Realtime publishers

"Leading the Conversation"

The Essentials Series

IT Compliance Volume II

sponsored by

SECURE COMPUTING

by Rebecca Herold

How Access Management Compliance Supports Good Business

by Rebecca Herold, CISSP, CISM, CISA, FLMI ***February 2007***

Many business leaders I speak with now have great concern for data protection law and regulation compliance, which is certainly prudent. However, often when digging into the details of their compliance plans and activities, I find most of the effort and budget is going towards initiatives for firewall and perimeter protection, with increasing implementations for encryption.

These are definitely important! But when I ask about any plans they have for improving their authentication methods, a large number, with perhaps the exception of the online banks, say something similar to, "Oh, we are comfortable with our current authentication solution; our passwords must be strong, and must change every 90 days. And we have not experienced any problems with our access control systems. So, we should already be in compliance with these types of legal requirements." But will single-factor re-usable passwords continue to be an acceptable practice for authenticating enterprise users as incidents continue to occur on an ever more frequent basis?

Similarly, when I ask about plans for improving access control methods, many business leaders have a response similar to, "Our access controls are based upon departmental responsibility and manager oversight. We have used this method for several years. It seems to work fine, and we have trust in our managers' capabilities." Will the old way of establishing and managing access controls still be acceptable as the insider threat continues to negatively impact businesses and their customers? Will these practices pass muster with regulatory oversight agencies that check for compliance?

Legacy Systems Create Vulnerabilities

Systems and applications created two and three decades ago are still being used, typically to support the newer systems and applications installed. Effort goes to the new systems and technologies, but security of legacy systems is often not updated to address the new vulnerabilities created by new systems and applications connected to the legacy systems. A good example of the vulnerabilities from legacy systems comes from the State of Wisconsin 2006 financial audit:

> *Condition:*
>
> *The provider system was developed in the early 1990s and has not been able to easily accommodate changes that have occurred over time, which has resulted in errors occurring within the system. Fund staff estimate approximately 15 to 20 hours a week are needed to address the problems that have developed. Further, these system issues have also limited the Fund's ability to address system access control weaknesses.*
>
> *Effect:*
>
> *The aging system presents an increased risk to the integrity of the Fund's financial operations. Access control weaknesses increase the risk that unauthorized or erroneous changes could be made to provider system data without being detected. In addition, increased time spent to correct processing problems that arise with the current system results in less time available for more productive tasks for the Fund.*

This situation is very similar to the situations within a large portion of businesses. Businesses have valid reasons to keep old legacy systems to continue providing processing power, storage repositories, and back-office functions. However, along with the decision to keep the legacy systems comes the decision to maintain the security controls of these old systems to an acceptable level. Not only is this necessary to protect business assets but also it required through numerous laws and regulations.

Protecting Business Operations Is a Basic Management Objective

Protecting the resources that provide critical business operations is a basic management objective for every organization. This objective is realized largely by designing and implementing controls that prevent, limit, and detect unauthorized access to computing resources, programs, and information. Electronic access controls include user identification and authentication, authorization, boundary protection, cryptography, and auditing and monitoring of security-related events.

Network and applications activities must be linked to specific individuals to create accountability, provide a history of the activities, and to catch inappropriate activities. Using identifiers that are unique to each user links the accountability of activities to a specific individual. Appropriate access, and subsequently accountability, can then be assigned to individuals using the identifiers. Too many times within organizations, the authentication and access control policies and supporting processes are implemented in ways that lose the important accountability and history components.

A few excerpts from the August 2006 GAO Audit Report for the Centers for Medicare & Medicaid Services (CMS—available at http://www.gao.gov/new.items/d06750.pdf) demonstrate how proper authentication and access controls are often lacking. I have highlighted a few sentences that seem to be a problem for all organizations throughout all industries:

> *Although CMS has many information security controls in place that are designed to safeguard the communication network, there were significant weaknesses in electronic access controls and other controls designed to protect the confidentiality, integrity, and availability of the sensitive, personally identifiable medical information it transmits. Our review of the communication network revealed 47 weaknesses in electronic access controls and other controls.* ***A key reason for these weaknesses was that CMS did not always ensure the effective implementation of its security policies and standards.*** *As a result, sensitive, personally identifiable, medical data traversing this network are vulnerable to unauthorized disclosure, and these weaknesses could lead to disruptions in CMS operations.*
>
> *CMS did not ensure that its contractor adequately identified and authenticated users responsible for managing the communication network.* ***For example, CMS's contractor did not enforce sufficiently complex passwords for access to certain network devices.*** *This increases the risk that unauthorized users could gain access to CMS systems and sensitive information.*
>
> ***CMS did not ensure that its contractor sufficiently restricted network access and privileges to only those users and processes requiring them to perform authorized tasks****. For example, CMS's contractor did not adequately restrict access paths on certain network devices. In addition, the contractor had several sensitive world-writable files on network management servers, granting inappropriate privileges to these files. These conditions provide more opportunities for an attacker to escalate their privileges and make unauthorized changes to files.*

Laws Specifically Require Authentication and Access Controls

Growing numbers of systems, technologies, network tools, and applications are used throughout the enterprise to enable or streamline business: Web site applications, proxy server firewalls, databases, email servers, data-mining applications, customer relationship management tools, and a seemingly infinite number of other types of business applications. Each of these must effectively enforce authentication and access controls in one way or another. However, many times they do not.

Authentication and access control weaknesses are seen in the findings of almost every information management audit. These weaknesses are also in the findings of almost every regulatory compliance audit. Dealing with authentication and access controls in a consistent, well-documented manner addresses these specific requirements within numerous laws, and results in removing those findings from many different audits, in one fell swoop, saving the business from penalties and fines.

The following table shows just a few of the laws that require authentication and access controls, and the variety of regulatory oversight groups involved.

Law	Sample excerpts requiring authorization and access controls	Covered entities	Regulatory oversight agency
Gramm-Leach Bliley Act (GLBA)	"§ 6801. Protection of nonpublic personal information (b) Financial institutions safeguards… (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer."	All financial institutions regulated by the U.S. Office of the Comptroller of the Currency (OCC)	U.S. (OCC)
Health Insurance Portability and Accountability Act (HIPAA)	"§ 164.312 Technical safeguards. (d) Standard: Person or entity authentication. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed."	U.S. healthcare providers, insurers, and clearinghouses.	U.S. Department of Health and Human Services (HHS)
21 CFR Part 11; Electronic Records and Electronic Signatures	"Subpart B—Electronic Records § 11.10 Controls for closed systems. (d) Limiting system access to authorized individuals."	Companies, such as pharmaceuticals, regulated by FDA	U.S. Food and Drug Administration (FDA)
European Union (EU) Data Protection Directive 95/46/EC	"Article 17 Security of processing 1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing."	All Companies conducting business in EU member nations	EU Data Protection Supervisor and the EU country-specific privacy commissioners
Canada's Personal Information Protection and Electronic Documents Act (PIPEDA)	"4.7 Personal information shall be protected by security safeguards appropriate to the sensitivity of the information. The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held."	All organizations that have personal information about Canadian customers and employees.	Canadian Privacy Commissioners
Japanese Personal Information Protection Law	"Security Safeguards Principle: To prevent loss or unauthorized access, destruction, use, modification or disclosure of Personal Data, Data Collectors must implement security safeguards and provide proper supervision of employees and any other entities to which Personal Data may be entrusted."	Japanese private businesses	Japanese Government

Address Insider Threats

There are inherent risks in giving personnel access to sensitive information or the capability to perform network and applications administration. According to the 2006 11th Annual CSI/FBI Computer Crime and Security Survey (http://www.gocsi.com/forms/fbi/csi_fbi_survey.jhtml), 68 percent of organizations experienced security incidents from insiders. According to the Association of Certified Fraud Examiners (ACFE) 2006 report on occupational fraud and abuse (http://www.acfe.com/documents/2006-rttn.pdf):

- More than 30 percent of occupational frauds are committed by employees in the accounting department
- More than 20 percent are committed by upper management or executive-level employees
- More than 14 percent are committed within the sales department

Personnel at all levels of the company have the potential to do bad things; appropriate controls must be implemented from the very highest positions down through the rest of the enterprise to help prevent incidents caused by insiders. There have been many published accounts of such incidents. The following is just one example.

> On December 19, 2006, a Medco Health Solutions, Inc. computer systems administrator, Andy Lin, was indicted by a federal grand jury in the U.S. District Court for the District of New Jersey for attempting to disable his employer's corporate computer servers through the use of a concealed malicious software program. On or about October 3, 2003, Lin modified existing computer code and inserted new computer code (destructive code) into pre-existing scripts on the Medco Servers, which collectively were designed to delete the patient-specific drug interaction conflict database as well as databases identifying subscribers, plan coverage, prescription administration, and billing data. Part of the new computer code Lin programmed and inserted included a script designed to deploy the destructive code automatically on April 23, 2004, Lin's birthday. On or about January 1, 2005, a Medco computer systems administrator investigating a system error discovered the destructive code embedded within other scripts on the Medco Servers. Medco IT security personnel subsequently removed the destructive code.

Given the sensitivity and criticality of the business resources to which insiders have access and the large amount of money at stake for business processes and electronic resources, access must be controlled, logged, and audited. Compensating controls must exist, such as reviewing logs regularly to ensure insiders are not doing bad things and establishing code review procedures to ensure malicious code is not being put into production.

You will never be able to completely remove the insider threat. However, you can ensure that the access each person has matches, and does not exceed, the access the person actually needs.

Good Business Has Good Controls

Business leaders must address information risks in a comprehensive manner and not just focus on the issues that are the most exciting to work with or that are advertised the most. Authentication and access controls are some of the least glamorous issues to tackle, but if you fail to do so, information cannot be successfully secured and business is highly vulnerable to be given a harsh blow. When making your business decisions remember:

- New and old systems and applications mixed together create vulnerabilities that must be addressed
- Laws and regulations require business resource authentication and access controls
- Strong authentication and access controls lessen the risk of insider fraud, theft, and crime
- Strong authentication and access controls demonstrate due diligence and support legal actions
- Comprehensive security programs make business more efficient and profitable by preventing incidents and avoiding fines and penalties

Business environments are constantly changing as more users, business partners, systems, and applications are added to the business mix. Organizations must implement a comprehensive and effective information security program that protects business resources while meeting applicable compliance requirements within the context of their business objectives. Business leaders must ensure that the vital authorization and access control policies, procedures, and tools are not overlooked. Consistently applying strong access management is not only good business practice and necessary for compliance, it is vital to business success.