

Developing Effective Security Policies

By J. Craig Lowery, Ph.D.

Security measures are most effective when they arise from well-designed, comprehensive, broadly communicated organizational policies and are enforced by human engagement as well as technical solutions. This article discusses the importance of security policies and examines the security policies required in most organizations. It also provides guidelines on how to develop, implement, and enforce policies that are effective without being overly intrusive.

The need for increased computer security is driving organizations to shift significant portions of their IT budgets to fund the acquisition and deployment of security solutions. However, many implement unbalanced strategies that focus almost exclusively on the technical components, such as intrusion detection and prevention systems, public key infrastructures (PKI), user authentication, and access controls. Without a doubt, components such as these are crucial to creating safe and secure computing environments in a global climate replete with cyber-terrorism and fraud, but they are only half of a comprehensive security plan.

Many organizations lack a policy structure to back up the technical security systems they deploy. Although they have some policies in place, these policies are often incomplete or out-of-date. Policy gaps can become vulnerabilities as surely as poorly written code in an operating system; the latter simply receives more attention in the mainstream press, which unfortunately drives priority assignments in many IT departments. This article discusses the importance of organizational security policies and presents guidelines for assessing policy gaps, developing new policies, driving adoption and enforcement, and assuring periodic re-evaluation.

The security policy life cycle

Figure 1 shows a model incorporating the nine phases of the security policy life cycle:

- 1. Draft:** Representative committees write policies.
- 2. Adopt:** Administration reviews and approves policies.
- 3. Implement:** Administration defines procedures to implement the policies.

- 4. Educate:** Users receive information and training about the new policies and procedures.
- 5. Deploy:** Policies are put into effect; related technical solutions are deployed.
- 6. Monitor:** The information security department observes the computing environment for policy violations.
- 7. Enforce:** Violators are punished as prescribed by policy.
- 8. Re-evaluate:** Policies are periodically reviewed for continued relevance and accuracy; some may be retired at this point.
- 9. Revise:** Policies are revised as needed to keep them current, relevant, and accurate.



Figure 1. The life cycle of a security policy

Policies begin life in the draft stage and repeat the cycle over a period of years until the organization finds the policies irrelevant in step 8 and subsequently discards them. Each step in the policy life cycle is important, as is the order in which these steps occur. For example, monitoring and enforcement of a policy should not take place until users have been informed of the policy and have had opportunities to ask questions.

Each step in the policy life cycle is important, as is the order in which these steps occur.

Complete security coverage

The scope of computer security policies has evolved to be considerably larger than that addressed by the traditional acceptable use policy (AUP). Each new method of accessing a computer system—and each new technology developed to secure that access method—results in a new policy objective. For example, the addition of wireless networking introduces the possibility of a violator installing an unauthorized wireless access point, thus compromising a private network. A policy that sets forth requirements for deploying wireless technology in such an environment is essential.

Through its Security Policy Project, the SANS (System Administration, Networking and Security) Institute has developed several model security policies, which have been implemented by many large organizations. These model policies, in the form of templates, are available in the SANS reading room (<http://rr.sans.org>) and are freely accessible to any organization wishing to use them as a basis for developing security policies. The following list of SANS model policies demonstrates the breadth of coverage required to meet all aspects of modern computer system security.

- ▶▶ **Acceptable Encryption Policy:** This policy helps to ensure that encryption methods used in the organization have passed public review and are proven to be effective. It also addresses legal issues, especially where export law is concerned.
- ▶▶ **Acceptable Use Policy (security specific):** This policy defines what is and is not acceptable use of an organization's computing resources with respect to privacy, confidential information, copyright, unsolicited communication, hardware theft prevention, free speech, and related issues. This security-specific policy may complement a broader AUP.
- ▶▶ **Analog/ISDN Line and Dial-In Access Policies:** These policies help protect against intrusion through dial-in access and against espionage through dial-out connections. The policies also help control who can order fax and modem lines by instituting an approval process tied to business cases and strict operational requirements. In addition, they define the process for obtaining dial-in access, the rules for appropriately granting such access, and the situations in which dial-in access should not be used (such as unencrypted mobile phones).
- ▶▶ **Anti-Virus Process:** This guideline provides recommendations for preventing viruses and related problems such as spam, chain mail, executable e-mail attachments, unknown download sources, infected floppies, writeable file shares, and infrequent backup. Although this document is written as a guideline (suggestions that are recommended but not required), many will want to adopt it as a policy (requirements that all within the organization must meet).
- ▶▶ **Application Service Provider (ASP) Policy:** This policy establishes rules for determining, largely based on information sensitivity, when it is appropriate to host a project outside the organization. An associated document should define base-level security standards that an ASP must meet to be considered as an external host for the organization.
- ▶▶ **Acquisition Assessment Policy:** This policy defines how an organization assimilates the computing assets of an acquired organization. It provides guidelines for replacing, re-imaging, or auditing systems and networking components and for re-establishing Internet connectivity.
- ▶▶ **Audit and Risk Assessment Policies:** These policies empower the security team to conduct security audits and risk assessments on any computer system or component owned by the organization.
- ▶▶ **Automatically Forwarded E-Mail Policy:** This policy prohibits unauthorized forwarding of e-mail to external systems.
- ▶▶ **Database Credentials Coding Policy:** This policy specifies that usernames and passwords used by a program to log into database systems must be stored securely and external to the program's source code.
- ▶▶ **Extranet Policy:** This policy governs how third parties gain access to the organization's intranet. It requires organizations to review the third party's security readiness and the business case justifying the access.
- ▶▶ **Information Sensitivity Policy:** This policy defines levels of information sensitivity such as "restricted," "confidential," "internal use only," and "public." It defines appropriate forms of data storage and distribution for each level.
- ▶▶ **Internet DMZ Equipment Policy:** This policy establishes standards to be met by all equipment deployed outside of the organization's private network or within its demilitarized zone (DMZ).

- ▶▶ **Laboratory Policies:** For organizations with development labs that must relax computer policies to perform their work, several policies exist to define such relaxations and to stipulate additional requirements such as naming an individual to be the single point of administrative contact.
- ▶▶ **Password Protection Policy:** This policy sets password management standards such as maximum password life, global password databases, rules for constructing strong passwords, and prohibitions against password sharing or divulgence.
- ▶▶ **Remote Access and VPN Security Policies:** These policies govern all forms of remote access across all classes of individuals performing such access. Essentially, they extend all relevant internal security policies to remote access. They provide additional rules for virtual private networks (VPNs), such as requiring that all network traffic pass through the VPN when it is active, instead of over both the VPN and the unsecured connection.
- ▶▶ **Router Security Policy:** This policy sets router configuration standards for the organization, such as packet-filtering rules to prevent spoofing, Simple Network Management Protocol (SNMP) community settings, and “no trespassing” signs.
- ▶▶ **Server Security Policy:** This policy establishes standards for server configuration and registration, such as disabling of unnecessary services, mandatory logging of services, timely patching, limitations on trust relationships with other servers, and physical security of server hardware.
- ▶▶ **The Third Party Network Connection Agreement:** This agreement is a contract between the organization and a third party for which the organization will provide network connectivity.
- ▶▶ **Wireless Communication Policy:** This policy defines minimal encryption standards and restrictions on deployment of unregistered wireless access points within the organization.

Hallmarks of effective security policies

Because security policies govern by defining appropriate and inappropriate behaviors, they are naturally susceptible to opinionated discussion. Effective security policies are supported by the majority of those governed while at the same time protecting the interests of the organization. To the extent possible, such policies have the input of those governed.


Organizations often convene committees charged with drafting policies. These committees are usually chaired by a senior individual with job responsibilities in the area governed and composed of representation from legal counsel, affected support staff, and users. Once drafted, the policies should be reviewed by a larger group of similar makeup.

Policies should be clear without being overly specific—general requirements documents, not implementation plans. Documentation of related procedures is necessary but should be separate from the policies themselves. If a policy includes too many details or variable data (such as a requirement directed specifically at the virus threat of the moment), then it must be revised more frequently to stay current. Furthermore, policies that micromanage or over-regulate tend to squelch productivity and engender user contempt because they can become unwarranted roadblocks to completing job tasks.

Without enforcement, effective policies can do little to improve the security of an organization’s information systems. All policy templates referenced in this article include an enforcement section explicitly stating that violators will be disciplined. Discipline is typically an action taken by the human resources department through measures such as performance penalties or even employment termination.

Finally, effective policies provide a framework and motivation for educating users by directing their attention to what is most important in building a secure computing culture. Because security policies dictate what is and is not appropriate behavior, and because they empower the organization to act against those who do not comply, policy objectives should be incorporated into employee orientation curricula.

Staying current

Although effective policies will be resilient to change, they must be evaluated periodically and updated as needed. New technologies, new solutions, or simple cumulative changes in the IT environment can create gaps in policies and procedures, rendering an organization vulnerable. IT organizations should schedule annual reviews of policies and procedures to help ensure that they remain congruent with the current environment. Furthermore, events such as major upgrades, new software deployments, or new technology deployments should trigger re-evaluation of related policies. 

J. Craig Lowery, Ph.D. (craig_lowery@dell.com) is a software architect and strategist in the Software Development Group of the Dell Enterprise Systems Group. Craig received an M.S. and a Ph.D. in Computer Science from Vanderbilt University and a B.S. in Computing Science and Mathematics from Mississippi College. His primary areas of interest include networking, performance modeling, and operating systems.

FOR MORE INFORMATION

For more information on security policies, please visit the SANS Institute Information Security Reading Room at <http://rr.sans.org>