
# The Security Policy

### Terms you'll need to understand:

- ✓ Security policy
- ✓ Security wheel
- ✓ Secure
- ✓ Monitor
- ✓ Test
- ✓ Improve

### Techniques you'll need to master:

- ✓ Separating a security implementation into stages
- ✓ Assigning a task to a stage in the security wheel

Cisco is quite plain in the SAFE Blueprint: "This document presumes that you already have a security policy in place. Cisco Systems does not recommend deploying security technologies without an associated policy." Everything that follows from this early paragraph in the Blueprint assumes that you are implementing your organization's policy; the Blueprint is about the technologies to do that effectively. To look at the problem another way, the SAFE Blueprint offers the most effective technical means to do the job; the security policy defines the job to be done. If you don't know what you're supposed to be doing, how do you know if you've done it well—or done it at all?

# What a Security Policy Is

An organization's security policy often contains a number of policies, each addressing a particular problem, such as remote access, encryption, email retention, and password management. (You can view examples at the SANS Web site in the resource list at the end of the chapter.) But taken as a whole, a security policy answers some very basic questions for an organization:

- *Assets*—What do you want to protect?
- *Threats*—What are you protecting them from?
- *Risks accepted*—What threats are you choosing to not counter (or not counter completely)?
- *Security technologies*—How will you protect your assets?
- *Authorities*—Who has the power to implement these policies?
- *Acceptable use*—What responsibilities does everyone have?
- *Audit*—How will you know if you're compliant with your security policy requirements?
- *Incident response*—What will you do if something goes wrong?
- *Revisions*—How will you make changes?

As you can see, a security policy is based on security concepts, which build in a logical sequence, but it actually covers quite a bit more. The "quite a bit more" is necessary, though, to make the security choices work. Among the additional material is the endorsement of the organization's highest management, which gives the policy its teeth.

Especially in the current litigious environment, enforcing policies that have been adopted to protect the organization is important. Of course, this means

that the security policy adopted must be enforceable. Often the real world doesn't work quite the way you expect, so you have to go back and refine your plans. Cisco uses a concept called the security wheel to address that problem. We'll cover the security policy itself, and then how it is managed and improved via the security wheel.

## Assets

Every organization has a unique set of assets to protect. However, the protection starts with enumerating them, understanding what they are, and why they are valuable. Typically, assets are described by a combination of location and hardware and/or software type. Some security policies spell out the risk to the organization if this asset is compromised, corrupted, or lost (as in a physical disaster). For another look at enumerating assets, review Chapter 2, "Information Assets."

## Threats

This portion of the security policy describes the threats to the organization's assets. Not all threats are network threats, per se. Physical security matters, too—physical access by an unauthorized person makes many cybersecurity technologies irrelevant. The threats listed are those that can make the assets less valuable to the organization, and they depend partly on what assets the organization has. Threat types were discussed in more detail in Chapter 3, "Threats."

## Risks Accepted

Most organizations do not choose to protect against every possible threat (for instance, the threat of flooding in Las Vegas, Nevada). Two questions must be addressed:

- Is the threat likely to materialize? If so, what will it cost?
- Can you protect the threatened asset at a cost less than the financial risk involved?

Both questions must be answered affirmatively before it becomes prudent to counter the threat. Business resources—and security resources—are limited and must be used where they will actually do the most good.

Some organizations simply do not mention the risks they choose to accept. Others clearly state the threats they have chosen not to counter and the reasons why. This might offer them protection in legal proceedings because

they can show that they considered the matter (as opposed to being negligent, or worse) and that they applied their limited resources to more likely risks. That choice should be taken only after consulting the organization's legal adviser because laws and liability practices vary widely.

## Security Technologies

This portion of a security policy covers the technical means by which an organization protects its assets. These can include networking architectures, encryption, firewalls, intrusion-detection system (IDS) sensors, and antivirus protection.

Not all security technologies need to be used, and not all assets need to be protected in the same manner. For instance, some data, such as empirical test data, might be costly to replace, and security technologies should include those needed for disaster recovery. Other data must be protected from unauthorized access, requiring strong use of access controls and possibly encryption. The appropriate technologies depend on the nature of the assets, the threats to the organization involving those assets, and the level of risk the organization has chosen to bear.

## Authorities

This section declares the security policy to be a matter of policy for the organization, and it designates who within the organization has the authority to implement the policy or portions of it. That first part might seem a little vague, but it is the key to the policy's teeth. The organization's management specifically endorses the security policy and requires compliance with it. As a result, violations of the policy are not condoned (which is usually more legal protection for the organization).

More of interest to most network administrators and engineers is the designation of who has the authority to implement given technologies. This is usually IT or IS, but some portions, such as physical access control, might be given to other organizations.

## Acceptable Use

This portion describes what activities are and are not allowed with the organization's information assets—those that are and are not acceptable use (AU). Amazingly, outside auditors have discovered pornography sites hosted on organizations' networks, and those businesses have been able to do nothing more than remove the materials: They could not terminate the people who

ran the site or even reprimand them. The reason? The organizations never stated that such use was not acceptable, and legal counsel advised that they would not win a challenge.

More mundane, but also important, is whether the organization allows personal use of the network and other information assets. Is all personal email verboten? Is IM/IRC (Instant Messaging/Internet Relay Chat) allowed, but only approved IM software and for business use only? Some AU policies are very detailed; others simply require that the business assets be used only for business purposes. There should also be statements concerning whether email, IM, and/or IRC will be monitored.

## Audit

No one loves an audit. But just as in financial matters, an audit determines whether things really are as good as they seem or whether trouble lurks beneath the placid surface. This part of the security policy specifies who is authorized to perform security audits (which implicitly rules out people doing their own checks, including unsolicited penetration tests). It might specify audit frequency requirements as well (such as having the full network audited annually but critical systems audited quarterly). Much of IT audit efforts depend on system and activity logs, so policies addressing logging are likely to be in this section.

## Incident Response

Despite the best of plans and implementation, sometimes something goes wrong (also known as "things happen"). A good security policy plans for this with an incident response section. This details who will respond and in what ways: who will constitute the team to respond to the incident, who will gather which data, how the data will be handled, what checklists will be prepared in advance, and so on. The quality of the organization's response is generally directly proportional to the degree of preparation, a general truth amplified by the fact that incidents are inherently disruptive to normal operations.

## Revisions

"No plan survives contact with the enemy" is one of the principles of military thought, and the general idea behind it applies to the security policy as well. The business network will evolve, some assets will be added, and other assets change character. The security policy must have a mechanism to evolve and change with the network. That mechanism might simply be a

general statement that changes discovered in the annual audit will be incorporated into the operating security policy. It could also lay out a formal change-management system, complete with proposal, review, and acceptance procedures. But revision as well as implementation is the idea behind the security wheel.

# The Security Wheel

The security wheel is a figure symbolizing the iterative process of network security. At the heart of the process is the Network Security Policy. The security wheel is shown in Figure 4.1.


You might see the entire process visualized in the security wheel described in other Cisco documents or Cisco Press books as a Security Posture Assessment, or SPA. Regardless of which term is used, the idea is the same: It is an iterative process to improve the security of a network. For the CSI Exam, you will probably not see the term *SPA*, but you might see a reference to the security wheel.

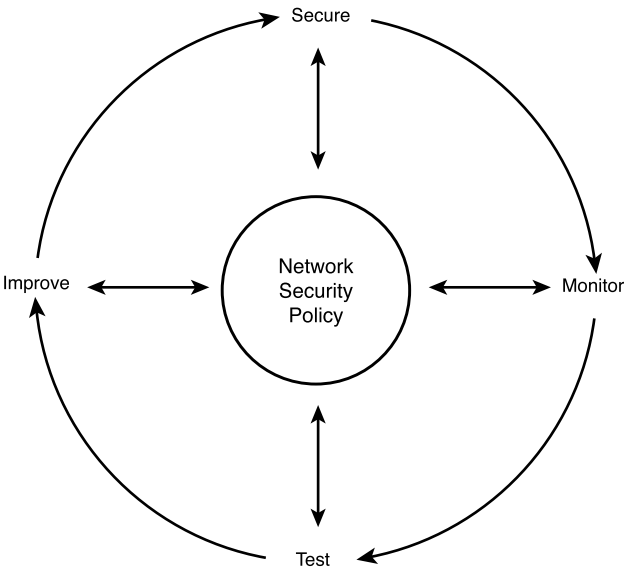


**Figure 4.1** The security wheel.

Everything you do in the process of securing, monitoring, testing, and improving security occurs with reference to the network security policy. Because it is an iterative process, we could start anywhere, but for convenience we'll take it from the top.

## Secure

This is the stage where many things can change: It could also be called the implementation stage. At this stage of security, the technologies are actually applied to the network. The Secure stage can be done in pieces of varying size, depending on the needs being addressed and the comfort level of those who are responsible for making it happen (which could be IT management or even corporate management).


The SAFE Blueprint uses a modular approach when tackling the implementation of security on a network. Handling things in this way has two advantages. First, each module's security needs can be developed and implemented independently of what happens in other modules, keeping a problem to a reasonable size in both management and cost. Second, the architecture can focus on the relationship between any two modules. If you see a multidevice simulation problem on the exam, you should follow the same approach: Tackle it in pieces.

In the Secure stage, hardware is deployed in the form of firewalls, VPN concentrators, more switches and/or routers to isolate problem traffic, and so forth. Simultaneously, configurations on existing devices usually must be changed. Access controls are refined (or added), AAA is implemented, unused ports are disabled, routing update authentication can be implemented, and so on. The endpoint of this stage comes when the secured network is operational: Testing and troubleshooting are complete (in terms of the additions and modifications made).

## Monitor

It is always possible to collect so much data about the network's behavior that it is not all read. However, some data is more important than other data, and the point of the Monitor stage is to observe the data that indicates the behavior of the security devices and processes.

SAFE assumes that you monitor the critical ingress and egress points on your network, as well as the security measures placed on interior significant assets. This is the stage in which you look for weaknesses that you did not know existed or possibly chose not to repair, whether for technical or financial reasons, and watch to see if others attempt to exploit them.

Part of the Monitor stage involves responding when you detect a problem. This interaction with the security policy will probably lead to revisions and improvements after every major incident (which, hopefully, will be both few and seldom). Depending on your specific IDS and its settings, you might have automatic responses for an incident or access attempt. In that case, an important part of the Monitor stage involves validating that the response

happened as it should. That might require you to compare data from perimeter device logs against IDS logs. During any investigation, of course, you will be comparing entries from numerous logs and cross-checking what happened where and when.


During the Monitor stage, as you compare data from multiple devices, it is very important that the devices have synchronized clocks. A subtle attacker might change the system time on a device to help hide his trail in the log analysis, something we'll talk about again in Chapter 5, "Management Protocols and Functions." You should know what it takes to be sure of the accuracy of the time stamps in your monitored data.

# Test

This stage of the security wheel is one that you might have to explain to management because it is different from the way that most business operates. The speed of change varies among industries, but the IT sector has a very rapid rate of change. Those who try to advance their careers are acutely aware of this, of course, as the volume of material to know seems to grow more rapidly than the time available in which to learn it.

However, this is even more true when it comes to security. Many hackers who develop attacks are the most knowledgeable people about how systems work. Hackers have been known to explain to developers exactly what happens in various operations of the developers' own software. Although these hackers are numerically rare, the tools that they develop are often widely available and frequently are copied and used by a large community, some of whom craft improvements or refinements that they, too, make available.

In most product development, managers would love to have this kind of virtuous circle effect. The result for security, however, is that some of the fastest product development takes place on the other side—new vulnerabilities are constantly uncovered and are often exploited within days, at the most. That makes the testing stage an unsung hero in protecting the network.

The testing stage is not about testing what you have against the threats that you designed against (the existing product competition). It's about testing against the new threats as they emerge (the next generation of competition). What's more, you test the network as it exists at the moment, which is not necessarily as it was when the last audit was conducted. That matters because networks as well as threats evolve: New hosts are added, new applications are deployed, patches are added, hardware is upgraded, existing software is moved to different hosts, and so on. In other words, the testing stage is about knowing where you stand against the competition's latest and greatest options, the ones most likely to wreak havoc. Unfortunately, too many people are unprepared.

## Improve

In this stage, you determine the changes needed, as identified during testing. Cisco understands that this is often a hard sell to management: You must justify the cost in terms of something not happening, without being able to guarantee that it absolutely would happen if you don't make the changes. Nonetheless, unless you make the improvements, security will stall at one level of protection while the threat evolves to another. This stage, of course, morphs into the first stage (secure) as you actually get the new improvements into place.

# Tradeoffs

The SAFE Blueprint is intended to lay out an architecture that implements a secure *and* functional network. As with any operating arrangement in which two sets of goals do not align (such as politics), compromises must generally be made to get anything actually done. You might see a graph like the one in Figure 4.2 in any book about implementing security; it helps you visualize where and when to make the compromises. (The SAFE Blueprint has design alternatives available to help you frame the compromises.)

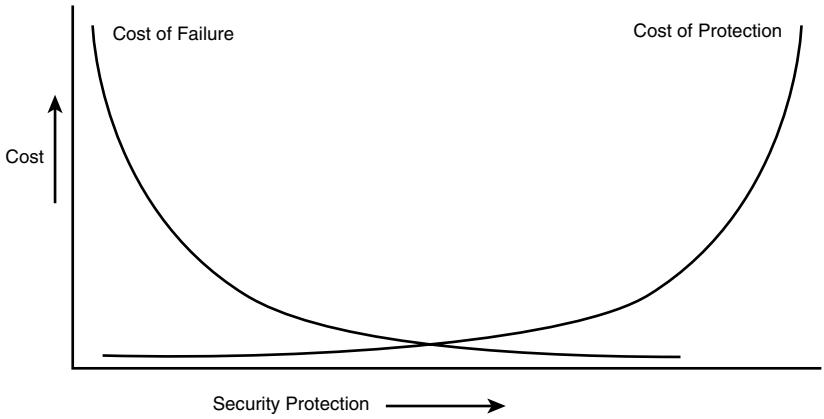


**Figure 4.2** Tradeoffs between cost and protection.

The more you increase your security protection, the more it will cost you, and the costs increase at an increasing rate because the cost of more sophisticated protection increases rapidly. At the same time, as you increase your security protection, the cost of failure declines, though at a decreasing rate (because the protections become more problem-specific and thus have a narrower applicability across the spectrum of remaining issues).

As you progress in applying the SAFE Blueprint to a network, the principles behind Figure 4.2 will be one of your guides. Many security exposures could be corrected, but some will not be financially feasible. With no security protection in place, so many possible points of failure exist that the cost is very high. At the same time, many security improvements are not expensive to implement, although some improvements (such as a stronger password policy) lead to human inconvenience and higher indirect costs.

The net result is that you will reach a point at which the cost of the security improvement exceeds the savings from reduced security failure cost. There is no business reason to go further—and SAFE recognizes that the network and its security are subject to business analysis, just like any other organizational expense.

# Example Security Policy

Remember that the CSI Exam is focused on the SMR SAFE Blueprint. That Blueprint assumes that an appropriate security policy is in place and is being enforced. As you think about implementing SAFE (and that is the title of the exam: "Cisco SAFE Implementation"), you are implementing a design that is intended to implement a security policy.

The *Cisco Security Configuration Guide* has a section that discusses security policies, but sometimes it helps to look at one that could be used by a real business. The following example is an example that is appropriate to a small or medium-size organization. It provides one last bit of foundation that Cisco assumes you already have in place when you think about implementing SAFE. Note that by actually enumerating assets and technologies in the appendixes rather than the body of the policy, the company has simplified the revision process. This example is used by permission of $S^2$ Networking, Inc.

## Example Security Policy

**Information System (IS) Security Policies**

© $S^2$ Networking, Inc.

**Statement of Authority and Scope**

<Company Name> ("the Company") uses an internal information systems (IS) network ("the network") with access to external IS networks, including, but not limited to, the Internet. The network exists to further the Company's business. Every person using the network is expected and required to treat the network and its components as a business asset. Users have access via the network to information with a wide range of sensitivity levels; this policy is intended to provide a guide to protecting and ensuring the appropriate use of this information, consistent with those sensitivity levels.

**Definitions**

**Device** A computer (workstation, laptop, server, etc.), networking device (router, switch, hardware firewall, etc.), storage unit (drive array, CD jukebox, etc.), printer, or any other hardware unit interconnected with other hardware units and its associated software system, including configuration and other operationally necessary files.

**Information Systems (IS) network** A set of devices that has been interconnected both physically and logically to exchange information.

**Integrity** The condition in which data or information is trusted to be unaltered from its previously known state. No unknown or unauthorized modifications have been made.

**Network resources** The devices comprising the network, their constituent components, and the information (programs and data) input to, stored thereon, or output from it.

**Security** The process of managing access and modification rights (such as read, write, change, delete, execute, etc.) to network resources.

**User** Any person accessing the network or one of its constituent devices, whether directly or indirectly connected (to include connecting from another, external network). It includes employees, contractors, owners/partners, and any other person.

**Intended Audience**

This policy applies to all personnel:

Company employees, including managerial employees

Company owners, partners, and others with an equity stake

Company contractors

Any other user of the Company's network resources

**Responsibilities**

The security and integrity of the information stored on and accessed via the network is the responsibility of all users. While certain individuals or positions may be assigned particular duties with respect to the network's operation or its inputs or outputs, that does not absolve any other user of their aforementioned responsibility.

**Acceptable Use Policy**

The network is a Company asset, to be used for the Company's legitimate business purposes. Such purposes must be approved by the Company's management. The Company may allow users to engage in limited personal use of the network (such as browsing the Internet), but such permission is entirely discretionary on the Company's part and subject to change. If any limited personal use has previously been allowed, the Company will clearly indicate to all personnel the new usage policy.

Any copying of network resources for personal use is never acceptable; software copying for business use will solely be in accordance with the relevant license agreements.

Any other use beyond the acceptable use policy, by any user, shall be deemed an unacceptable use.

Unacceptable use of the network or any of its component devices may be grounds for disciplinary action, to include termination, or legal action, at the Company's sole discretion. Prior inaction by the Company concerning any occurrence of a user's unacceptable use does not constitute or imply the Company's endorsement or acceptance of such use, nor does it negate the Company's right later to take disciplinary or legal action, as deemed appropriate by the Company, against such users.

**Authentication, Authorization, and Accounting (AAA) Policy**

The following describes the standards by which network use will be validated and recorded:

**Authentication** methods shall be used to verify the identity of users.

**Authorization** methods shall be used to verify a user's access to network resources.

**Accounting** methods shall be used to record which users accessed sensitive network resources, when those accesses occurred, and the duration of such accesses.

Together, AAA provides an audit trail capability to assure network and information integrity, as well as supporting any response to security incidents.

**Remote Access Policy**

Remote access to the network by any user shall be permissible only for the advancement of the Company's business. Remote access shall not be permitted to compromise the network's security or integrity, nor that of any of its resources. The Company may therefore require those granted remote access to demonstrate that they have taken appropriate precautions on the systems they use for such remote access, and on any systems connected to them.

**Incident Response Policy**

The Company recognizes that no security is perfect, and unacceptable use, data compromise, network abuse, intrusion, or other incidents may occur despite the Company's efforts to prevent them. The Company will monitor the network resources for unacceptable use and will act promptly when any such unacceptable use is detected. The Company will:

Determine the nature of the unacceptable use,

Determine its entry point into the network,

Take corrective action to prevent further unacceptable use,

Determine the extent of unacceptable use,

Determine whether malicious software ("malware") has been installed,

Determine whether the Company's data and/or network integrity have been compromised,

Repair the network and/or restore the data from backups, if necessary.

These actions may be taken, at least in part, in parallel. The persons performing these actions shall keep permanent records ("logs") of the observations and actions. These logs are the property of the Company and fall under the purview of this policy as they are created; they will be used to establish the extent of any damage to the Company, and may be used in support of legal proceedings, as the Company deems appropriate.

**Personnel Departure Policy**

This policy applies to all personnel departures from the Company, whether voluntary or involuntary. No departing personnel are authorized to copy or remove any information from the network, or to alter any information before their departure except as required in the ordinary course of their work before the effective date of departure. All network accounts will be disabled or removed, and all authorizations will be discontinued, by the network administrator immediately upon the termination of work by the departing user.

**Internetworking with Other Entities**

The Company's network may interwork with other entities' networks (such as those of business or process partners). The Company will make every reasonable effort to assure itself that the other entities with which it exchanges information will treat any information so exchanged with substantially equivalent care. The company will also protect information received from other entities, or via other entities' networks, as though that information originated within the Company's network.

**Appendix A: Points of Contact**

**Network Administration**

Name _____

Telephone _____

Mobile _____

Email _____

**Network Security**

Name _____

Telephone _____

Mobile _____

Email _____

**Management/Other**

Name _____

Telephone _____

Mobile _____

Email _____

**Appendix B: Network Resources and Protection Levels**

The Company has designated the following Protection Levels for its network resources:

**Level 1** protection shall be applied to business-critical network resources. Loss of these resources or questionable integrity in them when present threatens the continuing existence of the Company. The underlying assumption is that of no access unless specifically authorized by the Company's management. Level 1 protection shall include strict AAA, with access limited on a strict "need-to-know" basis.

**Level 2** protection shall be applied to those network resources whose compromise (actual loss or loss of integrity) may cause serious damage to the Company. Authentication and authorization technologies will be applied in Level 2 protection; accounting may or may not be applied, on a resource-by-resource basis.

**Level 3** protection shall be applied to Company proprietary information. All users accessing Level 3 information shall be authenticated; authorizations will be granted on an individual or group membership basis. Accounting may or may not be applied, on a case-by-case basis.

**Level 4** protection shall be applied to all other network resources. Authentication will be required for access to all network resources; authorizations may be global for all authenticated users in Level 3 protection, but will not generally include users external to the Company. Exceptions (such as contractors needing access to fulfill their obligations) may be granted access on a case-by-case basis.

In addition, the entire network will be protected from external threats by implementing a firewall at every connection to external networks, antivirus software installed and aggressively used on every workstation, and filtering configurations on network connecting devices (routers and switches). Each network device will be periodically examined for malware; the following periods apply:

**Workstations** _____

**Servers/storage**_____

**Routers/switches** _____

**Other devices** _____

**Level 1 Protected Network Resources:** _____

_____

_____

_____

**Level 2 Protected Network Resources:** _____

_____

_____

_____

**Level 3 Protected Network Resources:** _____

_____

_____

_____

**Level 4 Protected Network Resources:** _____

_____

_____

_____

**Appendix C: Technologies Employed**

**Perimeter Security** _____

**Network Monitoring/Intrusion Detection** _____

**Network Administration** _____

**AAA**

**Authentication** _____

**Authorization** _____

**Accounting** _____

**Remote Access** _____

**AntiVirus** _____