https://doi.org/10.48009/2_iis_2005_124-130

THE ROLE OF INFORMATION SECURITY IN SARBANES-OXLEY COMPLIANCE

Manying Qiu, Virginia State University, mqiu@vsu.edu
Carl Wright, Virginia State University, cwright@vsu.edu

ABSTRACT

Information security is mandatory to minimize business risk and ensure compliance with government regulations. This paper aims to help IT professionals understand the dramatic changes that the Sarbanes-Oxley Act of 2002 has made in the accounting/auditing profession and to help them realize the role of information security in the compliance process.

Keywords: Sarbanes-Oxley compliance, audit, information, risk-analysis, security control.

INTRODUCTION

Accounting/Auditing in North America was adopted from England. However, while British public companies were required to have audits under national law known as the Companies Act, American public companies audits were not regulated by U.S. government. The recent plague of corporate financial scandals has shaken investor confidence to its foundations. Faith in corporations and their CEOs and CFOs has never been lower [7]. As a result, the Sarbanes-Oxley Act was signed into legislation on July 30, 2002 to make public companies more transparent in their financial reporting and more proactive in sharing material information with other participants in the financial reporting chain such as auditors, audit committees, analysts, and investors. The Sarbanes-Oxley Act of 2002 has dramatically changed oversight of auditing by establishing the Public Company Accounting Oversight Board (PCAOB), which is appointed and overseen by the Securities and Exchange Commission (SEC), an agency of the Federal government.

Sarbanes-Oxley Act requires publicly held companies to attest to their internal financial controls. Audit and compliance experts estimate range from a low of 5% to between 20% and 25% of the 4,000 companies filing reports in 2005 will reveal “material weaknesses” in their financial controls. Almost all the audits are using computers and software tools. There is dispute over how often information technology (IT)-related deficiencies contributed to failures to meet the requirements of the Sarbanes-Oxley Act of 2002 [6]. Instead of pointing fingers at each other, Accounting and IT professionals should work together to comply with the requirements of the Sarbanes-Oxley Act. IT professionals must understand what a difference the Sarbanes-Oxley Act of 2002 has made in the accounting/auditing profession. In order to help IT professionals meet requirements, this paper briefly reviews the history of accounting/auditing and investigates the role of information security in Sarbanes-Oxley compliance.

AUDITING IN BUSINESS

It is known that as early as the fifteenth century, auditors were requested to assure the absence of fraud in the records kept by stewards of wealthy household estates in England. When the audit function was exported to the United States, the British form of reporting was adopted but there were no comparable United States statutes [11]. The absence of statutory requirements for audits to be submitted to stockholders resulted in nineteenth-century audits that varied from balance sheet audits to full, detailed examinations of all accounts of corporations. An auditor was not independent from his client but engaged usually by management or the board of directors of a corporation, and his report was addressed and directed to these insiders rather than shareholders.

The American accounting profession developed rapidly after World War I [11]. In 1917 the Federal Reserve Board published a reprint of a document prepared by the American Institute of Accountants (which became the American Institute of Certified Public Accountants in 1957) dealing with uniform accounting. The accounting/auditing profession rapidly developed common report language through the AICPA. The audit reports are the representations of management about its effectiveness in administration of resources to the stockholders. An audit has value because management's representation on its performance and stewardship are examined and reported on by an expert outside management's control.

Sarbanes-Oxley Compliance

As a response to the startling corporate fraud cases of Enron and WorldCom, Sarbanes-Oxley Act is the most far-reaching regulatory reform of publicly traded markets since the Securities and Exchange Act of 1934. Sarbanes-Oxley Act is designed to reduce fraud and conflicts of interests, while increasing financial transparency and public confidence in the financial markets. Compliance with Sarbanes-Oxley Act means interpreting what it says, understanding where an organization currently stands, documenting a plan for achieving compliance, executing it, and devising measures and controls to prove that the organization has implemented the plan [8].

Sarbanes-Oxley Act requires publicly held companies to disclosure in all material aspects the operational and financial condition of the company. Material information that is used to generate periodic reports must be retained and available to the public. Sarbanes-Oxley compliance requires a statement of management's responsibility for establishing and maintaining adequate internal control over financial reporting for the company, attested to by the company's auditor. This statement includes an assessment of the controls and identification of the framework used for the assessment. Financial statements must be complete and representative. The process that is used to generate statements must be accurate and meet an accepted industry standard. The goal is to protect investors from delayed reporting of material events which may increase their loss.

After over a century since the accounting profession was introduced to North America, auditing is required to be overseen by the Federal government. Because the processes and internal controls are implemented mainly in Information Systems, Sarbanes-Oxley compliance involves a detailed assessment of these systems. Process changes to meet compliance must be documented and implemented by the IT professionals. Since most organizations extensively use information technology for financial reporting, IT management plays a major role in auditing and compliance processes.

Auditing and Information Security

Auditing is about "Who did what when". Security is about legitimate access by appropriate users. Auditing is about knowing if money is stolen from the ATM machine and whether the security camera was working. Security is locking the ATM machine and setting up a security camera to keep the thief from robbing the bank in the first place. Auditing must not be confused with security. Auditing does not prevent access or change to data; it only identifies or monitors the access and change. Security will prevent (or control) access or change to data. To put it another way, security is before the fact while auditing is after the fact.

INFORMATION SECURITY

Information as Valuable Assets

ISO17799, an internationally recognized Information Security Management Standard, was first published in December 2000 [5]. It addresses information as an invaluable asset that may exist in many forms in an organization. The goal of information security is to properly protect assets in order to ensure business continuity, minimize business loss and maximize return on investment. The requirements for protecting information are confidentiality, integrity and available. ISO17799 is broad in scope and conceptual in nature. It is up to the organizations to interpret and implement ISO17799 standard as general guidelines and "Best Practice." IT professionals should re-examine their security policies and controls to ensure Sarbanes-Oxley compliance.

Confidentiality. This requirement ensures privacy of information and ensures that only authorized users can access the information. It is possible to maintain user anonymity on the Internet. The security requirement for authentication becomes critical in the context of the Internet. Authentication assures that the data is from a source it claims to be and the data in transaction cannot be picked up by a third party masquerade as the receiver. To respond to the growing need for assurance related to business transacted over the Internet, the AICPA and the Canadian Institute Chartered Accountants (CICA) jointly created the WebTrust assurance service. WebTrust is an attestation service, and the WebTrust seal is a symbolic representation of the CPA's report on management's assertions about its disclosure of e-commerce practices. The WebTrust assurance service is primarily designed by CPAs to provide assurance to management, the board of directors, or third parties about the reliability of information systems used to generate real-time information [2].

Integrity. This requires data and programs to be changed (added, modified or deleted) in an authorized manner. Information systems should preserve the accuracy and completeness of information and processing methods. It is important to identify the information assets relevant to Sarbanes-Oxley compliance, especially the critical assets. Public companies must disclose information on material changes in their financial condition or operations on a rapid and current basis. Companies must consider how quickly the data could be processed in time for accounting or auditing.

Availability. This requires the Information Systems function properly so that the authorized users can receive the service whenever they request it. IT professionals must establish policy and plans to protect the information against all types of losses and disasters. Information security should be a top priority leading to compliance, yet it is the weakest link in most organizations' strategy and policies. There is no perfectly secured information system; organizations must identify their information assets, assess the risk involved with each asset and develop policy to protect the most critical assets. Asset control requires identification and logging of all assets.

Risk assessment goes a step further in assigning levels of risk to each identified class in order to develop information security policies that focus on the most critical assets.

The Importance of Assets Classification and Control

Asset classification and control address the ability of the security infrastructure to protect organizational assets. These are mechanisms to maintain an accurate inventory of assets, and establish ownership and stewardship of all assets. Identifying the critical assets is essential for many reasons. An organization will come to know what is critical and essential for the business. It will be able to provide appropriate level of security to protect the assets and to decide about the level of redundancy that is necessary by keeping a backup copy of the data or a backup server.

Identification of Assets

IT assets can be broadly classified into the following categories [3]:

1. Information assets include databases (e.g. customers, suppliers, products, transactions), data files (e.g. income statements, balance sheets, reports, emails), operational and support procedures, archived information, disaster recovery plans and business continuity plans. Also they include the people in an organization who possess unique skills, knowledge, and experience that are difficult to replace (e.g. DBAs, IT auditors, CPAs).
2. Software assets include application software and system software (Oracle DBMS, Microsoft MS Money, Mail Order Manager). Organizations may have their in-house developed system software.
3. Physical assets include computers (e.g. desktops, notebooks, servers), communication equipments (e.g. routers and fax machines), storage media (e.g. disks and CDs), technical equipment (e.g. power supplies and air conditioners), furniture and fixtures.
4. Services include computing services, communication services (e.g. voice mail and WAN) and environment conditioning services (e.g. heating and lighting).

Identification of critical information is based on the nature of the information not just the face value of the data. For example, information about a CEO permitted $10.00 exceptional spending for an employee can be critical.

Table 1. An Asset-Based Threat Tree for End Users Using Network Access

Asset	**Critical Asset**															
Access	**Network access**															
User	**Inside User**								**Outside User**							
Motive	**Accidental**				**Deliberate**				**Accidental**				**Deliberate**			
Outcome	Disclosure	Modification	Loss, destruction	Interruption	Disclosure	Modification	Loss, destruction	Interruption	Disclosure	Modification	Loss, destruction	Interruption	Disclosure	Modification	Loss, destruction	Interruption

Risk Assessment

The next step is to assess the threats to these assets. Security accident and breach may occur both inside and outside of the organizations. Table 1 illustrates an asset-based threat tree for end user using network access [1]:

Risk priority level can be defined based on redundancy (back up availability), the condition of operating equipment (e.g., computer, router, air conditioning, etc), and the severity of consequences if equipment fails (e.g., potential permit violation, network breakdown, etc) [3].

Security Controls

The selection and employment of appropriate security controls for information systems are important tasks for Sarbanes-Oxley compliance. Security controls are the management, operational, and technical safeguards or countermeasures prescribed for information systems to protect the confidentiality, integrity, and availability of the system and its information [10].

Technical controls. Technical controls are measures incorporated into the network architecture. For example, antivirus software, firewalls, strong authentication, Tripwire, and encryption that are implemented on the hardware, software or firmware in the network.

Operational controls. Operational controls are best practices, procedures, personnel, and physical measures instituted to provide an appropriate level of protection for security resources. Examples of operational controls are security awareness and training, security reviews and audits, and security plans, such as disaster recovery, contingency, and business continuity plans.

Management controls. Management controls are policies, guidelines, procedures, and enforcement that enable decision makers to manage security and the risks that threaten information security. Some examples of management controls include: People in charge of conceding access privileges are clearly identified; Protect access control mechanism against intrusions; Database management system provides appropriate field-level sensitivity; When employee changes job, eliminate all his/her old access privileges; Network server is isolated and its physical access is restricted.

Human Errors

Controlling human error will present the greatest challenge in protecting computer network in an open-access environment. Human errors are most likely to cause vulnerabilities in deploying and configuring network devices and applications, user-access procedures and practices, and the application development process.

Ill-configured network devices, applications, and security software. Configuration errors are typically found in the Common Gateway Interface (CGI) programs in Web servers. Among other things, CGI programs support interactivity, such as data collection and verification functionality. Hackers often find CGI programming oversights relatively easy to locate and tend to misuse or to subvert CGI scripts to launch malicious attacks on the site, such as vandalizing Web pages, stealing credit card information, and setting up one of their most trusted weapons: backdoor programs. In general, demonstration CGI programs should be removed from the application before going online.

Misconfigured access control lists in both routers and firewalls. In routers, human error in setup may lead to information leaks in certain protocols, including ICMP (Internet Control Message Protocol), IP, and NetBIOS (network basic input/output system). This category of breaches usually enables unauthorized access to services on DMZ servers. A misconfigured access control list in a firewall can lead to unauthorized access to internal systems directly or indirectly through the Web server in the DMZ. In general, when configuring network components, use checklists to ensure proper setup, test thoroughly for desired execution before components go into production, and harden the devices or applications Hardening network devices involves eliminating or deactivating extra services, sample utilities, and programs that are no longer needed in the application environment.

Poor password administration, which includes the use of weak or easy-to-guess passwords. To achieve effective password administration in e-business computing environments, companies are turning to awareness training for employees, coupled with incentives and/or penalties connected with acceptable practices for password use. Companies are also considering and implementing single sign-on solutions that are offering companies a cost-effective solution, especially when multiple passwords are required.

Not properly maintained application development/tools. Applying patches and enhancements to development suites in a timely fashion are challenging, especially in IT departments with a high rate of turnover or activities. One approach to address this critical issue is to include security specialists throughout the volatile code-writing stage of application development to ensure that common security vulnerabilities are precluded from the final application. Unfortunately, this internal activity provides no remedy for vulnerabilities programmed in vendor-developed applications. Because of the serious implications of this issue, some vendors may incorporate a security review when writing their respective applications. Make sure that patches and upgrades are applied to vendor applications as soon as they are released. Applying patches on a regular basis will reduce the risks associated with vulnerability-exploited attacks.

Information Systems Audit

IT audit could be defined as the process of collecting and evaluating evidence to determine whether a computer information system safeguards assets, maintains data integrity, achieves organizational goals effectively and consumes resources efficiently [9]. Typically, IT Security auditing has three functional areas [4]:

Policy audit. Policy auditing is the comparison of current status of the information systems to the business-oriented security policy. Although other business functions (internal audit and external audit) need to do this occasionally, the central security control should perform policy audits as a normal and ongoing process.

Intrusion detection. Intrusion detection is a software product category. These tools identify sequences of events, such as failed logins or patterns of error packets, as indicating an attempted break-in. To identify the attempted security breach, a security manager looks for suspicious behavior across multiple systems and devices. When an event-detection tool determines that such a pattern exists, it communicates this to the network management console, or command and control center through the use of Simple Network Management Protocol (SNMP).

Attack simulation. One valid approach to security auditing is to attempt a breach to determine the effectiveness of policy enforcement. Attack simulation is the testing function of security auditing. It plays a valid role but is effective only as part of the three-tiered approach to auditing—that is, policy audit, intrusion detection, and attack simulation.

CONCLUSION

Although Sarbanes-Oxley does not directly regulate information technology, IT is the backbone of the financial reporting processes that the law regulates. Therefore, IT professionals play a critical role in achieving compliance. To protect information confidentiality, integrity and availability, it is important to classify information assets in an organization, assess risks and/or threats to these assets, select and implement security controls for information systems and the information in the systems. Controlling human errors is a challenge when developing and implementing network devices and accounting/auditing applications. Companies should conduct an IT audit to collect and evaluate evidence to determine if an information system safeguards information security.

REFERENCES

1. Alberts, C. & Dorofee, A. (2002). *Managing Information Security Risks: The OCTAVE^{SM} Approach*. MA: Boston, Addison-Wesley.
2. Arens, A. A., Elder, R. J. & Beasley, M. (2006). *Auditing and Assurance Services: An Integrated Approach* (10th ed.). NJ: Upper Saddle River, Prentice Hall.
3. BITS. (2002). Expectations Matrix Assessment.
4. Byrnes, F. C. & Kutnick, D. (2002). Securing Business Information: Strategies to Protect the Enterprise and its Network. MA: Boston, Addison-Wesley.
5. Carlson, T. (2001). Information Security Management: Understanding ISO 17799, INS Whitepaper.
6. Hoffman, T. (2005). IT Role in Sarb-Ox Problems Is Unclear: Users Find Multiple Compliance Hurdles, *ComputerWorld*, (Feb 7), 14.
7. OpenPages. (2003). Sarbanes Oxley Express SOX 404: An Internal Controls Documentation Module, An OpenPages White Paper. www.csboston.com/exhibitors/openpages1.pdf
8. Rozwell, C., Bace, J. and Leskela, L. (2005). Compliance Management solutions Can Create Improved Business Performance, *Gartner*, Jan 17.
9. Sayana, S. A. (2002). The IS Audit Process, *Information Systems Control Journal*, (6). http://www.isaca.org/PrinterTemplate.cfm?section=IT_Audit_Basics.
10. Wares, W. H. (1979). Security Controls of Computer Systems, Report of Defense Science Board Task Force on Computer Security Published for the Office of the Secretary of Defense.
11. Willingham, J. J. & Carmichael, D. R. (1979). *Auditing Concepts and Methods* (3rd ed.). NY: New York, McGraw-Hill Book Company.