Solution Brief

The Business Need for Updated Information Security Policies

InformationShield

About Information Shield

Information Shield is a global provider of security policy, data privacy and security awareness solutions that enable organizations to effectively comply with international security and privacy regulations. Information Shield products are used by over 7000 customers in 59 countries worldwide.

Information Shield, Inc.
2660 Bering Dr.
Houston, TX 77057
www.informationshield.com
sales@informationshield.com
P: 888.641.0505
F: 866.304.6704

Contents

Information Shield Solution Brief

The Business Need for Updated Information Security Policies

By David J Lineman
Information Shield

Summary

Information security policy development should not be a one-time event. In order to effectively reduce risk and maintain a proper governance structure, organizations must periodically update written security policies as part of an ongoing management process.

In this overview we discuss the business requirements for updating security policies, some of the organizational challenges faced by organizations trying to implement policy updates, and some time-saving solutions for addressing these challenges.

Limit of Liability/Disclaimer of Warranty: While the copyright holders, publishers, and authors have used their best efforts in preparing this work, they make no representations or warranties with respect to the accuracy or completeness of its contents and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. The advice and strategies contained herein are based on the author's experience and may not be usable for your situation. You should consult with an information security professional where appropriate. Neither the publishers nor authors shall be liable for any loss of profit or any other commercial damages, including, but not limited to, special, incidental, consequential, or other damages.

The World Changes – Do your written policies?

Auditors, regulators, and federal courts have consistently sent the same message - No organization can claim that it is effectively mitigating risk when it has an incomplete, outdated set of written policies. Written policies form the "blueprint" for the entire information security program, and an effective program must be monitored, reviewed and updated based on a continually changing business environment.

There are a variety of environmental and market factors driving the need to keep information security policies up to date:

1. **New Threats** – The world of information technology changes rapidly. The internet has enabled criminals to create newer, more sophisticated threats in shorter and shorter time periods.

2. **New Technologies** – To be competitive, organizations are constantly evaluating and deploying new technologies. Each new technology introduces new vulnerabilities and enables new threats. In today's mobile world, employees are bringing their own technology into the workplace.

3. **New Regulations** – In order to maintain a proper governance structure, organizations must respond to the even-changing regulatory landscape. New regulatory updates, guidance, fines and rulings may change the way in which security controls are implemented.

Each of these factors can impact the organization's own risk profile and possibly require additional or updated security controls.

Business Requirements for Updated Policies

Regulatory Requirements

Keeping information security policies up to date is not only good practice for reducing risk and liability – it is a consistent requirement in every data protection regulation across all regulated industries, including government, healthcare, finance, retail and energy. (Table 1) The first core element of the ISO/IEC 27002 international information security standard is the requirement to have written and updated security policies.

Reducing Legal Exposure

Written and updated information security policies are critical for reducing risk in lawsuits or federal sanctions. Many organizations have lost critical legal battles because their written policies were either absent, lacking or inconsistently applied. The updated *Federal Rules of Civil Procedure* now considers the analysis of written policies as a key factor in determining penalties. Organizations that fail to create an environment where security policies are consistently applied are more likely to suffer regulatory sanctions or increased fines.

Table 1: Specific Regulatory Requirements for Updated Security Policies

Regulation/Standard	Industry	Policy Update Requirement
ISO/IEC 17799:2005 Section 5.1 Information Security Policy Document	Security Framework	5.1.2 Review of the information security policy "The information security policy should be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness."
HIPAA Security Final Rule (Health Insurance Portability and Accountability Act of 1996)	Healthcare (U.S.)	Policies and Procedures 164.316 (a) (R) Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart.
Sarbanes-Oxley Act, Section 404 - based on COBIT (Control Objectives for Information Technology – V4.1)	All Publicly Traded Companies (U.S)	Control Objectives, Section 6: 6.2 Management's Responsibility for Policies PO6.3 IT Policies Management Develop and maintain a set of policies to support IT strategy. [...] Their relevance should be confirmed and approved regularly.
PCI-DSS Version 1.1	Credit Card	Requirement 12: Maintain a policy that addresses information security for employees and contractors 12.3 Are information security policies reviewed at least once a year and updated as needed?
Gramm-Leach-Bliley Act (GLBA) Title V - Section 501 Interagency Guidelines Establishing Standards For Safeguarding Customer Information	Financial Services (U.S.)	"Each Bank shall implement a comprehensive written information security program [policies] that includes administrative, technical and physical safeguards." III.E. Adjust the Program E. Each bank shall *monitor, evaluate, and adjust,* as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its customer information, internal or external threats to information.
FERC Cyber Security Standard CIP-003-1 Security Management Controls	Energy/Infrastructure (U.S.)	Requirement 1. The Responsible Entity shall create and maintain a cyber security policy that addresses the requirements of this standard and the governance of the cyber security controls. R1.3. *Annual review and approval* of the cyber security policy by the senior manager
Federal Information Security Management Act (FISMA) NIST SP 800-26	Federal Government (U.S.)	4.3.1 Security Program Management "An *up-to-date security policy* is written that covers all major facilities and operations agency-wide or for the asset."

Policy Update Challenges

Even for organizations that understand the need to regularly updated policies, there are a number of organizational challenges that can make it difficult to implement security policy updates:

Resource Constraints

There are few organizations that would consider themselves adequately staffed with respect to information security. In most organizations, it is just the opposite, with the information security department competing for staff and budget dollars with other revenue-generating departments.

Security policy development requires coordination with different business units and departments, with the review and sign-off process sometimes taking many months. With the desire to update policies on an annual basis, this creates a significant need for planning and coordination – further draining the time available for actually research and writing policies.

Qualified Staff

Even for organizations that have adequate security budgets and staffing, many internal personnel do not have the time or training to be dedicated to security policy development. Information security policies usually fall under more long term security goals, versus more immediate security requirements such system patching, anti-virus and incident response. Thus, security staff is often overwhelmed with immediate security needs.

Policy development takes a combination of business, technical and writing skills. It takes considerable time to research the latest trends, incidents and technologies in enough detail to formulate an appropriate policy control. Even then, it is difficult to assess a new policy in the context of broader industry standards such as ISO 27002, or as it addresses common regulatory requirements such as PCI-DSS, HIPAA or GLBA.

Organizational Resistance

Unfortunately, information security policies are often viewed as productivity inhibitors within some organizations. In some cases, senior management takes a “check the box” approach to simply do the minimum amount effort to satisfy regulators. While this is changing slowly, security professionals often need to “sell” senior management on the need for updated policies. This can involve a significant education effort highlighting the latest threats and incidents, and building a business case to show how policies can actually reduce the organization’s risk profile.

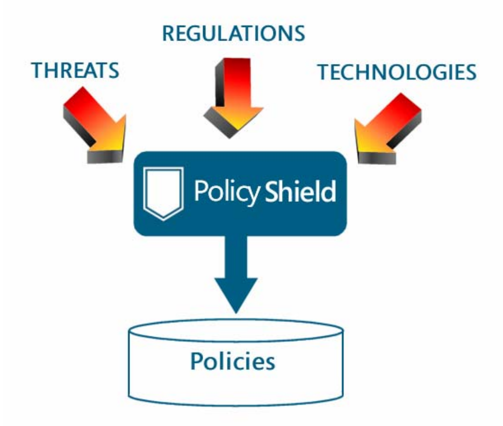
The deployment of new and updated policies also creates demands on the entire workforce. Policies need to be reviewed and acknowledged by various personnel according to their job roles and responsibilities. Updated technical policies may require changes to system settings or new technology deployment. All of these point to a need for policy updates to be regular, planned events rather than ad-hoc projects.

Staying Up to Date – PolicyShield Policy Subscription

PolicyShield is a new information security policy subscription service based on the "gold standard" policy development guide, *Information Security Policies Made Easy*. *PolicyShield* is design to allow your organization to build and maintain a robust set of written information security policies with the least amount of effort. To achieve this goal, the PolicyShield library is regularly updated with new policies and resources to help you address new risks.

PolicyShield acts as your "on-demand" security policy consultant. Our team of information security professionals continually monitors the technology landscape to look for new risks to your organization's information assets. These risks may include new threats (such as botnets), regulatory changes (including enforcement actions) and new technologies (instant-messaging, VOIP, etc.)

Each quarter we add more new policies to the existing library of over 1500 pre-written controls. Updates may include pre-written information security policies, policy development resources, sample documents, news items and policy-related incidents. *PolicyShield* is an extremely cost-effective way for an organization to keep written policies up to date and help protect against the latest threats.



Addressing Policy Update Challenges

PolicyShield can help address the common resource and organizational challenges to keeping security policies reviewed and updated. For example, *PolicyShield* enhances the productivity of internal staff by dramatically reducing research and development time to develop new policies. PolicyShield resources and templates further reduce the development effort by providing regulatory guidance, tools and checklists.

Security policies within the *PolicyShield* policy library are tied to the ISO 27002 security framework, with convenient mappings to additional regulatory and audit frameworks, helping internal staff build a common set of policy controls that satisfy multiple requirements. This "unified" approach to policy development can save time when coordinating efforts with legal, human resources and compliance efforts.

PolicyShield also helps build a business case for new policies by tying written policies to both real-world incidents and regulatory guidance. By eliminating the time required for research and policy development, internal staff can thus focus on the critical tasks of getting policies approved and integrated.

References and Additional Resources

[1] Payment Card Industry (PCI) Data Security Standard, Version 1.1 – Published September 2006, PCI Security Standards Council.

[2] 12 CFR Part 30, Interagency Guidelines Establishing Standards for Safeguarding Customer Information, February 2001, Published in the Federal Registrar.

[3] ISO/IEC 17799:2005 (ISO 27001) – Code of practice for information security management - Published by ISO and available at BSI [http://www.bsi-global.org/]

[4] Control Objectives for Information Technology (COBIT™) 4th Edition – Published by ISACA, November 2005. [http://www.isaca.org]

[5] Health Insurance Portability and Accountability Act of 1996 (HIPAA): Final Security Rule. Department of Health and Human Services; Published in the Federal Registrar.

[6] NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems, November 2001. Published by the National Institute of Standards and Technology (NIST).

[7] Information Security Policies Made Easy, by Charles Cresson Wood - Published by Information Shield, Inc. 2002-2005. [http://www.informationshield.com]

[8] Information Security Roles and Responsibilities Made Easy, by Charles Cresson Wood - Published by Information Shield, Inc. 2002-2005. [http://www.informationshield.com]