driven needs are considered. Relationships with people, effective communication and human resources management are required. Security professionals deal with people, both criminal and non-criminal. (Armstrong & Jayaratna, 2002; Zhang & Suhong , 2006).

Evaluating threats and risks: A proactive approach to new threats and risks, is a component of strategic management, as well as enterprise strategic planning. A business impact analysis identifies threats and possible attacks where potential damage is then assessed (Whitman & Mattord, 2005, p. 209). Evaluating these threats and risks prioritizes investments for information security. Enterprises must adapt themselves to rapidly changing circumstances in order to survive in changing external environments (Kim & Leem, 2005). As the environment changes, so do the threats and risks. A proactive approach to new threats and risks, instead of reacting to incidents, is a major component to enterprise strategic planning.

Summary: Development of enterprise security architecture requires a common vision shared by planners, constructors, and administrators. It integrates management processes and policies for enterprise information security (Kim & Leem, 2005). The security professional must be able to advise top management on strategic security decisions.

Benefits: The results of strategic information security are a competitive advantage, feedback to the board about problems, feedback about risks impacting stakeholders, ensuring due diligence, lower costs, promote trust with partners, and increase sales since customers know their information is protected (Ezingeard et al, 2004; Zhang & Suhong, 2006).

Tactical Management — How are security problems mitigated?

Tactical management answers the question "how are security problems mitigated?" It involves how the security systems are developed and implemented to satisfy policies. Activities include planning, designing, establishing standards, and implementing security tasks. Security blueprints are created through tactical management. They included defining tasks/responsibilities of personnel, how information needs are related to tasks, how information is shared, and the identification, valuation and classification of data assets (Kim & Leem, 2005; Steinke, 1997; Whitman & Mattord, 2005, p. 186).

Planning: It involves the implementation of schedules, management, and controls as stated in the security policies (Kim & Leem, 2005). There are three types of security planning: incident response, disaster recovery, and business continuity (Whitman & Mattord, 2005, p. 207). Incident response deals with detection and reaction. Disaster recovery deals with crisis management and recovery operations. Business continuity plans for backup systems and sites to ensure continuous operations.

Design: It involves the implementation of security domains, perimeters, and control procedures in order to protect data and software (Kim & Leem, 2005). Examples of such activities include 1) determining firewall types, such as application gateways, circuit gateways, and MAC layer firewalls; 2) designing filters for firewalls; designing VPN as either transport mode or tunnel mode; and 3) designing intrusion detection systems (IDS) as either application, network, or host. (Whitman & Mattord, 2005, p. 288).

Standards: These documents provide details supporting security policies (Whitman & Mattord, 2005, p. 174). They explain the system development, management, and operational requirements (Merkow & Breithaupt, 2006, p.70). Security Standards take into account all assets and the systems and technology within the enterprise (Kalbaugh, 2001).

Implementation: Security controls require project management, such as the implementation of start and end dates, the assigning resources and funding, system testing, use of Gantt/PERT charts, and deciding conversion methods. A tactical question for implementation is to "outsource or not?"

Summary: The tactical aspect of information security can be viewed as a security development life cycle (SecDLC) which includes the development of security standards and effective security management practices (Whitman & Mattord, 2005, p. 187). These are the tasks performed by a security analyst.

Benefits: Confidence and accountability are assured. Compliance, for regulatory and legal requirements, is provided. Risks are lowered and control increases. And usable information is made available. The tactical benefits have a positive impact on the organization's relationship with its partners (Ezingeard et al, 2004).

Operational Management — What security procedures and practices are to be utilized?

Operational management answers the question "what security procedures and practices are to be utilized?" Use of analysis tools, auditing tools, physical controls, scanners, and packet sniffers are utilized. The procedures maintain and monitor the technology, in order to enforce information security policies.

Maintenance: Operation management involves maintaining the day-to-day controls, access methods, and practices of users. Examples are the maintenance and updating of access controls, such as router filters and user permissions. Passwords and permissions must be created or deleted, as employees join or leave the organization. Teer et. al. (2007) indicated the need for operation management to insure the day-to-day practices of future employees using anti-virus software, strong passwords, and patching the client operating systems.

Monitor: Watchdog duties are done at this management level. Intrusion detection systems and alters are managed. Log files, honey pots, and padded cells are used to trap and trace intruders. An issue with monitoring is determining false negatives/positives alerts on systems. Another issue is monitoring behavior practices of users.

Summary: Procedures to monitor and maintain day-to-day information security are performed by the security technician and user.

Benefits: Operation security procedures provide business continuity; secure and easy access to reliable information. Supply chain and customer services are improved. The integrity and availability are assured. And strict control procedures stop unauthorized access or software use in the day-to-day operations. Business processes and customer service improve. (Ezingeard et al, 2004).

Summary of Management Security Levels

Four major components of information security management are people, security, processes, and technology (Rangaswami, 2005). Three additional components are policies, standards and procedures (Merkow & Breithaupt, 2006. p 70-74). These seven information security components best summarize the three management levels of security management. Strategic management is people and policy focused (management). Tactical management is security process and standards focused (development). Operational management is technology and procedure focused (maintenance & monitoring).

CURRICULUM

A joint industry and academia project indicated four main topics for an Information Security Manager: security policy, risk management, implementation and training, and management. (Kim & Surendran, 2002). In 1996, two areas of security were identified: operations and technology, creating a need for different information security education and training (Barnett, 1996). Since 1996, there have been many changes in information security, due to e-commerce and the Internet. In general, information systems curriculum needs balance between business operations and technical content (Plice & Relining, 2007). However,

Information security has been struggling with operational management, tactical management, and strategic management as noted earlier in this paper. Kim and Chio (2002) stated: "education programs should be structured differently for Information Security Managers (management) and Information Security Systems Developers (technical)." However, different curricula already address information security at these different levels of management.

DIFFERENT SECURITY DEGREE CURRICULUM BASED ON MANAGEMENT LEVEL

There is a need for educational institutions to initiate security related curricula at the Masters and Bachelors levels (Surendran et. al., 2002). Security management and technical skills are required in a college undergraduate program (Logan, 2002). Short term career goals are realized with such technical content (Plice & Relining, 2007). University programs focus more on strategic management and policy aspects rather then technical skills (Anderson & Schwager, 2002). Long term career goals are realized with business/management content. When universities shift to technical content, the student's ability to move into management related career paths is impaired (Plice & Relining, 2007). Different security degree curriculum based on management levels are explained as follows:

Strategic — Master's degree

A security professional requires a wide range of backgrounds, such as top level management knowledge, external knowledge of laws, and awareness of social issues/trends. Information security professionals must learn business functions such as accounting, finance, marketing, and management to better understand information security in a holistic business context (Rainer et. al., 2007). An alliance with the criminal justice department strengthens a security curriculum (Logan, 2002). A security manager should have a good working relationship with local, state, and federal law enforcement agencies. Along with core computer courses, other liberal arts studies are needed since information security also requires perspectives of the environments computer systems to work within. Information security is a multi-discipline subject. A wide range of educational experiences provides a good foundation for a career in Information Security. (Merkow & Breithaupt, 2006, p 7-8).

At one university, the requirements for a Master of Science degree in Information Security Management consist of the following courses:

Information Security Systems & Organizational Awareness
Legal & Ethical Practices in Information Security (IS)
Effective Writing in Information Security Analysis
Business & Security Risk Analysis
IS and Organizational Change
IS Project Management
Knowledge Management in IS
Strategic Analysis in IS
IS Policy Planning & Analysis
Policy Standards & Procedures
Incident Response Management

Graduate courses in information security do focus on strategic aspects and learn to develop policies, deal with people issues, and evaluate risks. Such courses are more managerial, less technical, and external issues are considered. An MBA with an emphasis in information security fits. Such a degree provides opportunities for an **Information Security Professional** position at top level management.

Tactical — Bachelor's degree

Tactical aspects consist of using technology and management in security development life cycle. Required skills and knowledge for such a security curriculum are problem solving, project management, risk management and technical skills (Armstrong & Jayaratna, 2002). Such undergraduate security courses must provide a balance between theory and practice (Hsu & Backhouse, 2002).

At one university, the requirements for a Bachelor of Business Administration degree in Infrastructure Assurance consist of the following core courses:

Operating Systems
Telecommunications
Secure Network Design
Information Assurance & Security
Cybercrimes & the Law
Intrusion Detection & Incident Response
Secure Electronic Commerce
Information Assurance Policy
Forensics
System & Access Controls
Programming & Data Structures

Along with these core courses, business courses in the areas of Accounting, Business Law, Microeconomics, Management, Marketing, and Finance.

These courses are a mix of managerial and technical topics. Upper-division courses in information security focus on tactical aspects; learning to develop standards and security systems. A Bachelor's degree with a major in information security fits. Such a degree provides opportunities for a **Security Analyst** position at mid level management.

Operational — Associate's degree

The day-to-day operations involve the use of technical tools from vendors, such as Windows web servers and Cisco routers. Educational programs from vendors offer the technical skills, but at a lower technical level to accommodate all ranges of class participants (Logan, 2002).

At one community college, the requirements for an Associate of Applied Science Degree in Security Administration Specialization consist of the following course:

Network Technologies
Client & Server Operating Systems
Networking with TCP/IP
Firewalls & Network Security
Computer Hardware
Programming
Intrusion Detection
Incident Response
Router & Routing (CISCO vendor products)
Computer Systems Forensics
Security Assessment and Audit

Such courses are technical and vendor specific. These lower-division courses in information security focus on operational aspects. An Associate's degree with a major in information security fits. Such a degree provides opportunities for a **Security Technician** position at lower level management.

SUMMARY

This paper introduced the different security management levels, and how curriculum addresses this model. The ability to develop strategic security policies, to deal with internal/external issues and to understand the "why," are what a Master's degree prepares future decision makers for. The ability to determine "how" to fix security problems, and the development of tactical standards, are what a Bachelor's degree prepares future security analysts for. The ability to know "what" to do, to maintain and monitor operational security, is what an Associate's degree prepares technicians for. This new corporate perspective and awareness provides better insight in security management for the corporate executive.

ACKNOWLEDGEMENTS

The author wishes to acknowledge his graduate students; G. Bautista, D. Bynum, M. Dieterle, S. Kurra, M. Myers, J. Robbins, and D. Robinson for critiquing this paper and providing suggestions. The author especially wishes to acknowledge M. Myers for her suggestions to refine content layout.

REFERENCES

Anderson, J. E. & Schwager, P. H. (2002). Security in the Information Systems Curriculum: Identification & Status of Relevant Issues. *Journal of Computer Information Systems*, 42(3), 16-24.

Armstrong, H. & Jayaratna, N. (2002). "Internet Security Management: A Joint Postgraduate Curriculum Design." *Journal of Information Systems Education*, 13(3), 249-258.

Barnett, S. (1996). "Computer Security Training and Education: A Needs Analysis." In Proceedings of the IEEE Symposium on Security and Privacy, p. 26-27, Los Alamitos, CA, May. IEEE Computer Society Press.

Ezingeard, J.N. & McFadzean, E. & Birchall, D. (2004). Board of Directors and Information Security: A Perception Grid. Paper No. 222 in Proceedings of British Academy of Management Confrerence, Harrogatte.

Ezingeard, J.N. & McFadzean, E. & Birchall, D. (May, 2005). A Model of Information Assurance Benefits. *EDPACS* 32(11), 1-16.

Hsu, C. & Backhouse, J. (2002). "Information Systems Security Education: Redressing the Balance of Theory and Practice." *Journal of Information Systems Education*, 13(3), 211-218.

Kalbaugh, G.E. (December, 2001). Security and Risk Assessment. *Rough Notes,* 144(12), 118-119.

Kim, K & Surendran, K. (2002). "Information Secuirty Management Curriculum Design: A joint Industry and Academic Effort. *Journal of Information Systems Education*, 13(3), 227-235.

Kim, S. & Choi, M (2002). "Education Requirement Analysis for Information Security Professionals in Korea." *Journal of Information Systems Education*, 13(3), 237-247.

Kim, S. & Leem, C. S. (2005). Enterprise security architecture in business convergence environments. *Industrial Management + Data Systems*, 105(7), 919-936.

TABLE 1. Summary of management level model.

Management Level	Position Titles	Education/Focus	Degree	Theme
Strategic (management)	Information Security	Graduate/ Professional	MBA (post-grad) Policies	**Why** security problems exist? Proactive
Tactical (development)	Info. Sys. Security	Upper-Division/ Analyst	BA in IS (4 yr) Standards	**How** are security problems fixed? Development & legal requirements.
Operational (technology)	Network Security Technician	Lower-Division/ Procedures	AA in Tech (2 yr)	**What** to do? Maintain & monitor. Reactive

Logan, P. Y. (2002). “Crafting an Undergraduate Information Security Emphasis Within Information Technology.” *Journal of Information Systems Education*, 13(3), 177-182.

Lohmeyer, D. & McCrory, J. & Pogreb, S. (2002). Managing Information Security. *The McKinsey Quarterly*, 2002, p. 12.

Merkow, M. & Breithaupt, J. (2006). *Information Security: Principles and Practices*. Pearson/Prentice Hall, Upper Saddle River, NJ.

Misra, S. & Kumar, V. & Kumar, U. (2007). Aligning the Information Security Policy with the Strategic Information Systems Plan. *Computers & Security*, 25(1), 55.

Nosworthy, J. (2000). Implementing Information Security in the 21st Century — Do you have the Balancing Factors? *Computers & Security*, 19(4), 337.

Plice, R. K. & Relinig, B. A. (2007). Aligning the Information Systems Curriculum with the needs of Industry and Graduates. *Journal of Computer Information Systems*, 48(1), 22-30.

Purser, S. (2004). Imporving the ROI of the Security Management Process. *Computers & Secuirty*. 23(7), 542.

Rainer, R. K. & Marshall, T. E., & Knapp, K. J., & Montgomery, G. H. (2007). Do Information Security Professionals and Business Managers View Information Security Issues Differently? *Information Systems Security*, 16(2), 100-108.

Rangaswami, M. R. (Feb, 2005). Finding Security. *Optimize*, 4(2), 67-68.

Steinke, G. (1997). A Task-Based Approach to Implementing Computer Security. *Journal of Computer Information Systems*, 38(1), 47-54.

Surendran, K. & Ki-Yoon, K. & Harris, A. (2002). “Accommodating Information Security in our Curricula.” *Journal of Information Systems Education*, 13(3), 173-176.

Teer, F. P. & Kruck, S.E. & Kruck, G. P. (2007). Empirical Study of Student’s Computer Security Practices/Perceptions. *Journal of Computer Information Systems*, 47(3), 105-110.

Vijayan, J. (2005). Strategic Security. *Computerworld*, 39(15), 48.

Whitman, M. E. & Mattord, H. J. (2005). *Principles of Information Security,* 2nd Ed. Thomson/Course Technology, Boston, MA.

Zhang, C. & Suhong, L. (2006). Secure Information Sharing in Internet-Based Supply Chain Management Systems. *Journal of Computer Information Systems*, 46(4), 18-24.