CITADEL
INFORMATION GROUP, INC.

Seven Requirements for Successfully Implementing Information Security Policies and Standards

A guide for executives

Stan Stahl, Ph.D., President, Citadel Information Group
Kimberly A. Pease, CISSP, Vice President, Citadel Information Group

August 2011

www.citadel-information.com
2060 Hercules Drive
Los Angeles, CA 90046
Tel: 323.876.1441
Fax: 323.876.7794

TABLE OF CONTENTS

WHY AN ORGANIZATION NEEDS INFORMATION SECURITY POLICIES AND STANDARDS

Information security policies form the cornerstone of an organization's information security program. Without formal information security policies and standards, an organization cannot effectively secure its critical information assets.

The simple fact that policies and standards are the necessary foundation of effective information protection is why[1]

- Legal compliance with Information security regulations like HIPAA and Gramm-Leach-Bliley require information security policies and standards
- MasterCard and Visa require organizations that accept their credit and debit cards to have information security policies and standards
- Every information security effective practice contains a requirement for organization-wide information security policies and standards
- In the event of an information incident negatively affecting 3rd-parties, it may be argued that the absence of information security policies and standards is evidence of information negligence

Information security policies and standards can significantly reduce the frequency, duration and cost of information security incidents.

Information security policies and standards

- establish management's commitment to securing critical information assets
- establish uniform organizational standards for securing critical information assets
- provide guidance to managers and other employees as to their information security responsibilities, obligations and duties
- provide standards for use by IT personnel in securely configuring and maintaining the IT Infrastructure
- provide the foundation for complying with legal responsibilities associated with holding sensitive information of others, such as personal health or financial information, or proprietary information belonging to others
- set the *security tone* for the organization

[1] *An Emerging Information Security Minimum Standard Of Due Care*, Robert Braun and Stan Stahl, Privacy and Data Security Law Journal, March 2006

INFORMATION SECURITY POLICY OBJECTIVES

According to *ISO 27002/17799*,[2] information security policies and standards should include, at a minimum, the following guidance:

- a definition of information security, its overall objectives and scope and the importance of security as an enabling mechanism for information sharing
- a statement of management intent, supporting the goals and principles of information security
- a brief explanation of the security policies and standards, principles, standards and compliance requirements of particular importance to the organization

SEVEN REQUIREMENTS FOR SUCCESSFULLY IMPLEMENTING INFORMATION SECURITY POLICIES AND STANDARDS

Management's biggest challenge lies not in the writing of specific policies and standards but in the orderly development and implementation of policies and standards. An organization can increase the odds that its information security policies and standards will actually influence security by adhering to the following seven "requirements."

Requirement 1. Identify organizational issues that impact information security policy

Information security policies and standards need to accurately reflect the organization they are to serve. To the extent they do not, the organization will find itself in conflict between information security policies and standards and desired practices.

Conflict between information security policies and standards and organizational realities can

- Waste organizational energy
- Increase cynicism towards the organization's commitment to information security
- Diminish the effectiveness of the information security policies and standards
- Increase the probability of serious costly information security failures

[2] Information Technology—Code of practice for information security management, International Standards Organization, ISO 27002.

Consequently, it is very important to build information security policies and standards in the broader context of the organization's business.

Here are a dozen things to consider:

1. The organization's strategic focus and evolving business direction
2. The nature and type of information used in the organization
3. The different classes of information users and the types of information each uses
4. The needs for information sharing and protection between different parts of the organization
5. The needs for information sharing and protection between the organization and its suppliers, vendors, customers, and other business partners
6. Legal information privacy compliance requirements, obligations and duties
7. The organization's security culture and the its opportunities for cultural change
8. The organization's current and evolving technology infrastructures
9. Any history of information losses that might provide lessons-learned for policy developers
10. Other informational needs for confidentiality, integrity or availability
11. Already existing information security policies and standards
12. Other organization policies and standards

Requirement 2. Identify the various classes of policy users

Different classes of users have different information security roles and responsibilities. Your receptionist, your lead IT director, and a vendor all have different responsibilities. The organization may very well need different information security policies and standards for each of its different classes of users. These will, of course, have to be consistent across different classes of users.

These different kinds of users may include:

1. Management, including Boards, executive management, and other management
2. End users, including employees, contractors, and consultants
3. Information system personnel, including employees, contractors, and consultants
4. Customers
5. Vendors, suppliers and other business partners

Make sure you understand these different kinds of users and the different kinds of information they are going to need to do their job.

Requirement 3. Organize information security policies and standards into meaningful categories

While information security policies and standards can be organized in many different ways, we have found that they are most useful when organized as follows:

1. Introductory policies and standards, including information security management structure and responsibilities
2. Information classification and control
3. Physical security
4. Personnel security
5. Policies and standards for employees and other Information users
6. IT Infrastructure policies and standards
7. System and Application Development Policies and standards

These categories (or other information security categories, such as, e.g., the chapter headings of ISO 27002) form the top level of a *Table of Contents* for the organization's policies and standards.

Below is a sample *pro-forma Table of Contents* for an organization's information security policies and standards.

Requirement 4. Review draft policies and standards with management, users, and legal counsel

This is a critical feedback step that is too-easily overlooked. Policy validation is required to ensure that management and users will support the policies and standards, and that the policies and standards are consistent with the business and other needs of the organization.

Information security policies and standards need to be reviewed by the enterprise's legal counsel to assure they comply with State and US laws, legally protect the enterprise, and are otherwise consistent with the enterprise's business practices.

Requirement 5. Train all personnel in the organization's information security policies and standards

All staff needs to be provided regular awareness training and education. Without such training and education, personnel will not know what they are to do nor why they are to do it.

Training and education programs need to emphasize:

- The enterprise's need to secure critical information assets
- Management's commitment to securing the critical information assets
- Each person's individual responsibilities for securing critical information assets
- Consequences for failure to abide by the policies and standards, both organizational and individual

Requirement 6. Enforce the information security policies and standards

Without enforcement, adherence to the policies and standards will degrade over time. In addition, unless policies and standards are uniformly enforced, the organization may find itself in legal jeopardy should it choose to enforce the policies and standards, particularly if the enforcement is directed against an individual in a legally protected class.

Technology can make it easier to enforce certain information security policies and standards. For example, prohibitions on employee access to pornographic or gambling-related web sites can be blocked by web filters. Workstation backup policies and standards can be implemented by programs running on the organization's servers. Password policies and standards can be enforced with systems that require regular password changes and that refuse to accept "weak" passwords.

The technology infrastructure can also be used to monitor and/or log user compliance with policies and standards. While some may argue that this violates employee privacy rights, increasing numbers of organizations are deciding to monitor and/or log employee behaviors. Because of the potential legal implications, surveillance activities must be coordinated with legal counsel.

Requirement 7. Review and modify policies and standards, as appropriate but at least annually

Situations change: business and operational needs, legal duties and obligations, technology opportunities. Information security policies and standards must evolve to reflect changing circumstances.

Consequently an organization needs to regularly review and, if necessary, modify its information security policies and standards.

PRO-FORMA INFORMATION SECURITY POLICIES AND STANDARDS TABLE OF CONTENTS

A FEW SAMPLE INFORMATION SECURITY POLICIES AND STANDARDS

The following are two sample policy statements and four standards for a fictitious company named *BeBop Inc*.

Policy 3: *Bebop* manages the security of sensitive information in its possession through an *Information Security Manager (ISM)*, who

a. is appointed by the President and has the responsibility, accountability and authority for information security management and leadership;

b. publishes security documents, including standards, processes, procedures, and guidelines designed to extend and "make real" these policies;

c. provides training and education to information users and leads the *Bebop* community in creating a security-aware culture.

Policy 4: Working in collaboration with the *Information Security Manager*, each Department is responsible for managing the security of the information it generates and uses. Department managers are expected to

a. identify, classify and control their information in accordance with the harm that would result from a loss of confidentiality, integrity or availability;

b. identify those groups or individuals authorized access to information, granting only the access needed to do one's job ("least privilege" and "need-to-know") based upon the job duties and job requirements of each individual;

c. manage the security of sensitive information in accordance with security documents established in collaboration with the *Information Security Manager.*

Standard 3.3: Security Classifications

Information Owners determine the sensitivity of the information they "own." In doing so, they follow a "standard" language that helps ensure that everyone will know how to protect the information they use in performing their professional duties.

Bebop classifies information into three categories:

- Public Information
- Internal Use Only Information
- Restricted Information

Standard 4.1.1: Login-ID and Passwords

Access to the *Bebop* IT network and information systems is protected and managed by access control procedures. Prior to gaining access to the *Bebop* IT network systems or protected information systems, a user must "present" both a *Login ID* and a *password*. Both of these are unique to the user, thereby providing a measure of certainty that the user is who he/she claims to be.

Standard 7.2.5: Malware Protection

IT is to install *ISM*-approved anti-malware software on all workstations and servers to prevent, detect, and eradicate malicious code (e.g., viruses, Trojan horses, spyware, key loggers, adware etc.).

IT is to configure anti-malware software so that

- All files coming from external sources are checked before execution or usage
- Suspected malware is logged and IT is alerted
- Full malware scans are conducted daily
- Malware signature files are updated daily
- Program updates are installed as soon as available

The *ISM* is to be notified immediately if malware is found on any device.

Standard 7.7.2: Access to Restricted Information Based Upon Need-to-Know

IT is to limit access to *restricted* systems and information to only those individuals whose job requires such access, as determined by the information *Owner*. IT is to implement a mechan*ISM* for systems with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.