Enterprise System Security
Regulatory Policies

Steve Strickland
Steve Strickland Consulting
www.s3cc.net

Steve Strickland Consulting (S3CC IT Consulting) specializes in outsourced IT services and consulting in the areas of managed IT & Computer Services (including repair), Network Security, Data Backup/Protection & Disaster Recovery, Document Management Solutions, Microsoft SharePoint Consulting, Hardware/Software sales, Computer Asset Management, Paperless Office Solutions, and Electronic Medical Records (EMR) Consulting.

Certified Veteran-Owned Business.

Table of Contents

Executive Summary

Vulnerabilities are defined as a weakness in an information systems' security procedures, internal controls, or implementation procedures that could be exploited (Information Security Terms Glossary, 2008). Vulnerabilities exist anywhere there are information systems present – whether or not they are connected to a network or another computer or device. As vulnerabilities do exist, organizations like the Federal Bureau of Investigation (FBI) and the SysAdmin, Audit, Network, Security (SANS) Institute partner together to create top lists of security risk for network and security administrators to review, study, and learn to aid in implementing corporate security policies for their organization. In 2007, the FBI and SANS released the SANS Top 20 2007 Security Risks (2007 annual update) outlining security risks in groups such as client-side vulnerabilities, server-side vulnerabilities, security policy and personnel, application abuse, network devices, and zero-day attacks (SANS Top-20 2007 Security Risks (2007 Annual Update), 2007). The FBI and the SANS Institute, teaming together as two leaders of information security, bring together the most current and top rated security information for administrators and organizations disposal. This information, while not filling the gap for vulnerabilities, will aid in their reduction through knowledge transfers.

This paper details corporate security policies for employees. The paper will cover a Windows-based network with analysis on corporate security policies that directly apply to COBIT security which is a base for the Sarbanes-Oxley Act (SOX) and Health Insurance Portability and Accountability Act (HIPAA). The paper will also discuss other corporate security policies and compliances such as PCI compliance, Federal Information Processing Standards (FIPS) security guidelines outlined by the National Institute of Standards and Technology. Other topics of discussion will engage in acceptable usage policies, remote access policies, user account/password policies, firewall policies, their implementation and enforcement from a network and management point.

The approach to achieve this deliverable is to conduct research on the various compliances and policies that show their effect. While some software titles can enforce security throughout a network down to the user and desktop level, having a written policy is a must for any organization.

Regulatory Policies

The number of regulatory policies mandated by the federal and state governments, and the frequency of change to those policies are ever increasing. Organizations are not only seeing regulatory policies pile on, such as the Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act (SOX), and Peripheral Component Interconnect (PCI) standards, but also internal corporate policies. A major internal policy instituted by the International Organization for Standardization, and although not enforced by law, but highly encouraged by government entities, can be the ISO 17799 standard. The ISO 17799 standard establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization (ISO/IEC 17799:2005 Information technology). The ISO 17799 outlines general categories and practices in the areas of information security, such as:

- Security policies
- Organization of information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development and maintenance
- Information security incident management
- Business continuity management
- Compliance

While the ISO 17799 standard is not a regulatory policy, it is a standard that is encouraged to be used for when an organization must comply with federal or state regulations, such as HIPAA, SOX, or PCI.

HIPAA and Technical Safeguards

The Health Insurance Portability & Accountability Act (HIPAA) was established August 1996. This act amended the IRS service code of 1986 which required “improved efficiency in healthcare delivery by standardizing electronic data interchange and protection of confidentiality and security of health data through setting and enforcing standards” (HIPAA Primer - What is HIPAA?, 2005). Additionally, HIPAA called upon the Department of Health and Human Services (HHS) to publish new rules that will ensure standardization of electronic patient health, administrative and financial data, unique health identifiers for individuals, employers, health plans and health care providers, and security standards protecting the confidentiality and integrity of "individually identifiable health information," past, present or future” (HIPAA Primer - What is HIPAA?, 2005). Inside HIPAA are security and standards, which apply directly to information technology security known as Security Rules which require

developing and maintaining internal privacy and security management practices and enforcement. Incidentally, the National Institute of Standards and Technology (NIST) wrote Special Publication 800-66 directly for the HIPAA Security Rule when IT personnel implement HIPAA security in their organization (Publications).

Deep within the Security Rule is a sub-section titled Technical Safeguards which pertains directly to information technology security. Other Security Rules apply to administrative safeguards, physical safeguards, and organizational requirements, which do not pertain to information technology. Technical safeguards are defined as the technology and the policy and procedures for its use that protect electronic health information and control access to it (National Institute of Standards and Technology, 2008). In an article written by Steven Weil, he notes the technical safeguards as five categories:

1. Access control – these are policies, procedures, and implemented processes for computer systems that contain electronic health information and who has access to what (or who does not get access), and what software can contain or obtain certain electronic health information.
2. Audit controls – Abilities through processes and procedures to record or capture, examine and explain activity on or in computers systems that store electronic health information (e.g. database xyz contains patient social security numbers. Application ABC accesses that database and database transactions should be recorded).
3. Integrity – policies, procedures, and processes that will eliminate the destruction or intentional alteration of electronic health information (e.g. only the database security administrator can archive and delete information from database xyz. End-user John Doe is only allowed to view certain patient data and not allowed to alter any information pertaining to patients).
4. Person or entity authentication – This policy falls closely in line with integrity where as policies, procedures, and processes should be implemented that can verity a person is who they say they are, and what their intentions are on accessing electronic health information (e.g. Nurse Jane Doe has access to application ABC using her username and password to input patient data, whereas the receptionist is not allowed to access application ABC for any reason).
5. Transmission security – These are policies, procedures, and processes that protect data to prevent unauthorized access to electronic health information when transmitted over a local area network or the Internet. This falls in line with encryption standards and securing data through backup policies and even disaster recovery.

(Weil, 2004)

SOX and COBIT

The Sarbanes-Oxley Act (SOX) was established in 2002 by the United States Congress in the wake of a number of corporate accounting scandals, notably from Enron, Tyco International, and WorldCom. Although SOX only pertains to public company boards, management, and public accounting firms and most goes into corporate board responsibilities to the organization and the public, which include criminal penalties, and requires the SEC to implement rulings on requirements, there are information security guidelines and policies that said organizations must follow, which is dubbed SOX 404 (Sarbanes-Oxley Section 404). The SOX 404 guidance requires the usage of an internal control framework, such as the COSO framework. The IT Governance Institute's Control Objectives of Information and Related Technology (COBIT) are used as a framework supporting IT SOX 404 efforts (Sarbanes-Oxley Act, 2008).

COBIT is the main framework that information technology departments use when implementing policies, procedures, and processes for IT security when engaging in a SOX audit to become compliant, although COBIT can also be used by organizations that desire to increase their corporate security policies and procedures as well. The purpose of COBIT is to provide management and business process owners with an information technology (IT) governance model that helps in delivering value from IT and understanding and managing the risks associated with IT (COBIT Frequently Asked Questions (FAQ)). The entire COBIT comprises of six areas for an organization to use – executive summary, framework, control objectives, IT assurance guides, implementation tools sets, and management guidelines. While COBIT can encompass an entire organization to streamline processes and procedures and can be used by many departments to varying degrees, information technology departments uses it widely in four domains such as plan and organize, acquire and implement, deliver and support, and monitor and evaluate. Since COBIT plays a large role in aiding with security in SOX and governance policies, and among organizations desiring to increase and streamline security, it is necessary to expand upon the four domains of COBIT.

Plan and organize is divided into ten sub-categories which are:

- Define a Strategic IT Plan
- Define the Information Architecture
- Determine Technological Direction
- Define the IT Processes, Organization and Relationships
- Manage the IT Investment
- Communicate Management Aims and Direction
- Manage IT Human Resources
- Manage Quality
- Asses and Manage IT Risks
- Manage Projects

Within each sub-category are definitions, policies, procedures, and even sub-sub-categories. Defining a strategic IT plan presents businesses with plans and cases that can bring together an

organization that utilizes information technology and solidifies it within the organization. Defining the information architecture encompasses the development of a corporate data dictionary with the organization's data syntax rules, data classification scheme and security levels. This process improvises the quality of management decision making by making sure that reliable and secure information is provided and that information systems and resources are appropriately matched against business strategies. Determining technological direction guides management with the creation of a technological infrastructure plan that sets and manages realistic expectations of what technology can offer (the organization) in terms of products, services, and delivery mechanisms. Defining the IT processes, organization and relationships aids management and committees to establish and oversee that IT processes, administrative policies, and procedures are in place for all functions with attention to control, risk management, QA, IT security, and data and system(s) ownership. Managing the IT investment is the planning and implementing of policies for total cost of ownership, budgets, and stakeholders value. The management of communication aims and direction is part of the defining and development of an enterprise IT control framework that communicates policies and procedures. Managing IT human resources is the management of IT services into human resources by establishing procedures and policies that support recruiting, training, performance evaluation, promotion, and termination. Managing quality assurance (QA) practices the providing requirements, policies and procedures. Asses and manage IT risks is essentially risk management. Manage projects provides guidelines, procedures, and policies that define project management (IT Governance Institue, 2007).

Acquire and implement is divided into seven categories which are:

- Identify automated solutions
- Acquire and maintain application software
- Acquire and maintain technology infrastructure
- Enable operation and use
- Procure IT resources
- Manage changes
- Install and accredit solutions and changes

Identifying automated solutions encompasses the needs and considerations of alternative sources, the review of technological and economic feasibility, execution of risk analysis and cost benefit analysis, and conclusion of a decision to make or buy solutions. Acquire and maintain application software falls in line with applications that are made available with business requirements (e.g. accounting software – the purpose, need). Acquire and maintain technology infrastructure requires a planned approach to acquisition, maintenance, and protection of the technology infrastructure. Enabling operation and use outlines definitions, policies and procedures and the production of documentation to support manuals for users providing training to ensure proper usage, including security guidelines. Procuring IT resources requires the definition and enforcement of procurement procedures, vendor selection, and contract setup of hardware and software, including security measures taken. Managing changes of documents policies and procedures and necessary steps to be taken in a controlled manner of

maintenance, security, upgrades/patches, related to the infrastructure and applications. Install and accredit solutions and changes are when applications and hardware have been tested and moved from a testing environment to production and are well documented ensuring systems and software are functioning correctly (IT Governance Institue, 2007).

Delivery and support is divided into thirteen sub-categories which are:

- Define and manage service levels
- Manage third-party services
- Manage performance and capacity
- Ensure continuous service
- Ensure systems security
- Identify and allocate costs
- Educate and train users
- Manage service desk and incidents
- Manage the configuration
- Manage problems
- Manage data
- Manage the physical environment
- Manage operations

Defining and managing service levels ensures the alignment of key IT services with a business strategy, such as focusing on service requirement, agreeing on service levels and monitoring the achievement of service levels. Managing third-party services is managing the suppliers, vendors, and partners on the services that support the organization in ensuring they meet business goals. Managing performance and capacity forecasts future needs based on workload, storage, and contingency requirements. Ensuring continuous service develops, maintains, and tests IT continuity plans, utilizing off-site backup storage, and providing periodic continuity plan training for staff. Ensuring system security is maintaining the integrity of information and processing infrastructure while minimizing impacts of security vulnerabilities and incidents, defining IT security policies, plans, and procedures, which include monitoring, detecting, reporting, and resolving security vulnerabilities and incidents. Identifying and allocating costs is building a system that captures, allocates, and reports IT costs to the users of services to review cost of ownership. Educating and training users is identifying the training needed for users on what hardware and software and ensuring they are properly used. Managing the service desk and incidents is designing a service desk and incident response team. Managing the configuration is establishing and maintaining an accurate and complete repository of asset configurations. Managing problems is establishing a system that records problems, tracks problems, and resolves problems. Managing data is managing the completeness, accuracy, availability, and security of data. Managing the physical environment is managing and maintaining the physical IT asset environment from access, damage, and theft. Managing operations is meeting operational service levels for scheduled data processing, protecting sensitive output, and monitoring the infrastructure (IT Governance Institue, 2007).

Monitor and evaluate is divided into four sub-categories which are:

- Monitor and evaluate IT performance
- Monitor and evaluate internal controls
- Ensure compliance with external requirements
- Provide IT governance

Monitoring and evaluating IT performance is monitoring, evaluating and reporting metrics and implementing performance improvement strategies, mainly on hardware and software applications. Monitoring and evaluating internal controls monitors the internal control processes for IT-related activities and identifying improvement actions. Ensuring compliance with external requirements is ensuring compliance with laws, regulations and contract agreements while reducing the risk of non-compliance. Providing IT governance is preparing board reports on IT strategy, performance and risks, and responding to governance requirements in line with board and organization directions (IT Governance Institue, 2007).

While COBIT might not be the de jure standard for an organization to use during SOX auditing and compliance, it is the mainstream framework that complies with the COSO framework when an organization implements controls which relate to information technology policies, procedures, guidelines and security. COBIT does not specifically state defined requirements (such as "all computers should have a minimum of 500MB of random access memory), but the overall framework and domains of COBIT allow the IT staff to use "best judgment" when implementing policies and procedures. While the major four domains and all their sub-categories give fairly detailed information on what items to focus on, it is still up to the staff to define how they perceive the suggested policies and procedures, and how to implement and enforce them. COBIT is a standard for regulatory policies and when instituted into an organization, the policies and procedures ensure a greater level of processes and security that surround information technology.

Conclusion

Security is always a top priority in any organization that uses computers, networks, and data transmission. Security practices should be designed, established, implemented, and tested. According to Network World magazine, the top seven best practices are rolling out corporate security policies, deliver corporate security awareness and training, run frequent information security self-assessments, perform regulatory compliance self-assessments, deploy corporate-wide encryption, value, protect, track, and manage all corporate assets, and lastly, test business continuity and disaster recovery planning (Miliefsky, 2007).

According to Privacy Rights Clearinghouse, since January 2005 to June 2008, approximately 227,205,625 records containing sensitive personal information (organizational) (Clearinghouse, 2005) have had data that has been compromised in one way or another partially due to either non-existent or lax security policies in an organization. By incorporating corporate security policies and standards in an organization, whether a private company that simply wishes to increase overall security by having policies in effect, or a public company which is mandated by governing laws and standards to have policies in effect, security and awareness can be increased while malicious, illegal, and unethical activities can be decreased.

References

ISO/IEC 17799:2005 Information technology. (n.d.). Retrieved May 30, 2008, from International Organization for Standardization: http://www.iso.org/iso/support/faqs/faqs_widely_used_standards/widely_used_standards_other/information_security.htm

Clearinghouse, P. R. (2005, April 20). *A Chronology of Data Breaches*. Retrieved June 11, 2008, from Privacy Rights Clearinghouse: http://www.privacyrights.org/ar/ChronDataBreaches.htm#CP

COBIT Frequently Asked Questions (FAQ). (n.d.). Retrieved May 31, 2008, from ISACA: http://www.isaca.org/Content/NavigationMenu/Members_and_Leaders1/COBIT6/FAQ6/COBIT_FAQ.htm#1

HIPAA Primer - What is HIPAA? (2005, July). Retrieved May 30, 2008, from HIPAA Advisory: http://www.hipaadvisory.com/REGS/HIPAAprimer.htm

Information Security Terms Glossary. (2008, June 10). Retrieved June 10, 2008, from Key.com: https://www.key.com/html/A-11.2.1.html#V

IT Governance Institue. (2007). *COBIT 4.1 - Framework, Control Objectives, Management Guidelines, Maturity Models.* Rolling Meadows, IL: IT Governance Institue.

Miliefsky, G. S. (2007, Jan 17). *The 7 best practices for network security in 2007*. Retrieved June 11, 2008, from Network World: http://www.networkworld.com/columnists/2007/011707miliefsky.html?page=1

National Institute of Standards and Technology. (2008, May). *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule - Special Publication 800-66 Revision 1.* Retrieved May 30, 2008, from National Institute of Standards and Technology: http://csrc.nist.gov/publications/drafts/800-66-Rev1/Draft_SP800-66-Rev1.pdf

Publications. (n.d.). Retrieved May 30, 2008, from NIST - Computer Security Division: http://csrc.nist.gov/publications/PubsDrafts.html

SANS Top-20 2007 Security Risks (2007 Annual Update). (2007, November 28). Retrieved June 10, 2008, from SANS: http://www.sans.org/top20/

Sarbanes-Oxley Act. (2008, May). Retrieved May 30, 2008, from Wikipedia: http://en.wikipedia.org/wiki/Sarbanes-Oxley_Act

Weil, S. (2004, March 02). *HIPAA Security Rule*. Retrieved May 30, 2008, from Security Focus: http://www.securityfocus.com/infocus/1764