Information Security Management: The New Security Paradigm

Gregory A. Rondot

CISSP-ISSAP

August 16, 2005

rondotech CONSULTING INC

INTRODUCTION

Information is the lifeblood of all organizations and exists in many forms. It is printed or written on paper, stored electronically, transmitted by mail or electronically, shown in films, or spoken in conversation. In today's competitive business environment, such information is constantly under threat from many types of sources, including internal, external, accidental, and malicious. With the increased use of new technology to store, transmit, and retrieve information, we have all opened ourselves up to increased numbers and types of threats.

In the first half of 2005, there have been numerous dramatic information security breakdowns that resulted in highly publicized releases of millions of citizens' private financial information – social security numbers, home addresses, credit histories, etc. The unauthorized releases put each and every one of those citizens at high risk for identity theft. Sarbanes-Oxley also has increased the penalties and personal liabilities for security lapses to the corner office. These forces have led to a paradigm shift in enterprise information security.

Traditional Information Security Management

Over 70% of the security breaches in the past few years have been attributed to corporate insiders

Information security has historically been an IT-centric affair. It has traditionally concentrated on preventing unauthorized access to computerized records from outside the organization. Consequently, firewall and other network security product vendors have enjoyed a significant share of IT budget, while the internal aspects of information security have been neglected. One of the problems with this approach is that over 70% of the security breaches in the past few years have been attributed to corporate insiders, while IT has been focused on outsiders. The security gap is obvious.

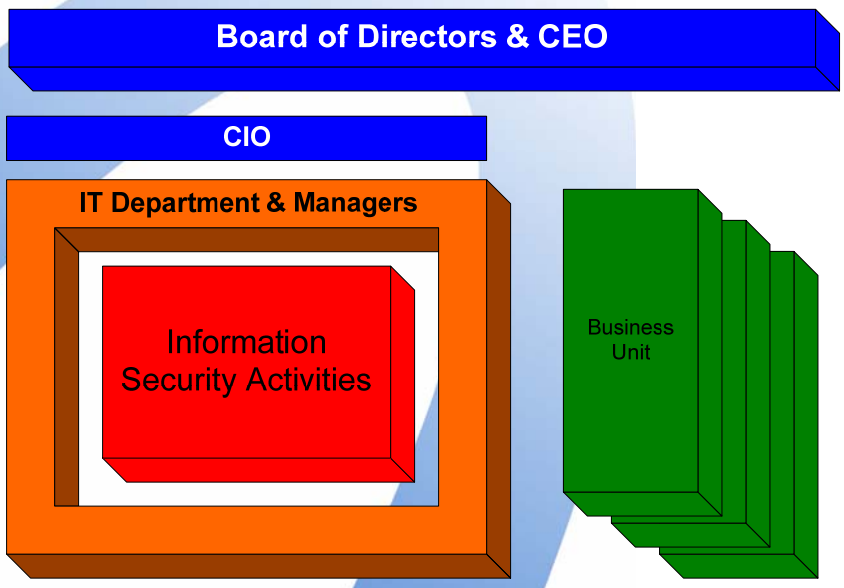

Figure 3

Figure 1 illustrates the traditional form in which information security has been implemented and managed. Security was confined to the Information Technology Department and had limited, if any, involvement with other business units. Generally

the Board of Directors and C-level management had no visibility into the policies and actions of IT's information security staff.

There was no enterprise level manager responsible for information security across all activities and business units. IT managers below the CIO effectively set information security policy within their areas and then were responsible for implementing the supporting technical procedures, standards, metrics, etc. There was limited interaction with other business units except when they use IT-supported systems. Any information security activities and policies within non-IT business units was the product of their individual managers' and external regulatory requirements.

With the advent of SOX Section 404 control requirements, this structure is no longer viable – it does not support the CEO's and CFO's annual certification of the effectiveness of internal controls to the SEC.

The new paradigm of Information Security Management Systems is much more comprehensive, concentrating on business processes as a whole rather than on the IT aspects.

The New Paradigm

The new paradigm of Information Security Management Systems (ISMS) is much more comprehensive, concentrating on business processes as a whole rather than on the IT aspects. An ISMS is a systematic approach to managing sensitive company information so that it remains secure. It encompasses people, processes and IT systems. As a result of the increasing threats to businesses, there is a need to establish a comprehensive Information Security Policy within the enterprise. Management needs to ensure the confidentiality, integrity, and availability of both vital corporate information and customer information.

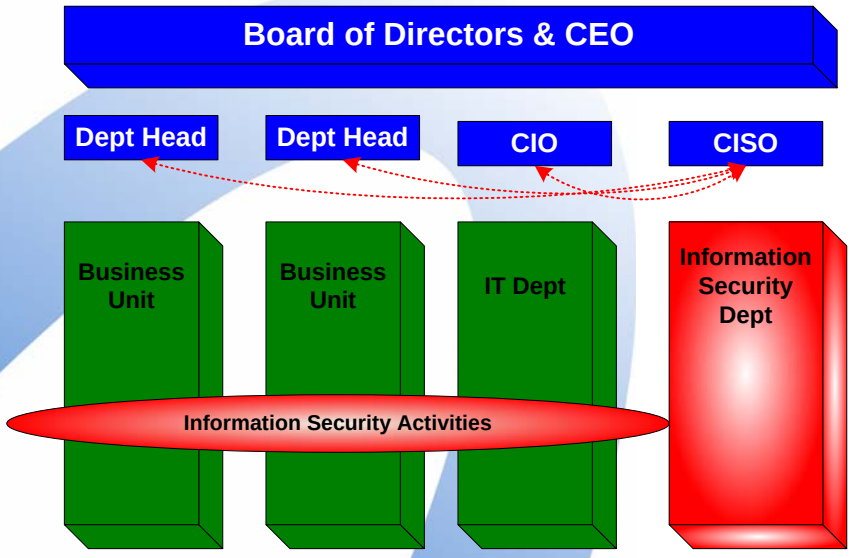

Figure 3

Figure 2 illustrates the new ISMS paradigm structure. The two key concepts illustrated are that the Board of Directors and C-level managers are directly involved in establishing both the enterprise wide information security program and the policies, reporting and management structure for the effort. Note that the IT department is no longer the "keeper of the keys" in this structure. IT is one of the business units involved in information security and IT happens to have responsibility for the tactical

implementation of security in the network, software development processes, etc., but it is not alone in these responsibilities. Information security management in this structure is a separate group within the enterprise and interacts with IT and other business units to ensure that the security policies and standards are implemented appropriately.

In the financial industry it has become common practice to have a Compliance Department to implement and monitor compliance with lending laws and other regulations that impart the line of business operations. It is more efficient to centralize monitoring and administration of these efforts rather than distribute these tasks to each business unit. A similar situation has developed in the information security arena as well and should be addressed similarly.

Since information security mandates are being issued by legislative and regulatory bodies all across the country, and apply to any firm that does business in that jurisdiction, multi-state enterprises should follow the financial industry's Compliance Department precedent with an Enterprise Information Security Department as well.

Many organizations have also established the position Chief Information Security Officer (CISO), or equivalent title, to oversee the firm's information security efforts. This individual generally reports directly to the CEO or Board of Directors Audit Committee. The CISO's responsibilities include:

- Continuously assessing the threats to the enterprise
- Develop appropriate standards, procedures, and countermeasures to mitigate those threats
- Perform appropriate testing to ensure that the information security countermeasures are effective
- Educate other business unit leaders in information security issues
- Engage other business units in assessing and mitigating the specific threats for each business unit
- Communicate with the CEO, other business unit heads, and the Board of Directors to keep them engaged and informed of the enterprise's information security status

ISMS International Standards

There are two internationally recognized standards for ISMS: British Standard 7799 and ISO Standard 17799. The ISO standard is a superset of BS 7799 with only small differences in wording between the two documents. There are two sections in each standard:

- Part One – Code of Practice for Information Management
- Part Two – Specifications for Information Security Management System

Together the two documents specify the concepts and controls that need to be included in an ISMS and provide an organizational outline of the management and reporting structure required of a 'best practices' organization. Part One of the standard concentrates on defining the best practices for ISMS. Part Two then continues with documentation of the specific practice areas and controls that are to be included in an audit of an ISMS.

Part 2 of the standards is organized into ten sections corresponding to the areas of concern of an ISMS. The ten sections are:[1]

- Security policy - Provides management direction and support for information security
- Organization of assets and resources - To help you manage information security within the organization
- Asset classification and control - To help you identify your assets and appropriately protect them
- Personnel security - To reduce the risks of human error, theft, fraud or misuse of facilities
- Physical and environmental security - To prevent unauthorized access, damage and interference to business premises and information
- Communications and operations management - To ensure the correct and secure operation of information processing facilities
- Access control - To control access to information
- Systems development and maintenance - To ensure that security is designed and built into information systems
- Business continuity management - To counteract interruptions to business activities and to protect critical business processes from the effects of major disasters or failures
- Compliance - To avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations, and any security requirements

An ISO-17799's ten sections are:

- ***Security policy***
- ***Organization of assets and resources***
- ***Asset classification and control***
- ***Personnel security***
- ***Physical and environmental security***
- ***Communications and operations management***
- ***Access control***
- ***Systems development and maintenance***
- ***Business continuity management***
- ***Compliance***

ISMS and Statutes: Mutual Support

The regulatory environment surrounding personal financial and medical information is more complex and demanding than ever before. Congress, the SEC, the FDIC, the FDA, state legislatures, and many more state, Federal and Government sponsored organizations regularly publish mandates that must be complied with on a daily basis. The need to address highly inflammatory incidents in the business world has led to the Gramm-Leach-Bliley Act, Sarbanes-Oxley Act, Health Insurance Protection and Portability Act, California State Bill 1386, and too many more laws and regulations to list.

Since impacted firm's have no control over the speed with which mandates must be implemented, the key to surviving and thriving in such a dynamic environment is to establish a system to interpret and implement new requirements quickly much as the financial industry does with their Compliance Departments. The only way to do this in a cost effective manner is to establish a repeatable, manageable process for determining the impact of new information security mandates, and to work with all affected business units to ensure that mandates are implemented and that the business can prove they were done correctly. The logical home for this type of process for handling mandates regarding personal privacy and information security is the Enterprise Information Security Department and they become the managers of the process.

An ISMS eases the burden of implementing and managing new privacy mandates. Once the ISMS is in place, adding new mandates to the environment becomes one of enhancing or adjusting the existing processes rather than inventing a new security process for each new requirement.

For example, at first glance SOX and an ISMS based upon ISO Standard 17799 Part 2 appear to have little in common. Deeper perusal, though, reveals that the Standard

supports the control requirements of SOX Section 404 very clearly. SOX's intention is to ensure that a firm's internal controls can effectively prevent and/or detect unauthorized modification of financial data or systems that support the financial reporting. This is also a narrow interpretation of the information security controls documented in the Standard. Figure 3 succinctly illustrates the correspondence between SOX control requirements and supporting ISO Standard clauses or controls.

An ISMS based upon ISO Standard 17799 Part 2 supports the control requirements of SOX Section 404 very clearly.

Sarbanes Oxley Act Section 404 Requirements	ISO 17799 Supporting Clause / Control (Per BS 7799-2:2002)
Data Center Operation Controls Controls such as job setup and scheduling, operator actions, backup and recovery procedures, and contingency or disaster recovery planning	A.5 Asset Classification and Control A.8 Communications and Operations Management A.11 Business Continuity Management
System Software Controls Controls over the effective acquisition, implementation and maintenance of system software, database management, telecommunications software, security software and utilities	A.8 Communications and Operations Management A.12 Compliance
Access Security Controls Controls that prevent inappropriate and unauthorized use of the system	A.9 Access Control
Application System Development and Maintenance Controls Controls over the development methodology, which include system design and implementation, outlining specific phases, documentation requirements, approvals, and checkpoints to control the development or maintenance of the project	A.10 System Development & Maintenance

Figure 3

If compliance with SOX was the only objective of information security, implementing these few clauses and controls would be good enough for any firm. The reality is that the Standard's clauses and controls cover all of the components of a "best practices" information security program and are generally used as the model for an ISMS. CobiT, HIPPA, GLBA, California SB1386 all map to the Standard's clauses and controls because they each apply controls to different aspects of the global realm of "information security". The Standard's "best practices" controls were designed to be broadly applied across all industries and businesses of varying sizes.

The ISO Standard's clauses and controls cover all of the components of a "best practices" information security program and are generally used as the model for an ISMS. CobiT, HIPPA, GLBA, California SB1386 all map to the Standard's clauses and controls

Alternate: The ISO Standard was designed broadly to apply to all industries and encompass the "best practices" for any firm's ISMS. Consequently, the major IT governance, i.e. CobiT, and regulatory mandated controls, e.g. HIPPA, GLBA,

California SB1386, etc, map easily to the clauses and controls that an ISO compliant ISMS would already have established. This clearly illustrates a key strength of an ISMS – newly mandated controls will in all likelihood already be in place requiring at most minor adjustments to be compliant. Thus an operating ISMS reduces the effort and costs required to implement new regulatory mandates.

Summary

The practice of information security has evolved from an IT centric effort to one requiring enterprise wide attention and C-level management involvement on a regular basis. Both regulators and shareholders have changed the definition of fiduciary duty to include responsibility for internal information security controls and made the CEO and CFO personally liable for certifying that the firm has effective controls. New mandates for protecting personal financial and medical information are being passed regularly and to maintain compliance across the enterprise Information Security Management Systems need to be implemented to systematize compliance with new laws and regulations. The stakes are increasing, both personally and as an enterprise. We have reached a "strategic inflection point", to quote Andrew Grove from *Only the Paranoid Survive*, in how firms handle information security. How firms respond to the new security environment can help determine whether they thrive or are consumed by litigation over information security incidents and questions of lack of due diligence. In this case, Mr. Grove was right – only the paranoid will survive.

About the Author

Gregory Rondot has over 25 years as a businessman and consultant, He has become renowned as an innovative architect and problem solver with a keen sense of harnessing technology to drive revenue to the bottom line in the real world. Over the course of his career, Mr. Rondot has built and fixed several IT organizations as a consultant or IT Director while concurrently maintaining an in-depth technical grasp of security management strategies and networking tools and technology. Mr. Rondot's expertise in both the business and technical aspects of information systems, infrastructure and security management provides a unique vantage point on enterprise-wide security practices and management systems that support rather than hinder the core operations of a business.

Mr. Rondot has earned ten internationally recognized technical and management certifications in security, networking and risk assessment including the CISSP, ISSAP and INFOSEC Assessment Methodology certification from the National Security Agency. Prior to founding RondoTech Consulting, he built government and commercial value added reseller organizations and consulted with organizations as diverse as the Department of the Navy, National Restaurant Association, Morgan Stanley and CareerBuilder.com.

Through his career in systems development and business consulting, Mr. Rondot has developed expertise in security, risk assessment, network engineering, and software development knowledge spaces. Through the course of his career, he has earned many internationally recognized certifications including Certified Information Systems Security Professional, ISO Information Security Management Systems Auditor and INFOSEC Assessment Methodology certification from the National Security Agency.

RondoTech Consulting, Inc
PO Box 2359 • Centreville • Virginia • 20122
703.830.4800 • eFax 703.832.8596

www.rondotech.com

