InformationShield

Building and Deploying Effective Security Policies

By David J. Lineman

Most security professionals will agree that security policies are a critical part of their information security program. In numerous surveys of corporate security programs, over 70% say that they have written security policies. And yet when pressed, most organizations will admit that they feel uncomfortable about the effectiveness of their security policies. In this article we describe 10 key steps for building and deploying effective security policies, using reference to Federal regulatory requirements as well as international security standards.

Defining Effective Security Policies

First, we must define what we mean when we say policies are "effective." One way to build this definition is by looking at the ways organizations feel their policies are *not* effective. For this discussion, we use the following criteria:

1. Effective policies adequately define the high-level security goals of the company to reduce operational risk.
2. Effective policies adequately protect an organization against legal action for possible violations.
3. Effective policies are read and understood by all employees and contractors in various roles within the organization.

Criteria #1 is based on the need for policies to be complete. An organization's policies must adequately cover the topics of an effective security program, including compliance with regulations. Criteria #2 reflects the organization's fear of damaging lawsuits, including possible violation of legislation. In fact, these fears are justified. Recent court cases are establishing precedents that would in fact hold most organizations liable. Criteria #3 reflects most organizations highest concern when it comes to

security. In fact, these three criteria are intricately related, and it is virtually impossible to adequately satisfy one without the other two.

Ten Steps to Effective Policy

In the following steps, we will discuss how each relates to the effective policy attributes listed above. One reference we make is to the guidelines of the US Sentencing Commission and the Office of Inspector General. [Ref. 1] They have defined seven elements for measuring if a breach in compliance has occurred. Another common reference we make is to ISO/IEC 17799 [Ref. 2], the international standard for security code of practice. We also provide tips within each section to help organizations achieve these goals.

1. Pick a standard structure for your policy documents

The policy development process is extremely challenging. Not only because of the subject matter, but because of the various personnel required to create, update, review and approve them. When done properly, policies follow a standard structure and are updated on a regular basis. Policies should include basic items such as effective date, responsible party, scope, exception reporting, and enforcement. The best way to encourage this is through a standard policy template used consistently throughout the organization. If our goal is to create a consistent security message that is read and understood by each member of the organization, the easiest way to fail is to have multiple different document types in different formats and in different places. (Only you know if this is true of your organization!)

A great way to help this process is to define three types of documents: Policies, Standards and Procedures. Policies are high-level statements that should remain relatively consistent over time. Standards, on the other hand, are the detailed items that enforce a high-level policy. Standards can be authored by department managers or IT staff, and can change more frequently. Procedures are the detailed steps that individuals will follow to implement the standards. This simple structure can be referred to as a “Policy Governance Structure” and can greatly reduce the simplicity of your security policy process.

This structure provides another great advantage that we will discuss in the area of monitoring compliance. By documenting procedures and standards in separate documents, organizations can easily map these business requirements against the security tools they monitor for compliance. Most security technologies, including firewalls, access control and vulnerability assessors are not designed to enforce a *policy*. They are designed to enforce a specific technical control on a particular platform.

2. Write it all down

Step #1 leads directly to the second requirement – making sure that you formally document all of your policies, standards and procedures. This requirement is either explicitly or implicitly stated in many security frameworks and regulatory requirements. The HIPAA Final Security Rule, for example, requires that policies and procedures are documented, and that these documents be kept for at least 7 years. The first "key control" of the ISO 17799 policy framework is to have a *written* security policy that is accessible to all employees.

The guidelines from the US Sentencing Commission note that an organization must have "documented" architecture of policy, operational, and technical controls. It sounds simple, but how can you validate compliance if you don't know what you are validating against?

If you don't have written policies, a good resource is *Information Security Policies Made Easy*, by Charles Cresson Wood. [Ref. 3] This resource contains over 1500 pre-written security policies covering all the domains of ISO 17799.

3. Assign responsibility for various security roles

This is another area where regulatory requirements are clear. It is critical that you identify and *document* key individuals who are responsible for various operational security roles.

For example, which high-level executive is sponsoring your security program? Which team or individual is responsible for updating security policy documents? Which team or individual is responsible for responding to security incidents? Most security or audit frameworks such as ISO 17799 and COBIT have clear requirements for assigning security responsibilities in these areas. However, if you don't document these, it is unlikely you will be able to prove that these roles actually existed. Imagine a trial lawyer asking for evidence that you were serious about security within the company. What document would you produce? How many times have you seen a policy document that has an "author" who is no longer with the company?

If you don't have documented security roles, a good resource is *Information Security Roles and Responsibilities Made Easy,* by Charles Cresson Wood. [Ref. 4] This resource has pre-written job descriptions and reporting relationships that you can easily customize.

4. Use a security framework

This item relates to Criteria #1 of *completeness*. Security frameworks are an organized set of security requirements, usually broken down into

numerous categories or domains. Fortunately, there are a number of these available. For example, ISO-IEC 17799:2005 provides a framework of ten security domains. The *Information Security Forum Standard of Good Practice* is another framework similar to ISO. [Ref. 7] For federal governments, the National Institute of Standards provides a framework for evaluating security in 17 key topic areas. NIST also provides guidance on how to measure effectiveness in each of these categories.

Security domains provide a benchmark for measuring the completeness of your policy program. Once again, if your goal is completeness – how can you measure progress against your goal?

5. Do risk assessments and have an exception process

Risk assessments are another key to effective policies. First, your policies should document when and how risk assessments are performed. In addition to being a foundation of most security programs, risk assessments allow organizations to define what levels of control are appropriate for their organization. If you look into the language of most security regulations, you see something like:

> "administrative, technical, and physical safeguards appropriate to the size and complexity of the [bank] and the nature and scope of its activities." – *Gramm-Leach-Bliley Act, Title V [Ref. 5]*

For example, the HIPAA Final Security Rule has a number of "required" and "addressable" controls. Addressable controls are deemed optional providing that an organization document that they performed a risk assessment and why they chose not to implement a particular control.

Once again, imagine facing the trial attorney who is asking that you document that your organization followed "due care" in your security program. Would a formal risk assessment help?

Key to this process is a "Risk Acceptance Memorandum." This is a simple form that documents who is accepting the risk, how long the exception should last, and what mitigating controls are in place. Sample risk acceptance memos are widely available on the internet.

6. Communicate your policies regularly

This requirement would be the "Achilles Heel" of policy. You have heard it by various names including "shelfware" and "policies collecting dust." And yet precedent after precedent shows that this is key to any policy program. For example, a number of lawsuits have been filed and won by employees who were fired for security policy violations. When the court

looked at the data, they found that the companies rarely or never communicated their policies to employees in the company.

In a recent lawsuit against a large public company, the court ruled that a simple email notification was not sufficient to notify employees of a change in policy. In fact, employees must acknowledge the receipt of this notification and demonstrate that they have some understanding of how the changes would affect them.

The Federal sentencing guidelines are clear on this point. Organizations must communicate compliance program requirements effectively, and employees and business partners must be aware of their role in complying with laws and policies. This is a key point: employees and partners must be aware of their *role* in security and compliance.

Communicating is not only required for your policies to be enforceable, is addresses the key area of security awareness. What better way to create security awareness than to educate your users on your own policies? Again, security-related regulations are clear on this point. For example, the HIPAA Final Security Rule requires security awareness and training in

> *[…organizations must] "Implement a security awareness and training program for all members of its workforce (including management)."*
> - *HIPAA* [section 164.308(a)(5) – Ref. 6]

7. Enforce consistently

Policies should document the process of enforcement, including who is responsible for enforcement. Policies should also be enforced consistently. Holding employees responsible for security, but given exemptions to senior executives is a common practice. Not only does this send a bad message to employees, but it will unravel your compliance program. The Federal sentencing guidelines state that "controls [policies] must be uniformly applied in the organization as they support compliance objectives."

Again, imagine yourself in front of the trial attorney, providing documentation that you have consistently enforced your policies. The first document would be your *documented* sanctions policy, and then the audit log which shows that *every* employee in the company understands what might happen in the event of a security violation.

8. Include incident response

Policies should define the organizational goals and responsibilities for incident response. Most organizations will experience security incidents, and the level to which they respond and recover can have serious impact

on their business. Not only is incident response a key element of security frameworks, most legislation that defines security requirements has specifics about incident response.

Incident response policies should not only define what an incident is, but they should clearly define how incidents should be reported and handled. Guidelines should be established on when and how incidents should be report to law enforcement. Once again, critical parts of your incident response policy should be communicated to employees and business partners.

A question to ask yourself is this: Would your employees know how and where to report a security incident?

9. Audit your policies for compliance

Your entire policy framework should be designed around the concept of auditing. Once again, performing security audits is a key part of security and regulatory frameworks. "Compliance" is the tenth key domain from ISO 17799, and includes action items like "reviewing security policies and technologies for legal and technical compliance." But what are you auditing against? The answer is your stated policy.

When you write a policy, you should consider what evidence would support an audit of this policy. For written policies, it may simply be the written document. When you create a standard or a procedure, it is a good idea to create the "test case" for that procedure. While auditing can be done easily on certain technologies, the questions get a bit trickier when we involve the human elements of security. For example, how can I verify that every employee in my organization has read and understood our security policies? Do I have evidence or an audit trail to support this?

10. Use automation for enforcement and auditing

As you consider all that is required for an effective policy program, you quickly realize that doing all of this "by hand" is nearly impossible. For example, how can I distribute my policy documents to every user in a company of 5,000 employees, and then demonstrate that they have read and understood them? Similarly, how can I verify that all of my Windows and Unix systems are enforcing my stated password and automated logoff standards? The only effective way is through automation.

This is an area where recent developments in automated policy tools can help. New intranet based tools, such as VigilEnt Policy Center from NetIQ Corp., can actually target individual policy and procedure documents at various individuals based on their organizational role. Management

reports organize and track who has read and acknowledged policy documents by department or role. These tools provide detailed audit logging of which policies were effective on which dates, and who signed off on which policies. Thinking like an auditor, these tools provide a great way for organizations to demonstrate compliance with training and awareness requirements.

On the technology side, there are numerous host-based vulnerability assessment tools that can verify the security settings on your various platforms. This is where the organization of your documents is key: If you define detailed standards in a separate document, you can easily verify that the controls (i.e. the individual machine settings that enforce these standards) match what is written in your documents.

Summary

Security policies form the foundation for your security and compliance programs. However, having written policies is not enough. Policies must possess certain criteria if they are to be effective in reducing organizational risk. Following these steps will dramatically increase your ability to defend yourself in both audits and possible lawsuits relating to information security.

About the Author

David Lineman is President and CEO of Information Shield. Mr. Lineman has 20 years of experience in software development, business consulting and security. He is a frequent speaker on the subjects of security policy and regulatory requirements.

References

[1] Federal Sentencing Guidelines, United States Federal Commission, November 2003. [http://www.ussc.gov/GUIDELIN.HTM]

[2] ISO/IEC 17799:2005 – Code of practice for information security management - Published by ANSI [http://www.ansi.org/]

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

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

[5] Gramm-Leach-Bliley Act, Title V – Federal Trade Commission. Also published in the Federal Registrar. [http://www.ftc.gov/privacy/glbact/]

[6] Health Insurance Portability and Accountability Act of 1996 (HIPAA): Final Security Rule. Department of Health and Human Services; Published in the Federal Registrar. [http://aspe.hhs.gov/admnsimp/index.shtml]

[7] *Information Security Forum Standard of Good Practice,* Published by the Information Security Forum. [http://www.isfsecuritystandard.com/index_ie.htm]

informationshield.com

2660 Bering Drive Houston, TX 77057 TEL 1.888.641.0500 FAX 713.783.5365