



I

Security Overview

CERTIFICATION OBJECTIVES

- I.01 Introduction to Security
- I.02 Data Classification
- I.03 Security Breaches

- ✓ Two-Minute Drill
- Q&A Self Test

This chapter introduces you to why network security has become more and more important over time and some of the problems you'll have to tackle when implementing a solution. This chapter is more of an overview to Part I, where Chapter 2 discusses some common attacks you can expect in your network and Chapter 3 discusses the basics of implementing security mechanisms, including the creation of a security policy.

CERTIFICATION OBJECTIVE 1.01

Introduction to Security

This section covers security challenges, security goals, and security components. “Security Challenges” introduces you to the scope of problems you’ll face in network security; “Security Goals” discusses the goals you should have in designing, implementing, and maintaining a security solution; and “Security Components” discusses some common components found in many network security designs.

Security Challenges

The Computer Security Institute (CSI) is an organization that provides education, community, and research for Information Technology (IT) security professionals. Besides providing seminars and courses, it also performs a yearly survey on security issues companies face. One statistic that has been constantly high year-in and year-out is the number of networks that have experienced a security breach: over 70 percent! Not all breaches have been severe, but any type of breach can create loss of data, loss of time, and thus loss of revenue. One of the interesting statistics created from these surveys concerned the location of the breach: inside versus outside. Of the 70 percent of networks that have experienced breaches, 60 percent have undergone *internal* breaches, and 40 percent external or perimeter breaches.



You need to examine security in your network from endpoint to endpoint, from where traffic enters your network, to where your users connect (switches, access points, and remote access VPN gateways). Cisco’s philosophy and product solutions focus on end-to-end security.

There are two main reasons why security has loomed larger and larger as an issue over time:

- The hacking and attack tools have become more and more dangerous, where an attack can cause serious financial damage to a company. For example, a denial of service attack on a business' e-commerce solution that sells services on the Internet might cause the loss of millions of dollars because legitimate users cannot access the site.
- The hacking and attack tools have become easier and easier to use—in most cases, they are automated, allowing even a novice to use them. For example, many scanning tools used in reconnaissance attacks are GUI-based and provide detailed, well-explained output of the vulnerabilities that a system has and how to exploit them.

Security Roles

Compounding problems in security is the fact that roles in security have changed over the years. It used to be that most networks were closed to the outside world, attacks didn't cause that much damage, and network administrators only had to worry about a company's internal policies. Because the Internet has exploded since the mid-1990s, it has become almost a given that your company will have Internet access, and that you'll need, at times, to send information (that might be sensitive) across it. Plus, you might even have other connections that traverse semipublic networks that can create security risks when sending data across them. Many companies have also begun selling goods and services via the Internet, doing what is called e-business or e-commerce. Again, maintaining security is paramount—any security breaches can compromise the trust that your buyers have with you. Therefore, developing a company-wide security solution, which encompasses all of these items, can be a complex process.

Today, the Internet is commonly used to provide connectivity between locations or for remote access from your small offices or users working from home. Companies rely more and more on e-commerce solutions to increase their profits: today's networks are much more open than they were ten or even five years ago. On top of this, because networks are becoming more open, there is a much larger concern over protecting confidential information: information important to a company's trade secrets, employee personnel files, or even sensitive data, like hospital patient records or financial records of customers. Because of these concerns, not only have

companies focused more and more on security, but governments have passed laws and procedures to protect certain types of data.

Sometimes your company must follow specific legal and government policies when enforcing security. Just recently, over 50 bills have come before the U.S. Congress related to online security and privacy issues. U.S. government institutions must annually perform self-assessments and independent assessments of their security policies and security solutions, mandated by the Government Information Security Reform Act. If you are a health care company, you might have to follow the Health Insurance Portability and Accountability Act (HIPAA) when implementing security procedures. So not only do you have to worry about internal policies related to your company's security, but you must also be aware of external policies, which may, in turn, affect your company's internal policies.

Security Issues You'll Have to Deal With

Breaking it down, there are three basic security issues you'll need to deal with when coming up with a security solution for your network or company:

- Security is not just a technology problem.
- There are many different security technologies to choose from.
- You must create a comprehensive security policy.

e x a m
W a t c h *Be familiar with the three basic security issues.*

Security is not just a technology problem: since people are involved with systems that are networked, you must create a solution that deals with both the people that use the systems and also the technology the systems use. The solution will need to involve procedures and guidelines for your employees, a fact that is commonly forgotten in a security solution.

There are many security technologies to choose from: for example, when talking about VPNs, you have to consider that they come in different types, like site-to-site and remote access; different protocols, like IPSec, L2TP, PPTP, and SSL; different protection methods, like encryption algorithms and hashing functions; different methods of authentication . . . and to top it off, a vendor might offer more than one solution. For example, Cisco provides you with many different products and choices

when it comes to VPNs. All of these choices can make your job more confusing as you try to decide upon what technologies and products to choose from.

The third main security issue arises when your company either lacks a security policy or has one that is poorly written or designed. One of the main tools you'll use to help combat security issues is the development of a comprehensive and detailed security policy. A security policy basically defines what is and is not permissible with the access and use of a company's networking equipment, including PCs, servers, and even networking equipment like routers and switches, as well as the different types of data and resources that systems use.

Security Goals

There are three main goals you should strive to achieve when designing a security solution:

- Create and implement a single, cohesive, company-wide security policy.
- Don't allow products to dictate security policies—policies should drive the products that you choose.
- Centralize security management.

To simplify matters, your first step should be to create and implement a single, cohesive, company-wide security policy. This policy should be flexible enough to allow your company to meet its objectives that are detailed in the company's business plan, but still protect your company's assets at a reasonable price.

Unfortunately, this step is not as simple as it sounds. You might have various router and RAS (remote access server) platforms; firewalls; PCs running Windows 2000, XP, and/or Vista; servers running Windows 2000, 2003, 2008, NetWare, and/or Unix; and even mini or mainframe platforms that you will need to secure. However, even though you are faced with centralizing a security solution that encompasses all of these devices, you should not let products dictate your security policies—security policies should drive the products that you choose in order to secure your network and its resources.

Given this, you might want to choose all your security products from a single vendor; however, the solutions that this vendor supplies might not meet all your security needs. You might have to buy security products from multiple vendors, which increases headaches with integration and management. And you might even

be forced to replace some of your existing networking equipment so that it can be integrated into a centralized security solution. Once you have your network security in place, many administrators often forget that you must manage it on a day-to-day basis—there is no solution on the market today that you can deploy and then just walk away from. Security is a constantly changing business, and you'll need to dedicate some, if not a lot, of your daily time to dealing with your company's security.

Security Components

It is important to remember that security is a *relative* or *subjective* problem—this means that what is important to one company is not necessarily important to a different company. Each company has different business plans and goals, and thus their security policies and solutions will be different. Typically, a security solution will address seven basic components:

- **Authentication** Verifying a person's identity (who they are)
- **Authorization** Controlling access to resources (what they are trying to do)
- **Privacy** Protecting confidentiality of information (what the content of the information is)
- **Integrity** Validating that information was not changed (verifying that the information that was received was not been modified or tampered with)
- **Availability** Providing redundancy for security (ensuring that you have a fallback solution in the event of a failure or security compromise)
- **Nonrepudiation** Proving that a transaction took place between two entities (when using online transactions, having verifiable proof that the transaction took place between two entities, like an online order at Amazon.com or an auction transaction at eBay)
- **Accounting** Recording information about an employee's actions when interacting with data and systems as well as information about the operation (including security events) of your networking devices

Because each business plan and set of business goals is different between companies, your company might need to implement all of these components. However, you will probably have to deal with at least two, if not more, of these in your security policy and solution.



Note that depending on the size of your company and the protection you need to provide, you might not need all seven of these security components.

CERTIFICATION OBJECTIVE 1.02

Data Classification

In order to create an appropriate security policy and design, you'll need to first classify your data. Sometimes, classification of data might be required by law. Benefits of classifying data include the following:

- Shows a commitment on the company's part to secure the network and its resources.
- Identifies data that is most sensitive in the company.
- Determines security measures that should be used to protect data.
- Provides a better cost-benefit ratio by focusing on data that has the most importance and therefore needs more protection.

The following sections will discuss classification levels, criteria and procedures, and roles.

Classification Levels

Data is classified slightly differently between public or government agencies and private companies. Public or government agencies commonly use the following classification levels:

- **Unclassified data** The data has few or no confidentiality requirements.
- **Sensitive but unclassified (SBU) data** The data could prove embarrassing if revealed, but no serious security breach would occur.
- **Confidential data** This is the lowest level of classified data, where data protection must meet confidentiality requirements.

- **Secret data** A significant effort must be made to secure data, limiting access to a small number of people.
- **Top secret data** Great effort and cost is used to secure data, limiting access to a very small number of people (commonly referred to as “need to know” access).

Unlike public or government agencies, private companies or nongovernmental agencies have a different set of data classifications:

- **Public data** This is data that is publicly available, as on a web site.
- **Sensitive data** This is similar to SBU data.
- **Private data** This is data important to a company; an effort must be made to secure it and verify that it is accurate.
- **Confidential data** This data is very important to a company, like trade secrets and employee records.

exam

watch

Be able to differentiate among the different classification levels

used by government agencies and private companies.

Classification Criteria and Procedures

Classification *criteria* for data define how data is classified or tagged. Classification criteria include the following:

- **Value** This is the most important criterion and indicates how important the data is to the organization.
- **Personal association** This is data associated with a person, like an employee file in Human Resources (HR).

- **Age** Over a period of time the value of the data decreases as events occur, such as changes in technologies being used.
- **Useful life** Newer information obsoletes older data; for instance, company products become end-of-life (EOL) and are replaced by newer ones.

Of the classification criteria, *value* is the most important.

Classification *procedures* define who is responsible for data, how it is classified, the policy that handles the classification, and when and how declassification occurs. Here's a quick summary of the items involved with classification procedures:

- Who is responsible for the data?
- How should the information be classified, with any exceptions?
- How are the controls used for classification policies?
- When and how does declassification of data occur?

Distribution of classified materials should be defined in a classification policy, for example, requiring the written approval of senior company management. Contracts with other companies, especially with government agencies, might require distribution of classified materials. And, if your company is brought to court, the court might order that the classified documents be shown in the court of law.

Classification Roles

Classification *roles* define the people and their roles when interacting with data. There are three roles: data owner, data custodian, and data user. Table 1-1 compares the three roles.

TABLE 1-1		Role	Description	Performed By
Data Classification Roles	Owner	Is ultimately responsible for the data.	Typically a member of the management staff	
	Custodian	Is responsible for the security of the data on a day-to-day basis.	Typically a member of the Information Technology (IT) staff	
	User	Is responsible for using the data according to defined policies and operating procedures.	Your typical user, who can “see the trees, but not the forest” in the company and who has a ground-level view of certain data	

Security Controls

Security controls are mechanisms used to protect data. Security controls fall under three types: preventive, deterrent, and detective. Here is a description of the three types:

- **Preventive** Used to prevent a data compromise
- **Deterrent** Used to scare away a certain number of ill-doers
- **Detective** Used to detect access to data

Of the three security control types, preventive controls are the most secure but typically cost the most to implement.

There are three categories that control the implementation of the security control types:

- **Administrative** Policy and procedural controls
- **Technical** Electronics, hardware, and software controls
- **Physical** Mechanical controls

exam

Watch

The three categories of security controls are administrative, technical, and physical.

Administrative controls deal with security-awareness training, background checks of employees, restrictive hiring practices, auditing the activity occurring on systems, change and configuration management control, and, most importantly, the development and enforcement of a security policy. *Technical* controls deal with network devices to implement security controls (VPN gateways, firewalls, IPS appliances, and

the like), methods of authentication and authorization (like directory services; authentication, authorization, and accounting, or AAA; 802.1x; and one-time password mechanisms, or OTP), security devices (like smart cards; network access control, or NAC, systems; and biometrics), and logical access control mechanisms (like access control lists, or ACLs, on routers and firewalls). *Physical* controls deal with the use of monitoring equipment to detect intrusions (like an alarm system), physical security devices (like door locks, door key codes or cards, safes, and secured rack systems for equipment), environmental controls (like UPS systems, sprinkler systems, and air conditioning and air flow devices), and security guards and personnel.



A good security implementation to protect data will have a good balance among administrative, technical, and physical controls.

CERTIFICATION OBJECTIVE 1.03

Security Breaches

In an ideal world, if you were wronged, you would receive due justice and the perpetrator would be punished. However, this is not an ideal world. When it comes to computer and network security, if someone hacks into a service, finding and bringing the person to justice can sometimes seem like an almost impossible process. The following sections will discuss some important topics related to security breaches and bringing justice to those who damage your network and its resources.

Law and Ethics

Laws fall under one of three categories:

- **Administrative** Deals with the enforcement of regulations, like how employees are taxed.
- **Civil** Deals with wrongs that are not crimes, like someone infringing on a company's copyright, patent, or trademark and being sued over damages this has caused.
- **Criminal** Deals with the enforcement of crimes, where fines and/or imprisonment are used as penalties.

Each government typically has differences in the classification and enforcement of laws.

Ethics are moral principles or values held higher than law that guide the behavior of a person. Ethics are basically guidelines and are not enforced by government laws; however, many laws are based on ethics. There are actually many organizations that have created codes of conduct for computer and resource usage, including INFOSEC (Information Security), ISC2 (International Information Systems Security

Certification Consortium), Computer Ethics Institute, IAB (Internet Architecture Board), and GASSP (Generally Accepted System Security Principles). INFOSEC has a certification that mandates that all INFOSEC-certified individuals must follow their local laws and abide by a code of ethics. The Computer Ethics Institute has the ten commandments of computer ethics, as follows:

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid.
7. Thou shalt not use other people's computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.

Prosecuting Attackers and Hackers

If you catch someone who breaches your network and/or data security, you need to be able to prove the following in order to successfully prosecute that person:

- **Motive** Why did they do it?
- **Opportunity** Were they available to commit the crime?
- **Means** Did they have the capability to commit the crime?

These three things are true of most courts of laws throughout governments of the world.

However, to prove these three things and successfully prosecute the criminal, you'll face many difficulties. When dealing with the computer world, most of your evidence is "virtual" and you'll need to maintain data integrity, which can be

difficult in a “virtual” world. For example, evidence you collect, like data and log files, can easily be damaged or modified, like timestamps that indicate when the file was created or modified.

When a breach occurs, don’t shut down or reboot a system until you perform a memory dump. Likewise, a disk image should be captured before working with data on the drive. Make sure you photograph the equipment and information before disconnecting it. You need to maintain a strict chain of custody of the equipment and/or information when working on it—who accessed it, when they accessed it, and what they did with it.



Contacting your company’s lawyer and the appropriate law enforcement agency for their expertise is very important if you want to successfully prosecute a security breach.

Liability: Legal and Governmental Issues

Beyond protecting the assets and interests of your company, your company and your security personnel might have to deal with liability and legal/governmental issues regarding security. Your company could be held liable if you don’t properly protect your systems from breaches. For example, if you don’t adequately protect sensitive customer data, such as financial information or employee files, and this information is stolen and made public, your company could be sued by your customers or employees! A company should practice due diligence (implementing protection mechanisms) and due care (implementing care in operation and maintenance of security mechanisms of due diligence) when protecting sensitive data and resources.

On top of liability, you might also have to deal with government laws that require you to meet a minimal security level when protecting certain resources. For example, in the United States, if you are in the health care profession, you have to deal with the HIPAA requirements. On top of this, many companies have to deal with Sarbanes-Oxley (SOX) standards, which are used to prevent corporate accounting scandals like the one that wracked Enron. Other government agencies, like the European Union, your country’s laws, or even your state or local laws, might require you to meet minimum security standards.

CERTIFICATION SUMMARY

This chapter focused on introducing security topics, including security issues you'll have to deal with, data classification, and security breaches. Security is an end-to-end implementation in a network, since about 60 percent of breaches are internal and only 40 percent are external or perimeter breaches. Therefore, you need to monitor not just the perimeter of your network but access from your users. Hacking tools have become more dangerous and easier to use, pushing security to the forefront of any network design. Many administrators and network designers forget that when designing a solution, the first step is to develop a security policy. On top of this, a decision must be made about the technologies and products that should be used based on the security policy. Finally, no matter how much technology you throw at security, people are involved in the process and this must be dealt with in your company's policies and procedures. Typically, a security solution will contain some, if not all, of these components: authentication, authorization, privacy, integrity, availability, nonrepudiation, and logging/accounting.

Classifying data is one of your first steps in a security design, since this will help focus your time and money on the most critical data and resources. Government agencies typically have these classification levels: unclassified data, sensitive but unclassified data, confidential data, secret data, and top-secret data. Private companies have these classification levels: public data, sensitive data, private data, and confidential data. You place data into these categories according to the following criteria: value, personal association, age, and useful life of the data. To help define policies for data, classification roles must be created based on the owner, the custodian, and the user of the data. To protect the data, you can implement three types of security roles: preventive, deterrent, and detective. The categories of controls that you can implement include administrative, technical, and physical.

When (not if) you experience a security breach, you'll need to make the appropriate response, which is typically outlined in your security policy. Determining the type of law that was broken—administrative, civil, or criminal—will help in determining the type of response your company will take. Assuming you have a strong suspicion of who committed the breach, you'll need to show motive, opportunity, and means in order to successfully prosecute the individual(s). Remember that you must also protect yourself and your company by following government laws, like HIPAA and SOX, to prevent lawsuits from employees or customers, because of a security breach.



TWO-MINUTE DRILL

Introduction to Security

- ❑ Most breaches are internal, not external, so a security solution should be end-to-end.
- ❑ Common security issues include these: security is not just a technology problem, there are many different security technologies to choose from, and there is either no security policy or a lack of enforcement of the security policy.
- ❑ Your three main security goals should include creating a security policy, ensuring that policies drive the products you choose, and centralizing the management of your security solution.
- ❑ Security components include authentication, authorization, privacy, integrity, availability, nonrepudiation, and accounting/logging.

Data Classification

- ❑ Government classification of data includes unclassified data, sensitive but unclassified data, confidential data, secret data, and top-secret data.
- ❑ Private companies' classification of data includes public data, sensitive data, private data, and confidential data.
- ❑ Classification criteria for data include value, personal association, age, and useful life, where value is the most important.
- ❑ Security controls include preventive, deterrent, and detective. Preventive is the most secure control method, but the most costly.
- ❑ The three categories that control the implementation of security controls include administrative, technical, and physical.

Security Breaches

- ❑ The three types of laws are administrative, civil, and criminal.
- ❑ To successfully prosecute a computer criminal, you'll need to show motive, opportunity, and means.
- ❑ Some U.S. government standards/laws include HIPAA and SOX.

SELF TEST

The following Self Test questions will help you measure your understanding of the material presented in this chapter. Read all the choices carefully, as there may be more than one correct answer. Choose all correct answers for each question.

Introduction to Security

1. Which type of security breaches should you be concerned about most?
 - A. Internal
 - B. External and perimeter
 - C. Perimeter
 - D. Internal, external, and perimeter
2. Which of the following is not one of the three basic security issues you'll face when designing a security solution for your network?
 - A. You must be concerned about people and the resources and data they use.
 - B. Your company doesn't have a security policy.
 - C. It can be confusing to choose a solution because of the many different security technologies and products that are available.
 - D. You must be familiar with the organization's politics to design a sufficient security solution.
3. Which of the following are not one of the three main goals you should strive to achieve when designing a security solution? (Choose two.)
 - A. Create a company-wide security policy.
 - B. A closed system is the best design choice.
 - C. Centralize security management.
 - D. Products dictate the policies that should be created.
4. Which security component protects the confidentiality of data?
 - A. Authorization
 - B. Integrity
 - C. Privacy
 - D. Nonrepudiation

Data Classification

5. What is the highest level of classification for government data?
 - A. Top secret
 - B. Unclassified data

- C. SBU data
 - D. Confidential data
6. Which of the following has the private classification levels in the correct order from least-to-most important?
- A. Public, sensitive, private, and confidential
 - B. Public, private, sensitive, and confidential
 - C. Public, sensitive, confidential, and private
 - D. Public, private, confidential, and sensitive
7. Which of the following is not a classification criterion for data?
- A. Value
 - B. Personal association
 - C. Useful life
 - D. Data location
8. Which category implements policy and procedural security controls for data?
- A. Technical
 - B. Physical
 - C. Security policy
 - D. Administrative

Security Breaches

9. In order to successfully prosecute a person that has purposefully committed a security breach, which of the following is not necessary?
- A. Motive
 - B. Opportunity
 - C. Ethics
 - D. Means
10. What category of law would be broken if a dishonest employee sold trade secrets of a new product to a competing company?
- A. Administrative
 - B. Civil
 - C. Government
 - D. Criminal

SELF TEST ANSWERS

Introduction to Security

- D.** Security is an end-to-end implementation and is concerned about internal, external, and perimeter security.
 Answers **A**, **B**, and **C** are incorrect because they don't include all access methods.
- D.** The organization's politics should not dictate the solution that you create, making this answer correct.
 Answers **A**, **B**, and **C** are the three basic security issues you'll face, making these answers incorrect.
- B** and **D.** **B** is incorrect because most networks today need access to external resources, like the Internet. **D** is incorrect because policies should dictate products, not the reverse.
 A and **C** are true and thus incorrect answers.
- C.** Privacy protects the confidentiality of information, which is commonly accomplished through the use of encryption.
 A is incorrect because authorization is used to control access to resources. **B** is incorrect because integrity is used to validate that information has not been changed. **D** is incorrect because nonrepudiation is used to prove that a transaction has occurred.

Data Classification

- A.** Top-secret data is the highest level of classification for government data, and great effort and cost is used to secure it.
 B, **C**, and **D** are incorrect because they are lower levels in the classification stratum.
- A.** Private or non-government classification levels start at public, which is the least important, to sensitive, private, and then confidential, which is the most important.
 Answers **B**, **C**, and **D** are incorrect because they have the levels listed in the incorrect order.
- D.** Data location is not a classification criterion for data.
 Classifications for data include value, personal association, age, and useful life, making answers **A**, **B**, and **C** incorrect.
- D.** Administrative controls define policies and procedures for accessing and using data and resources.
 A is incorrect because technical controls encompass electronics, hardware, and software controls. **B** is incorrect because physical controls encompass mechanical controls, like video cameras and key cards. **C** is incorrect because the controls are part of the security policy.

Security Breaches

9. C. Ethics are not laws but a “higher” standard of recommended guidelines and thus can’t be used to prosecute an individual(s).
 A, B, and D are typically necessary in most courts of law in order to successfully prosecute an individual(s).
10. B. Civil laws deal with wrongs that are not crimes, like someone infringing on a company’s copyright, patent, or trademark and being sued over damages.
 A is incorrect because administrative laws deal with the enforcement of regulations, for instance, how employees are taxed. C is incorrect because this is not a category of law. D is incorrect because criminal laws deal with punishment of crimes, where fines and/or imprisonment are used as penalties.