

Information Security Policy Essentials

Bill Young, CCSE, CISSP, Security Consultant, Chesapeake NetCraftsmen, LLC

Security Policies establish ground rules. They're just as essential to an organization as Human Resources policies, emergency procedures, and bookkeeping.

To many people, firewalls are guardians, weapons "in-hand," perched at the entrance to the network, ready to fend off attacks. Firewalls can help protect networks, but they're really just one element of a complete security program – based on security policies. Here are some scenarios that a firewall can't address:

1. One of your employees is harassing another through your e-mail system or instant messenger
2. A manager is downloading copyrighted music at the office, exposing your organization to liability
3. A UNIX administrator abuses his knowledge to open an outbound SSH session to the internet, and then uses that session to tunnel a back door into your network. He may have done this so that he can perform legitimate job functions, but he's just bypassed your two-factor authentication VPN solution

Security Policies establish ground rules. They're just as essential to an organization as Human Resources policies, emergency procedures, and bookkeeping. When employees use work resources for personal use, they can be held responsible, and possibly terminated. Why? Because it's against the rules. Security policies enable organizations to protect their information resources in the same way. By documenting your policies and educating your users about them, you extend the responsibility of security beyond your security team. Everyone plays a role. And everyone understands their individual responsibility and accountability.

Developing Security Policies

1. The first thing to determine is the scope of the policy you'll need – what it will cover. The key things to identify are the needs of the security team, IT management, senior management and the legal department. You'll want to assess the risks to your data and to the business as a whole. And you'll need to understand the worst-case consequences if your data is compromised.

Security Policies can include topics such as:

- Acceptable Use Policy for End Users
- Analog Line Policy
- Systems Security Policy (you could have multiple policies covering the unique security requirements for different environments (UNIX, Windows, Network, etc.)
- Vulnerability Scanning Policy
- E-Mail Policy
- Information Sensitivity Policy
- Remote Access Policy
- Wireless Policy

2. After you've documented the risks and identified the policies necessary for your organization, it's time to write the security policy. The most important requirement is keep it simple. You're writing for your user community. Avoid technical jargon or legal terminology that won't be understood by the total audience. If you feel that technical or legal details are necessary, use separate documentation for those details:

- Spell out technical requirements in a separate document, such as a Security Implementation Plan
- A Legal Security Policy may be appropriate, outlining security response by your legal team

3. Along with **keep it simple**, it's also a good idea to **keep it small**. Instead of creating a single, comprehensive document containing all of the policies for your organization, develop a modular solution. That offers a number of advantages. It's easier to change a single policy without impacting others. It's easier to obtain senior management approval on changes to shorter

documents. And modular policies are far easier and more cost-effective to distribute whenever changes are made.

Maintaining a United Front

1. For a security policy to be effective, it has to be enforceable, actionable and endorsed by the organization. Senior Management must be in agreement with the need for the policies, as well as **the reasons behind them**. If you only present the policy to the CIO, explaining that it's necessary for audits or other industry compliance, it's likely the policy will be rubber-stamped, placed in a binder, and only shown to auditors once a year.

2. Security Policies are the glue that holds an organization's InfoSec tools and corporate security procedures together. That's why it's important that senior management understands the policies, agrees that they are necessary, and is prepared to enforce them.

3. Any company with staff is aware of the issues and costs associated with improperly handling disciplinary processes and legal action. For those reasons, it's imperative that a legal representative review the policy to ensure that it is enforceable. It's also advisable to consult the Human Resources department.

As Soon as You're Done, There's More to Do

You've developed a security policy. (Whew, what a relief.) Now comes the realization that 40% of your systems violate your new policy. Don't worry – that's a good sign. It shows that you didn't develop the policy to work around your current security issues. You've recognized them and the need for their resolution.

That's why, along with a security policy, you'll want to build an implementation and remediation plan. Document the deficiencies you've found and present them during the approval process. By being up-front, you enable management to analyze the risks and to review the costs of remediation of those issues.

There's no such thing as a 100% secure network. If the cost of implementing the perfect security plan is too high, it's possible that exceptions need to be made. That's far better than ignoring sections of the policy that just aren't feasible. If that happens, it's the beginning of the end for your security policy.

If You Tell Them, They Will Know

Employee education is critical. Your Security Policy will only work if everyone is made aware of it and understands what is and isn't permitted. Often, employees are required to sign a form stating that they've read, understand and agree to the policy. (Consult your legal and Human Resources teams to ensure that you are in compliance with regulatory and legal requirements.)

Educate your users and new hires with training sessions. Employees have an interest in the company's success. If they understand why an activity hurts the organization, they are much more likely to support the policy and participate in its implementation.

Regularly Review the Policy

Inevitably, there will be changes to your network, your business plans and your security requirements. Set up a procedure to ensure that the Security Policy is regularly reviewed as well as when changes occur. Enforcing an obsolete Security Policy is difficult (or impossible) from both a functional and legal perspective. Revisiting your policy protects the work you've accomplished and maintains a secure environment.

Sleep Well at Night

By creating a multi-tiered, Defense in Depth Security Policy, you are building the fortifications that will protect your organization. There is no such thing as a hacker-proof network. But with effective security planning, design, implementation and operations, you can drastically reduce your risk, improve network availability...and sleep better.

Chesapeake NetCraftsmen, LLC delivers high-availability solutions for Network Design, Operating Systems, Applications, Security, Storage and IP Telephony with deeply experienced CCIEs who excel at Knowledge Transfer.

Chesapeake NetCraftsmen consultants include some of the most experienced Cisco CCIEs in the country. Most of our technical staff has a minimum of 10 years' networking experience and many have taught Cisco Certified training. Knowledge Transfer is a key part of every Chesapeake NetCraftsmen engagement, making certain that clients understand how to run and manage their newly implemented or re-structured networks.

For more information on Chesapeake NetCraftsmen, [click here](#).