

# Chapter 1



## Analyzing Security Policies, Procedures, and Requirements

---

### MICROSOFT EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ **Analyze business requirements for designing security.**  
Considerations include existing policies and procedures, sensitivity of data, cost, legal requirements, end-user impact, interoperability, maintainability, scalability, and risk.
  - Analyze existing security policies and procedures.
  - Analyze the organizational requirements for securing data.
  - Analyze the security requirements of different types of data.
  - Analyze risks to security within the current IT administration structure and security practices.
- ✓ **Analyze technical constraints when designing security.**
  - Identify capabilities of the existing infrastructure.
  - Identify technology limitations.
  - Analyze interoperability constraints.



Every day, your computer systems and the data they contain are at risk for theft, corruption, or misuse. These risks can come from, for example, malicious crackers outside your organization, internal personnel looking to profit from the data, or careless employees accidentally deleting data. The confidentiality, integrity, and availability of your data need to be protected. Before you can protect your data on a Windows Server 2003 network, you need to know what the policies, procedures, and requirements of the business are for security.

Securing a Windows Server 2003 network means you need to identify the assets that you need to protect, therefore allowing the business to continue to operate without disruptions caused by attackers or viruses. You will also need to evaluate the current security policies and practices to see if they are in line with the security needs of the business. These plans and procedures need to be evaluated and reevaluated as the use of the data and the network changes. This requires that the administrative staff and you understand technical constraints and design security that works within the constraints to meet the needs of the business. Finally, you will need to identify any technical constraints that will be a barrier to providing for the security requirements of the business and how you will overcome them.

In this chapter, you will learn how to evaluate the current IT security policies and procedures and analyze the organization's requirements for securing data. You will also learn how to evaluate risks of current IT practices with regard to security and how the current technologies and requirements of interoperability within the organization impact security.

## Analyzing Security Risks

*Security risk analysis* is the process of reviewing the asset that needs to be protected versus the cost of protecting the asset and the likelihood that the asset will be attacked. The first thing you need to do in determining security risks is to determine what you are trying to protect. The resources you are trying to protect are usually referred to as *assets*. You can identify assets by using the following categories:

**Hardware** This can be any type of computer hardware, such as servers, laptops, cables, routers, and switches.

**Software** This includes the installed operating systems and applications, source code, and so forth.

**Data** Data that needs to be protected includes private employee information, customer information, corporate secrets, and information about pending large transactions, and so on.

**Documentation** This includes, for example, security policies and procedures, floor plans, network diagrams, change logs, audit logs, and web logs.

You need to list all assets that can be affected by a security incident in the organization. You should analyze each asset with regard to availability, integrity, and confidentiality to determine where it is at risk. For instance, suppose you run an e-commerce website that uses a SQL Server 2000 database that contains customers' personal information (like credit card numbers), their orders, and the catalog of products. In addition, the website is hosted on a Windows Server 2003 machine using Internet Information Server (IIS). You will need to look at each asset as follows:

**Server hardware** If the physical server hardware is compromised then all other security precautions may be worthless. The physical security of the server or servers is important because without it most security can be compromised quickly.

**Internet connection** If the Internet connection is compromised, the web application will be offline to customers. The integrity of the data passed over this connection needs to be maintained to prevent someone from changing the information in stream to or from the server. You need to ensure confidentiality of data (presumably credit card numbers and customers' personal information) that passes over the connection.

**Internet Information Server (web server)** The web server needs to be protected because it is a great backdoor for attacks, especially if it is not patched. Also, the pages on the site and the code it runs could be defaced or changed. This could affect customer perception or personal information. Information moving through the web server will be confidential, so you'll need to take precautions with the connections to the database and the Internet.

**SQL Server 2000** If the database is not working properly, the website will not be available. A database is prone to corruption or misuse, which can affect the integrity of the data. The data is important to the website, so the integrity of the database must be maintained. It would not be good for customer relations if someone manipulated the prices or customers' personal information. The database in this web application stores customers' personal information, so the confidentiality of the data is important.

**Windows Server 2003** The server operating system provides applications running on it (IIS and SQL Server in this case), so it needs to be available for the applications to be available. Access to data must be controlled to maintain confidentiality and integrity if it is stored in the file system or Registry. This data usually includes the configuration information of the applications, without which they would not be available.

After you have determined the assets that are at risk, you will need to determine the threats to the assets and the likelihood of the threats being carried out. A *security threat* is anything that will prevent the availability, undermine the integrity, or breach the confidentiality of the asset. The following are some examples of threats to resources:

- A denial of service (DoS) attack on your web server is an example of a threat to the availability of the asset.
- A virus that corrupts data on the file system is a threat to the integrity of the asset.
- Improper application of network permissions that allows a user to access data on the file server is a threat to confidentiality.

## 4 Chapter 1 • Analyzing Security Policies, Procedures, and Requirements



We will address threats to specific technologies in the chapters in which the specific technologies are covered.

For example, viruses are really common on the Internet and through e-mail. This is a threat to almost all aspects of your organization's assets and is highly likely to occur. When you take into consideration that a virus has the potential to corrupt, steal, or prevent the availability of data, it's clear that virus protection would be a high priority in your security planning.

You can assess risks using varying approaches, but two of the most common are through quantitative analysis and qualitative analysis.

*Quantitative analysis* involves estimating the actual value of the asset or what it would cost if the asset was unavailable for a period of time or if it was lost. This kind of analysis is easier for the availability or integrity aspects of risk analysis. For example, you can set a price on the server hardware that might get stolen if the server room is not locked or how much business would be lost if the website were down. Confidentiality of data is more difficult to quantify because the data may be intellectual property, proprietary trade secrets, or private patient information. These assets don't have a definite monetary value but can cost you in terms of lawsuits or lost customers.

*Qualitative analysis* involves ranking the risks on a scale that reflects the resource's importance to your organization. You usually use two separate numbers for this process to give an accurate assessment of the importance of the resource and the likelihood of a threat being carried out against the resource. We use a scale of from 1 to 10 to put a number on the importance to the business and the chances that the threat will be carried out. We then multiply these numbers together to determine the ranking of the risk in relation to other risks. For example, an online business might assign a rank of 10 to both the importance of its website to the business and the likelihood of a denial of service attack launched against the site, resulting in a score of 100 for the risk. This would be one of the first security risks the organization would address with its available resources.

On the other hand, a small printing company might determine that its website contains only information about the products, services, and location and give it a ranking of 3 while the prospect of a denial of service attack would be given a ranking of 10, resulting in a score of 30 for the risk. This means the company might address other security risks first with its available resources.

You will need to determine the security risks and the likelihood that they will occur from information you have and information you obtain in interviews with key personnel in the organization. You should look at whether the risk has occurred before, because that makes it more likely to occur in the organization. Important risks can then be mitigated by subsequent security planning, as outlined in the next section.

### Understanding Types of Attacks

You will need to understand the types of attacks on a network to determine if your systems and infrastructure are vulnerable:



Defenses against these types of attacks will be addressed when we discuss individual technologies in future chapters.

**Spoofing** Changing the source information in a packet so that those at the destination cannot determine where it came from or to redirect the response to a request to a different device or to make traffic appear to be from a trusted party.

**Man-in-the-middle** Capturing a packet in order to eavesdrop or change some of the information in it and sending it on to the server. Can be used to gain network authentication on some weaker authentication schemes.

**Denial of service (DoS)** Sending such a large volume of traffic to a network device that it cannot keep up, changing routing tables or DNS entries, or otherwise affecting the network so legitimate clients cannot get to their network resources.

**Replay** Capturing packets and then sending them to a server at a later time. Some protocols are susceptible to this attack if the packets aren't numbered somehow.

**Packet sniffing** Using a program that captures packets crossing a device on the network. This type of attack can reveal any information that is weakly or not encrypted.

**Social engineering** Using non-computer techniques to obtain passwords or other information about a company. This can involve sifting through trash or conning users into revealing their passwords.

**Buffer overflow** Taking advantage of a common bug found in C/C++ programs (which include most services and operating systems). The programmer forgets to check the upper bounds of the data being stored in an array. This means that the attacker can enter data in such a way that it runs past the end of the array and into the same or another program's stack so that the overflow will be executed. In essence, this allows the attacker to insert their own information into your computer's memory, which means they can launch other applications or corrupt data. This is the mechanism that many of the worms use to infiltrate Windows systems. The only way you can guard against it as an administrator is by keeping your systems up-to-date with all critical hotfixes and patches, running only the minimal amount of services needed on the server, and not giving more permissions to the application than is absolutely necessary.

**Mail relaying/Spamming** Using an e-mail server to send unsolicited e-mail.

**Website vandalism** Altering a website with unauthorized material.

**Physical attack** Compromising, vandalizing, or stealing hardware through unauthorized access.

**Trojan horse** A program that allows an attacker to take over the host computer or watch what the user is doing.

**Worm** A program that uses the Internet to propagate itself.

**Virus** A benign or malicious program that self-propagates through other executable files.

**Password cracking** Using a brute force dictionary attack (which is trying all possible combinations of passwords, using a dictionary of words and common names) or some weakness in the password encryption algorithm to figure out passwords.

In the "Analyzing Security Risks" Design Scenario, you will analyze the security risks that a company may face.



## Design Scenario

### Analyzing Security Risks

Infinite Horizons relies on its website for 30 percent of its total orders. This accounts for \$200,000 in sales a year, and it is important that the site is up 24/7 so customers don't go to competitors for similar products. Infinite Horizons collects customer information with each sale in a SQL Server 2000 database. Some employees need to use this information to process credit cards offline because Infinite Horizons does not have an online merchants account. Marketing generates reports on the customers and sales information to determine how to position Infinite Horizons's products. Personnel in marketing must not have access to customers' credit card information. In the past, this has occurred. Employees need access to files on an internal file server for their appropriate departments. Employees are also required to log onto the network and has a strong password policy in place.

**1. Question:** Identify the security risks for Infinite Horizons. **Answer:**

- Denial of service attack on the web server
- Unauthorized access to credit card information
- Weak passwords
- Unavailability of SQL Server
- Unauthorized access to the file shares

**2. Question:** What are the two primary risks for Infinite Horizons? **Answer:**

- Denial of service attack on the web server
- Unauthorized access to credit card information

**3. Question:** Identify the kinds of attacks that can occur on Infinite Horizons. **Answer:**

- Denial of service attack on the web server
- Accidental deletion of data on the web server
- Malicious defacing of the website
- Physical destruction or theft of the web server or database server
- Corruption of the SQL Server database
- Improper access permissions on internal file servers
- A worm or virus causing data loss or denial of service

- An attacker sniffing packets on the network
- An attacker using social engineering to gain passwords and user IDs from your employees
- Theft of credit card information or changing of prices of products

**4. Question:** How can you mitigate the risks listed in step 3? **Answer:**

**Denial of service attack on the web server** Filter unwanted network traffic and employ intrusion detection of the firewall in front of the server. Notify appropriate staff if an attack is noticed because you will usually need to work with the ISP staff to solve this attack.

**Accidental deletion of data on the web server** Apply the appropriate permissions to users of the web server to prevent users from deleting data. Make sure you limit access to accounts that can modify permissions to users without proper training from writing or modifying permissions. Make sure you have a current and good backup of the server to recover files if there is a problem. Also, make sure that auditing is enabled.

**Malicious defacing of the website** Filter packets heading for your web server on the firewall to reduce the vulnerability footprint. You will need to verify permissions on the files on the web server. You should also filter the types of commands (verbs) that can be issued against your server.

**Physical destruction or theft of the web server or database server** Secure the room and building the server is in. Planning for destruction via non-malicious means like a natural disaster can help mitigate this particular risk.

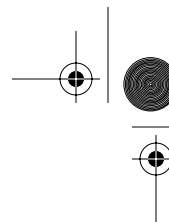
**Corruption of the SQL Server database** You need to make sure your SQL Server database has the proper permissions, limit access of the account used to connect from the web server, and preventing SQL injection attacks in the web applications code to prevent corruption. You need to make sure you regularly and successfully back up the database server so you can restore a clean version if you need to.

**Improper access permissions on internal file servers** Verify the permissions on the file servers and whether they meet requirements for securing these resources. You could run a baseline security analysis to verify the setup of the file servers.

**A worm or virus causing data lose or denial of service** Virus scanning software and education of users will aid in preventing these attacks. If some were to get through, you should have a backup strategy to deal with the data loss.

**An attacker sniffing packets on the network** You can thwart a sniffer by using encryption. Infinite Horizons would benefit from using SSL on its website.

**An attacker using social engineering to gain passwords and user IDs from your employees** Educate your users about what is expected of them with regard to security.



## 8 Chapter 1 • Analyzing Security Policies, Procedures, and Requirements

After you have determined what resources and services are at risk in your organization, you will need to determine if the current security processes are adequate to protect them. This will also give you a clearer picture of what amount of security will give you an adequate return on your investment and whether you are overspending on protecting less-important resources.

### Analyzing Existing Security Policies and Procedures

Securing resources in your organization is expensive because it involves additional infrastructure and personnel. In addition, it does not directly affect the bottom line (unless your business is security). In other words, security infrastructure is overhead. You will need to determine what resources need to be secured and whether it would be more cost efficient to protect some resources with an insurance policy. You can begin to determine if the current security is adequate or wasteful by analyzing the current practices in the organization. This information is usually defined in a document called a security policy.

*Security policies* explain what assets your organization secures, how they are secured, and what to do if the security is compromised. A security policy helps you make decisions about what type of security to implement by defining what an organization's security goals are. By doing so, you can determine what needs to be secured and at what level. You can also use the security policy to communicate these goals to users, administrative staff, and managers. If the organization does not have a security policy, you will need to create one.

After analyzing the risks to assets on a network, you will be able to evaluate and create security policies and procedures. You should create a security policy to ensure that efforts spent on security don't exceed the cost of recovering the assets should it be compromised. Security policies help you determine that your efforts are focused in a cost-effective and not overly burdensome manner to your organization. You need to make sure that the policies you implement adhere to government and industry regulations, so you may need to obtain legal council to verify compliance (HIPAA in the insurance industry or line monitoring in the financial industry, for example). You also need to make sure the policies adhere to the organization's culture and tolerance of procedures and policies, the exposure of resources to employees or customers, threats to the resources of the organization, and security requirements for these resources.

Security policies can be broken into two categories:

**Standard security policies** *Standard security policies* are implemented organization wide and represent a baseline of security in the organization. All users must comply with them, and hardware or software can be used to make sure they are enforced and to ease the burden of the security policies on the user. For example, password policies may create difficult-to-crack passwords, but if users need to write the passwords down your policies may not be effective. These policies are required, and any security solution you propose will have to adhere to them. You may need to recommend a change to standard policies if necessary to implement a new service or application.

**Recommended security policies** *Recommended security policies* may be necessary for only part of the organization. A division or department may choose to implement an optional security practice if they find it cost effective or determine it applies to their assets. You should take into account any recommended policies that apply to the part of the company you are trying to secure. Also remember that any new security policies you define might be candidates for recommended policies and should be shared with the organization.





## Real World Scenario

### Adjusting Security Policies to Comply with Government Regulations

One of our coworkers, Dave, recently received an assignment to evaluate a proposed database application for a pharmacy. They decided to create a database that would track the patients and the pharmaceuticals they purchased to make it easier to create internal reports and to address some regulations they have for tracking controlled substances. This reporting required a lot of paperwork and they had decided that automation was the answer.

The database and application was straightforward, but Dave needed to address the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA requires that patient information be confidential. The pharmacy did not have a security policy that stated that applications need to be in compliance with government regulations. This entailed further discussions about how to bring the database into compliance with HIPAA.

The cost savings of the project need to be evaluated to account for the additional work to bring it into compliance with HIPAA. The project was put into a state of limbo while they reevaluated it and their security policies.

Security policies do not define the technologies used to implement them. This is intentional because their purpose is to define the goals of providing security to the organization. Security policies usually involve the following, as described in RFC 2196, *Site Security Handbook*:

**Computer technology purchasing guidelines** Define the required or preferred security features on purchased technology. For example, if authentication in the organization is implemented through two-factor authentication (a form of authentication requiring a device and a password such as smart cards), then smart card readers are required for workstations and servers purchased.

**Privacy policy** Defines a user's expectations for privacy with regard to network and phone communications.

**Access policy** Defines the rights and permissions associated with resources to protect them from destruction or disclosure. The access policy could define guidelines for connecting to the network, for adding servers or new software to the network, and for notifying users of the policies.

**Accountability policy** Defines the responsibilities of the users, administrators, and managers with regard to security incidents and auditing.

**Authentication policy** Defines password policy and guidelines for trusted connections to the network.

**Availability statement** Sets expectations for availability of resources by defining scheduled downtime, operating hours, and the time it would take to recover resources. This is useful in determining the amount of protection and effort to apply to preventing downtime due to security incidents.

## 10 Chapter 1 • Analyzing Security Policies, Procedures, and Requirements

**System and network maintenance policy** Defines how internal and external administrators are allowed to maintain the network. You need to determine if remote maintenance is allowed and how it is implemented. This will be covered in more detail in Chapter 10, “Designing Secure Network Management.”

**Violations reporting policy** Defines what types of network security breaches or violations of security policies need to be reported and to whom.

Once you have defined the security policies for the organization, you will create security procedures to implement the policies. Security procedures define how to comply with policies and provide detailed steps that describe how to implement them. The procedures are where you will apply specific technologies, software, and hardware to the policies. The procedures for implementing security on the Windows Server 2003 family of products will be covered in the rest of this book.



You can read the entire RFC 2196 at <http://ietf.org/rfc/rfc2196.txt>.

Security policies are great, but the process of creating a security policy document can be a waste of time if management doesn't enforce the policies or if users and administrators ignore them. Effective security policies have support from all employees in the organization. This means that all the key stakeholders—including management, technical staff, and legal council—should be involved in the process of developing them.

Management will provide the budget to implement the policies and the authority to enforce or provide incentives for employees to follow the policies. It is most important to get management buy-in or the security policies will be difficult to enforce. After all, security policies are an additional burden to the users of the system. For example, it would certainly be easier to use a network if we did not need to worry about passwords.

The technical staff will provide information about limitations of the current technology that is necessary to implement a policy. This is not to say that the policy will not be implemented due to technical limitations. Appropriate means can be used to determine the cost of the risk associated with the policy versus the cost of implementing the policy.

The legal council is involved to make sure the wording of policies is correct, to explain legal problems that may arise from enforcing policies, and to make sure policies include requirements due to regulation and to make sure laws and regulations are followed.

You also need to make sure that the policies don't include too much legal or technical jargon that would make them difficult to understand for both administrators and users. Security policies and procedures should be straightforward and be written in declarative sentences like “All employees must follow the password policy created by the network security group” or “No employee shall have illegal copies of software on their computer.” You can then expound on the policy if necessary. You need to remember that policies that are too vague will result in interpretation by employees or, if they are too strict, that employees generally won't be able to do their jobs effectively. Such policies won't be supported by managers and will generally not be enforced.

The security policies (and later changes to them) should be easy to find. You should come up with a method of disseminating the information to the organization. E-mail, company intranet, bulletin



## Real World Scenario

### Pencils and Server Room Doors

A security policy often states that all servers must be in a physically secure server room. But being overly strict about this can cause employees to circumvent the policy to do their job. We were consulting at a credit card bank. The project was being developed on a test server that, due to various test cases, would hang up and need to be physically rebooted. Access was granted via swiping an employee's identification badge on the access pad by the server room door. The problem was that nobody on the development team was allowed into the server room, nor were we allowed to keep the server (even though it only contained test data) outside the server room. This meant that somebody else would have to reboot the computer, and since the server operators were busy with projects of their own, they would open the door and put a pencil in it so we could go back and forth at will without bugging them. This clearly opened the security room to a physical breach of security, but an inflexible and strict security policy that stated only server operators had access to the server room and all servers must be in the server room opened the door (no pun intended) to this kind of security circumvention in the name of productivity.

boards in employee lunch rooms, voicemail broadcast, employee reviews, and training programs are all great and varied ways to get the word out. Don't rely on one method because, for example, some employees never visit the intranet site or delete lots of e-mails without reading them.

Also make sure that the policies reflect current administrative practices, which will keep the policies from becoming outdated. Administrators will recognize when security policies are outdated and will deem them worthless. You need to make sure that they do not contain references to old technology or that they are for servers or networks that do not exist. You should make changing the policies part of the policies. You don't create security policies once; it is a constant work in progress as threats, data, or your organization change.

In the "Analyzing Security Policies and Procedures" Design Scenario, you will create the basis for a security policy for a company.

## Enforcing Security Policies on Windows Server 2003

The process of creating security policies and procedures will allow you to produce documentation that contains the following:

- The procedures and policies for security in your organization.
- Configuration information and procedures for each server, component, device, and application you have on your network. This should be detailed information that would allow you to create an exact copy of the configurations of the system.
- Change management procedures that define the policies and procedures to follow when changes to the network are made. You would define who needs to know and what needs to be done when changing configuration settings, applying software updates, or applying hotfixes and services packs.



## Design Scenario

### Analyzing Security Policies and Procedures

The folks at Infinite Horizons pride themselves for maintaining the confidentiality of all customers' data; therefore, security is very important to them. They have implemented password policies and their internal network is protected by a firewall. They have had laptops stolen that contained customer data in the past. They have also had some internal security lapses where shares were assigned incorrect permissions and employees had access to confidential customer data. Infinite Horizons needs to protect data between its customers and its corporate headquarters.

**1. Question:** What are some items that should be included in the security policy for Infinite Horizons? **Answer:**

- The customers' data must be confidential.
- Employees must follow the password policy issued by the network administrative staff that includes maintaining complex passwords.
- Employees must store customer data in a set of folders like a Customer Data folder or a subfolder with EFS enabled on their laptop computers to ensure that it is encrypted.
- Employees should not be able to access the network data or documents that have not been approved for use for their job function.
- Employees' actions should be recorded and audited to determine if access controls are adequate and if employees are complying with company policy.

All this will need to be applied to servers as they are built. They will also need to be reviewed regularly to determine if procedures are being followed by administrative staff. You will use the review process to address new threats not originally conceived of when the procedures were put in place. It is best if you schedule reviews to happen at regular intervals through the year.

A *security baseline* details the configuration procedures for each server, device, or application on your network. It contains the configuration of the operating system, settings for applications, permissions assignments, user accounts needed, and any additional settings needed to implement the security procedures. The security baseline is a tool that aids you in re-creating a server with the proper settings or in auditing a server at a later date to see if it is in compliance with the security procedures. It can be as simple as a checklist, or it can be a document that states the steps needed to configure a computer, or it can be something enforced in software (as you will see shortly). Implementing a security baseline can be tedious, so Windows Server 2003 contains the ability to automate the process of applying and auditing your security baseline.

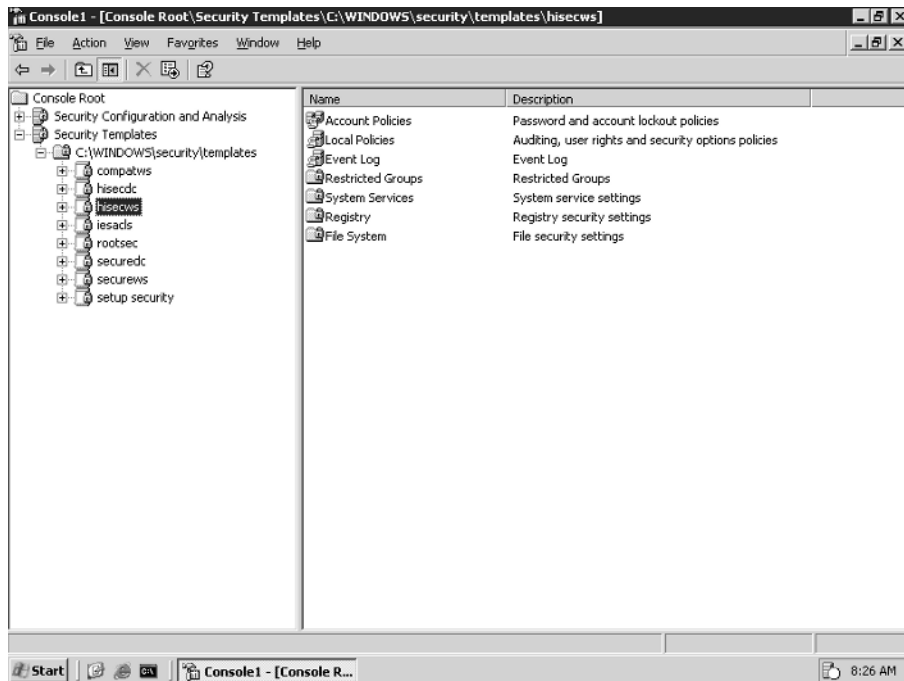
You can apply baseline security at the domain level and the computer level. At the domain level, it involves the settings to all computers that are a member of the domain. This is a good place to implement account policies like password length and authentication types allowed. These settings will override the local computer settings throughout the domain and gives you control over policies in one place.

You can implement a security baseline at the computer level in Windows Server 2003 by using the Security Templates and Security Configuration And Analysis snap-ins, the Local Security Policy administrative tool, or Active Directory Group Policy. These tools allow you to create a new template file or modify one of the existing templates, apply it to the configuration of the server, and test to see if the computer is in compliance with a previously applied template.

The templates are rich in settings that you can apply to the computer. You can define what services are allowed, rights user have to the box, account policies, IPSec policies, and lots of other security settings.

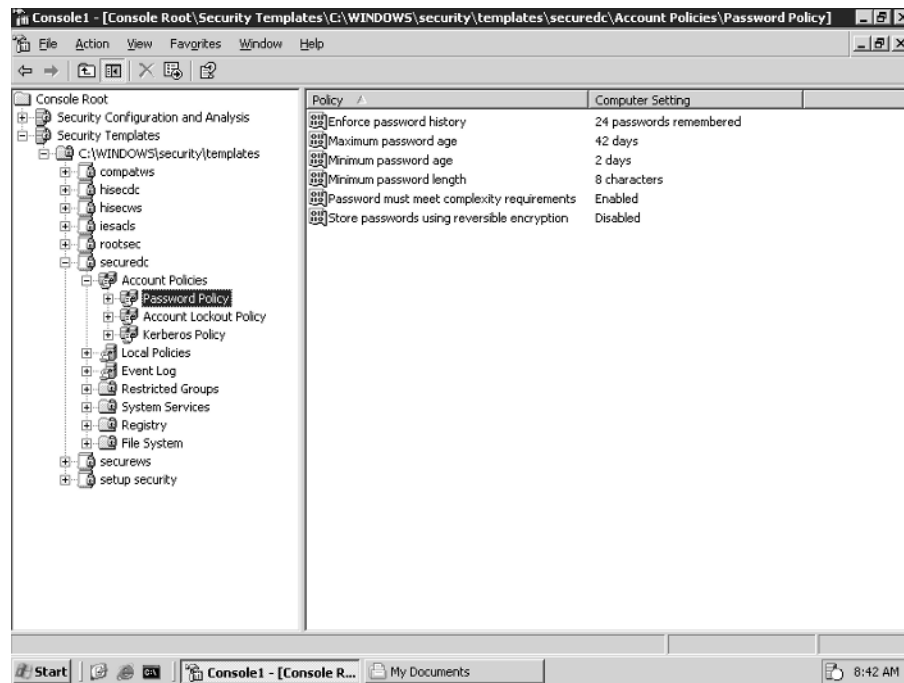
To apply templates and verify the security base of a computer, follow these steps:

1. Log on to Windows Server 2003 if you have not done so already.
2. Click Start > Run.
3. Type `mmc` in the Run dialog box to launch the Microsoft Management Console.
4. Click the File menu and choose Add/Remove Snap-in.
5. Click the Add button on the Add/Remove Snap-in dialog box, which opens the Add Standalone Snap-in dialog box.
6. Add the Security Configuration And Analysis and Security Template snap-ins to the console by clicking on the snap-in name and clicking the Add button.
7. Close the Add Standalone Snap-in dialog box.
8. Close the Add/Remove Snap-in dialog box. You will then see the security policy templates are now displayed in the MMC console.



## 14 Chapter 1 • Analyzing Security Policies, Procedures, and Requirements

9. Expand the Security Templates console tree. This lists the templates currently installed in the security templates folder (usually located in `WINDOWS\security\templates`).
10. Expand the `securedc` template. You should see the nodes that you can use to set the security policies for this computer. These policies can be used as part of the security baseline.
11. Expand the Account Policies node and click Password Policy. Notice that there is a default setting for each password policy.

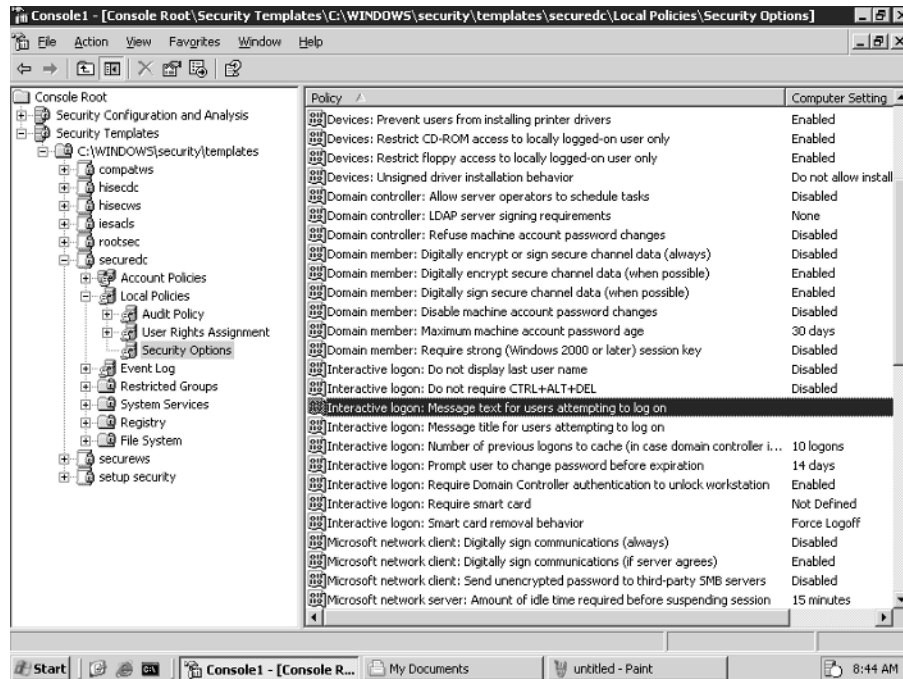


12. You can adjust these properties by double-clicking on the node and changing the value, but before you do, you should make a copy of the default template before you change it. To do this, right-click the `securedc` template and choose **Save As**. Type **DC Baseline** for the name of the template and click **OK**.
13. Open the DC Baseline template by double-clicking the DC Baseline node to expand the node.

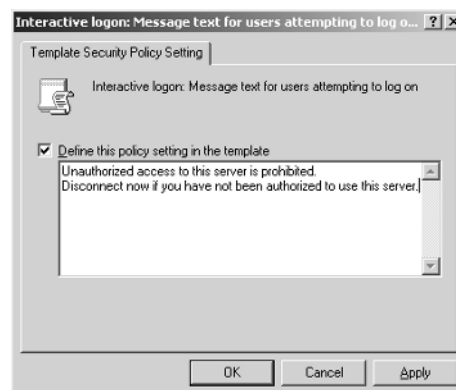
Feel free to explore the options you have for setting up the security template. In this case, set a message for users attempting to log in. To do that, follow these steps:

1. Navigate to the Security Options node by expanding the `securedc`, then the Local Policies node, then the Security Options node.

2. Locate Interactive Logon: Message Text For Users Attempting To Log On in the details pane (the pane on the right listing all the options).



3. Double-click the option to open the Template Security Policy Setting dialog box.
4. Make sure the text box is checked and type the following message:  
**Unauthorized access to this server is prohibited.**  
**Disconnect now if you have not been authorized to use this server.**



5. Save the template by right-clicking DC Baseline in the tree pane and choosing Save.

**16 Chapter 1 • Analyzing Security Policies, Procedures, and Requirements**

You can use security templates to define much more of the security baseline for this classification of servers by using security templates, such as which services are available on the box, Registry and file permissions, account and authentication settings, user rights, and so on.

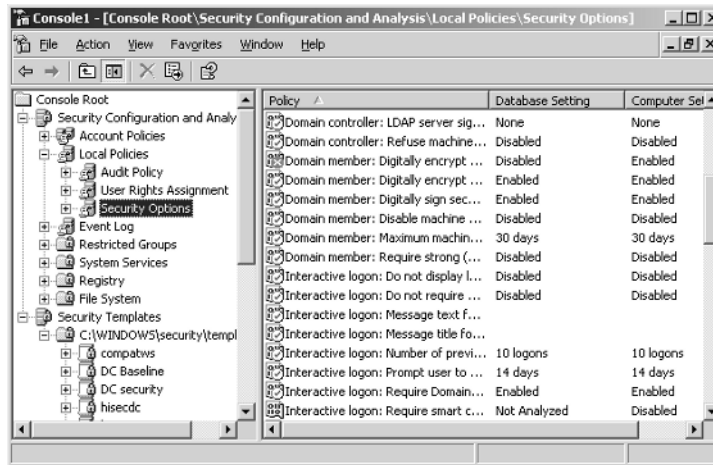
The Security Configuration And Analysis snap-in is used to apply the template we just created and to later analyze an existing server to see if it is still in compliance with the settings in the template (this makes it easier for you to verify your security baseline for the server through automation). The following steps show you how to use it:

1. Right-click the Security Configuration And Analysis node in the tree pane and choose Open Database.
2. In the Open Database dialog box, name the new template database by typing **DC Baseline** in the File Name field and click OK.
3. The Import Template dialog box appears. Choose the DC Baseline template from the list and click OK. You have loaded the DC Baseline template into the DC Baseline database. You could bring other templates into this database also and apply them all if desired.
4. To configure the server with the template settings, you need to apply it. Right-click the Security Configuration And Analysis node and choose Configure Computer Now.
5. Click OK to accept the default log path in the Choose Log Path dialog box. It may take a while for the template to apply.
6. Close the MMC by selecting Yes when asked to save the console. Save the console as Security Baseline Config.
7. Log off.
8. Press Ctrl+Alt+Del to log on and notice the message that is displayed.
9. Log in to your server using your user ID and password.

Now we will simulate how to verify whether a computer is meeting the security baseline described in the security policy template. To do this, follow these steps:

1. Open the Security Baseline Config console. It should be located in Start > All Programs > Administrative Tools.
2. Right-click the Security Configuration And Analysis node and choose Import Template from the context menu.
3. In the Import Template dialog box, choose the securedc template and click the Open button.
4. Configure the computer with the securedc template settings by right-clicking the Security Configuration And Analysis node and choosing Configure Computer Now.
5. Click the OK button to accept the default log path and wait for it to process the new template.
6. Assume that it is time to audit the security baselines of your domain controllers to see if they comply with the DC Baseline template you created. Right-click on Security Configuration And Analysis node and choose Analyze Computer Now from the context menu.
7. Click the OK button to accept the default log location.

8. After the analysis is completed, navigate to the Message Text For Users Attempting To Log On node (located in Local Settings\Security Options). You should see an X next to the node, indicating that the security policy has changed. The green check mark by other settings mean they match. A blue icon represents settings that are not defined in the security templates in the database.



## Analyzing Requirements for Securing Data

Organizations depend on the availability of their data. An organization needs to secure its data so that it can do business as usual. *Securing data* means controlling access to the data. Organizations will have different needs when it comes to securing data, so you will need to analyze the organizational requirements for securing data and build a plan. This involves more than just analyzing what access permissions are needed for the data. You need to consider the issues discussed in the following sections.



For more information on securing data, see Chapter 5, “Designing an Access Control Strategy for Network Resources.”

## Network versus Local Storage of Data

You need to decide whether the data will be stored on the network, locally, or a mixture of both. If you store the data on the network, it will be easier to secure and protect against loss than if it is saved locally. For example, it is easier to back up and physically secure data on a server than on individual desktops. You could then implement file synchronization to keep the server and laptop versions in sync with each other and make the data available to the laptop user when they are not connected to the network. Laptop computers do not stay in one place by their very nature. That means any data on the laptop is vulnerable to being lost or stolen if the laptop is

**18 Chapter 1 • Analyzing Security Policies, Procedures, and Requirements**

physically taken. This will need to be taken into account and can be somewhat mitigated by the Encrypting File System (EFS). If the data is really important, you should not allow it to be placed on the laptop computers. This would introduce another problem because the data on the server would not be available when laptop users are not connected to the network. You will need to weigh the security concerns with the productivity concerns.

**Back Up to Safeguard Against Corruption**

You should have a backup strategy in place to guard against lost or corrupted data. If a computer has been compromised, you cannot be certain that it is clean unless you rebuild the system and restore the data from a clean backup. You could have also fallen victim to a virus that corrupts data. A backup policy is an essential requirement to recovering data from corruption, which is one of the three risks to network security. First, you need to decide what data to back up. Important assets such as contracts, reviews, and other documents on the file server should be backed up when changed, whereas other files might need to be backed up once a week. You need to remember that data is stored in other places on the network, such as SQL Server 2000 or Exchange Server 2003 public folders, and not just on a Windows Server 2003 file server. The backup policy should include this data.

You also need to determine the frequency with which the backups should occur. You should use the service level agreement (SLA) to determine this requirement. The SLA should define the amount of data that the organization can tolerate losing. You will need to adjust the backup policies accordingly. For example, a financial organization we consult for requires that no more than an hour of transactions can be lost in a SQL Server–based application they run. We set up a transaction log backup every hour to meet this requirement. This will vary among the different types of data in the organization, so you need to figure out what the policy will be on a case-by-case basis.

You may also consider redundant hardware to guard against data loss. Using a Windows Server 2003 Enterprise Edition cluster or even just using RAID 1, 5, or 1+0 technology can protect against data loss due to hardware failure. You still need to back up your data because hardware technologies do not guard against corruption, whether malicious or accidental.

**Auditing Data Access**

You need to make sure you determine what type of auditing is necessary for your data. Important resources should be audited, and audit logs should be read on a regular basis to verify that only authorized users are gaining access to the data. In addition, you need to consider the audit log as valuable data and protect it. After gaining access to your data, a clever attacker will try to cover their tracks by cleaning up the audit log. You will also want to set policies that specify the length of time the audit logs need to be kept. This may be influenced by industry regulations, which you must take into account.



Auditing data will be covered in more detail in Chapter 5.

## Access to Data

You need to determine which users need access to data and apply the appropriate permissions to the type of data in question. This could include tasks that range from managing share and NTFS security permissions on a file server to applying physical security that controls access to the server room where the servers that house the data reside. You will also need to document and apply the appropriate permissions for software applications and other application servers on the network.

In a large organization, you will create a standard security policy and then have the database administrators, the e-mail administrators, or the administrator group of the application server craft domain-specific security policies. Once you have defined the permissions, you should create a script or template to reapply permissions at regular intervals. This will correct any unintentional mistakes that an administrator makes in applying permissions or undo any malicious changes. This is also useful in that the security administrators can use a tool to manage permissions that may make their jobs easier.



You will learn about securing the Windows Server 2003 filesystem, Registry, and Active Directory in Chapter 5.

## Data Retention

As part of the security policy, you need to determine how long you will keep data that is generated by your organization. For example, with backup policies in place, backup files will be generated. You need to determine the number of backups you need to keep to successfully recover corrupt data. You can use industry regulations and norms, gut feeling, or tradition for this, but we propose that you keep the backups that you have generated since the last time you verified that a backup was successful. (A backup is successful if you were physically able to recover from the backup to a recovery test server.)

You will need to apply data retention times to audit logs, windows logs, e-mails, backups, and versions of files, to name a few. Whenever possible, consider industry regulations and then consider the nature of the data. For example, how many audit logs do you need to keep to track down malicious user activities for use in a court case? We recommend at least 90 days but this may vary depending on the requirements for your industry and company.

After you have analyzed the organization's requirements for securing data, you will need to look at the security requirements of different types of data, such as data that is stored online, data that is stored locally, backups, audit and system logs, databases, application servers, and data being transferred across a network.

Data that is a common resource (such as for all employees or for clients and employees) is stored online, and requires that the access permissions must be maintained to prevent unauthorized access. You will also need to consider backup strategy and virus scanning to recover and prevent a common source of corruption. Viruses can cause corruption of data and so you will need to use virus scanning to prevent a virus from corrupting the data.

Data stored on a local workstation is not as secure as data stored solely on a central server like a file or web server because it is usually not physically secured. This is especially evident on laptops. This data would need to be encrypted to prevent someone from stealing a laptop and viewing the

## 20 Chapter 1 • Analyzing Security Policies, Procedures, and Requirements

data. The Encrypting File System included in Windows XP can be used to secure files in this manner. Local application data might need to be addressed separately. You also will need to consider the backup strategy and virus scanning with updated pattern files on the client to prevent corruption.

Backups will need to be secured themselves. If you lose the backup, you have lost everything. You should develop a plan for offsite storage of backup files or a plan that backs up the data to another location. You should also develop a plan to protect backup files that are stored on the network from attack.

The audit and system logs will need to be protected for the information they contain. You also need to determine how long you will keep them and who will have access to them.

Databases contain data used by many of the line-of-business applications of the organization. You need to work with the database administrators to create a policy to protect the database. This will involve access control, backup policies, and audit policies similar to those for file data.

Application servers like COM+, IIS, and even line-of-business applications store data about their configuration that would need to be available to bring the server back up. They also can generate temporary files that could contain sensitive information, and these files should be treated with the same care that you treat the regular data.

Data being transferred over communication wires needs to be secured. This could be files, important e-mails, and credit card information on a website. You need to configure the appropriate type of encryption if this information is confidential and is passing over a public or insecure network. You can use technologies like SSL/TLS to secure HTTP or SMTP data, S/MIME to encrypt e-mail messages, and IPSec to establish a security tunnel to move any type of data.

You need to make sure that you consider all forms that the data will take when analyzing it for security purposes.

In the following Design Scenario, you will analyze the requirements for securing data of a fictitious company called Infinite Horizons.

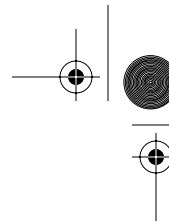


### Design Scenario

#### Analyzing the Requirements for Securing Data

An administrator at Infinite Horizons has been reviewing the audit logs and noticed that some data on the file server has been read by employees who are not supposed to have permissions to access it. This data is very important to the business and changes often during the hour. The business has deemed that it would not be cost effective to have to recover more than three hours' worth of data.

- 1. Question:** How can Infinite Horizons prevent unauthorized access to data? **Answer:** Make sure the appropriate access permissions are applied to the file server's data. This can be enforced by creating a security template and enforcing it with security policies.
- 2. Question:** What should the company do to decrease the likelihood of corruption of data? **Answer:** Centrally store data on a Windows Server 2003 file server and install antivirus software on each client and appropriate servers.
- 3. Question:** What else could you do to guard against data corruption? **Answer:** Create a backup policy that backs up the central server every three hours.



## Identifying Technical Constraints when Designing Security

Unfortunately, organizations are not homogenous when it comes to the technology that they implement. You will discover a variety of equipment and operating systems in your organization. The capabilities of the equipment, operating systems, and applications might limit your security options. You will need to evaluate the current network technologies used in your organization because they will affect what you can and cannot do with your security policies. If a risk is great and it is likely to occur, you might even need to change the existing infrastructure to accommodate a policy. Suppose, for example, that you would like to enforce software policies through Group Policy. This is most effectively accomplished through combining Group Policy and Active Directory. If you don't have Active Directory, it would be difficult. A short list of the technologies on your network that you need to evaluate follows:

- Authentication infrastructure
- E-mail
- World Wide Web service
- File sharing infrastructure
- Naming services
- Firewall/proxy services
- Custom software and services
- Remote access services
- PKI infrastructure
- Bandwidth
- CPU power of the servers (particularly with regard to encryption because it puts a heavy burden on processor power)



The means for securing each of the technologies in the preceding list will be discussed in greater detail in the appropriate chapter in this book.

You do not want technological limitations to guide your security policies. You should design security policies that would be theoretically best for the organization. You will need to identify areas where the security policies may not be consistent with the network's current technology. The organization can then decide whether it is cost effective to change or update the technology or whether to change the policy. Implementing a security policy that is not consistent with the network's technology puts an additional burden on the user by introducing interoperability constraints.

*Interoperability constraints* are restrictions brought on when two applications cannot communicate with each other and therefore cannot support the security protocols used to authenticate users on a network. Applications that have interoperability constraints could not support the necessary security





## Real World Scenario

### Exchange 2000 and Active Directory Distribution List

One situation in which you'll encounter technical constraints (and more specifically, interoperability constraints) is when you're trying to secure distribution group membership on an Exchange 2000 Server machine. If you need to support earlier versions of Windows than 2000 in Active Directory, then you'll need to enable the access group that's compatible with pre-Windows 2000 access groups to simulate the Everyone group in previous versions of Windows. This will allow down-level clients to enumerate the list of users in a distribution list. Unfortunately, it also means that everyone has permissions to view group membership, which leads to a problem with Exchange Server 2000. Because it relies on Windows 2000 Server security and distribution groups for its distribution lists, you will not be able to hide a distribution group's membership as long as you have earlier versions of Windows. You can either upgrade all the clients to Windows 2000 or greater and disable the group that's compatible with earlier versions or live without the ability to hide distribution group membership. You will need to decide, based on the security policy and cost, what you are prepared to do.

protocols used to authenticate users on the network. For example, if your organization's mainframe computer does not support Windows authentication, users would have to use a separate user ID and password to log on to the mainframe. Interoperability constraints can also be an issue when two different versions of an application are used. For example, you might need to use the less-secure protocol NTLM instead of Kerberos to authenticate users in a Windows domain because you need to support users on Windows 98 or Windows NT 4 computers in the domain. You will need to discover and investigate how interoperability constraints will affect your security policies and procedures.

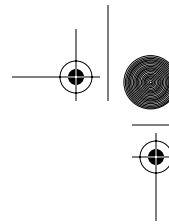
In the following Design Scenario, you will analyze the technical constraints that will impact the security of Infinite Horizons.



## Design Scenario

### Technical Constraints when Designing Security

Infinite Horizons has an outsourcing program for HR departments of client companies and needs to securely share information contained in its databases with customers. It also has some applications that the customers need to use to enroll employees in their benefits programs. They can also check on the status and current benefits of each employee. Infinite Horizons customers don't always use Windows-based computers, and those that do could be using any version from Windows 3.1 to Windows XP.



- 1. Question:** What are the technical limitations to Infinite Horizons's security policy? **Answer:** The client operating systems vary widely in capabilities. The client operating systems vary widely in capabilities, so use will not use the same ways of protecting them. For example, you might want to enforce a password policy that includes strong passwords, passwords longer than 8 characters, and a minimum of 4 days for the password. However, you may find that one of the operating systems that you are using does not support one of these features or you have to purchase a separate package.
- 2. Question:** What kind of interoperability issues might arise when clients connect to Infinite Horizons' network? **Answer:** Clients might not support the more secure version of authentication protocols or encryption technology that would be preferred for the sensitive data.

## Summary

Analyzing the existing security policy of an organization involves understanding what types of assets the company needs to secure and the cost effectiveness of securing them. Security policies are used to set goals that you will use to secure your assets. They need to be followed by users, IT staff, and managers to be effective. The risk that security policies are not followed can be mitigated through technology and personnel policies of incentives and punishments.

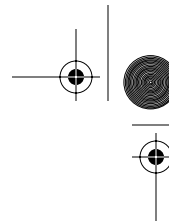
There are risks to hardware, software, people, and the data itself. All these risks can cause problems with availability of data and could ultimately affect a company's profits. It's important to know how to evaluate these risks and how to determine what technologies are needed to mitigate the risks. Some technologies may already be implemented on the existing network. Others may impose interoperability constraints, which will have an impact on what types of security and the level of security you can implement. Being able to recognize these situations and propose cost-effective solutions based on the requirements of the organization is the first step to providing effective security.

## Exam Essentials

**Know how to evaluate the most important security priorities for an organization.** Be able to choose the most important aspects of a company's security needs from the information you are given. You will be given more information than you need.

**Understand the requirements for securing data.** Know what data needs to be secured and the appropriate techniques for securing it.

**Recognize technical constraints or integration issues that are in conflict with security goals.** Know what the technical and interoperability constraints a company faces are and be able to take them into account when deciding on the appropriate technologies for policies.



## 24 Chapter 1 • Analyzing Security Policies, Procedures, and Requirements

**Consider government or industry regulations when designing security policies for a company.** You need to make sure that the policies you implement adhere to government and industry regulations. For example, the medical industry has guidelines for privacy of patient records.

**Know how to analyze what is successful or unsuccessful about the current security policy.**

Once you have determined where there are problems with the current security policies, you will need to decide whether to change the policy or update the technology; for example, you may have a password policy that requires 8-character passwords that are rotated every 45 days, but it is difficult to enforce on all of the devices on your network so there are some passwords that don't rotate every 45 days.

**Understand how risk is used to determine what needs to be secured.** You will be given many different choices about what to secure in an organization, but you will have limited resources and will need to determine which assets are the most important.

## Key Terms

Before you take the exam, be certain you are familiar with the following terms:

assets

security baseline

interoperability constraints

security policies

qualitative analysis

security risk analysis

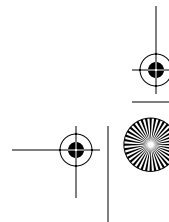
quantitative analysis

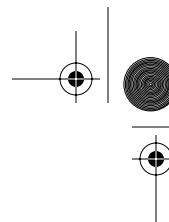
security threat

recommended security policies

standard security policies

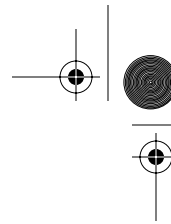
securing data





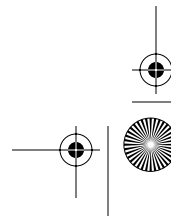
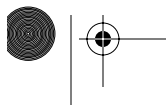
## Review Questions

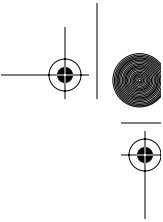
- Which of the following describes a security risk analysis?
  - Using the maximum amount of security possible on each asset in your organization
  - Reviewing the assets that need to be protected versus the cost of protecting the asset and the likelihood of the asset being attacked
  - Waiting for an attack to occur and then figuring out what you must do to repair the damage.
  - Determining what assets are at risk and providing the maximum amount of security to these assets
- When analyzing the security risks of a network, which of the following categories of assets should you be looking at? (Choose all that apply.)
  - Data
  - Hardware
  - Disks
  - Software
  - Backup plans
  - Documentation
- Jennifer's company is worried about sensitive company data being used on laptops that are stolen from time to time from the company's sales staff. The company sales force uses the data to sell products, issue quotes, and address customer concerns. There is not always a network connection and it is important that the sales force have the data. Jennifer wants to update the company's security policy to reflect this concern. Which of the following should she include in the security policy?
  - Laptop users need strong passwords.
  - Data should not be saved to laptop computers.
  - Laptop users must use smart cards for authentication.
  - A suitable form of encryption must be used on sensitive files located on laptop computers.
- Elliott is concerned about the servers in his company. Many are stored in spare offices or closets and a few have been stolen lately. What type of security should Elliott address in his company's security policy?
  - Logical
  - Physical
  - Data encryption
  - Password policy



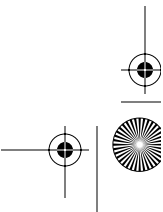
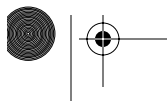
**26** Chapter 1 • Analyzing Security Policies, Procedures, and Requirements

5. Helena needs to connect a Unix server that does not support Active Directory to the network. Which of the following would be a technical constraint of enforcing security on the network by this addition?
  - A. Users on the Unix OS will not be able to use resources on the rest of the network.
  - B. Users on the Unix OS will not have secure access to files because Unix does not support access control lists (ACLs).
  - C. Administrators will be unable to enforce password policies through Group Policy for users on the Unix server.
  - D. Users on the Windows Server 2003 network will not be able to connect to the Unix server.
6. Faith works for a small firm that rents medical monitoring instruments to patients. Which of the following would need to be considered the most important part of its security policy?
  - A. Backup plan
  - B. Lockout period in the user password policy
  - C. Protection of data on laptop computers
  - D. Government industry regulations
7. Ann is the CTO of a large bank. The bank wants to provide a Web presence where its customers can view their financial records. What is the biggest risk to the customer that Ann should consider?
  - A. Controlling access to the internal file servers
  - B. Maintaining the privacy of financial records over the Internet
  - C. Making sure the users cannot manipulate cookies on their own computers
  - D. Avoiding ActiveX controls like Macromedia Flash in the building of its website
8. Dave manages a web application that his company's sales force uses to check on product information, place orders, and manage their customers' information. He only has a web server and FTP server installed. It is vital that this application is up for 24 hours, 7 days a week because it will translate into lost sales and potentially lost customers if it is down. Which of the following attacks should Dave be *most* concerned about?
  - A. Man in the middle
  - B. Spoofing
  - C. Spamming
  - D. Denial of service





- 9.** Lenin wants to automate the enforcement of many aspects of his company's security policy. What tools in Windows Server 2003 could he use to accomplish this purpose? (Choose all that apply.)
- A.** Active Directory Users And Computers
  - B.** Security Configuration And Analysis
  - C.** Security Settings
  - D.** Security Templates
- 10.** Which of the following should be considered when analyzing the requirements for securing data? (Choose the best answer.)
- A.** The type of data
  - B.** Data synchronization with mobile users
  - C.** Backup plan for the data
  - D.** Data access patterns



## Answers to Review Questions

1. B. Security risk analysis involves looking at the value of the assets you have. In other words, how much would it cost to replace or live without the asset? This will initiate a discussion of how much security you will need for each asset.
2. A, B, D, F. Data, hardware, software, and documentation are categories of items that should be looked at on a network when determining the network's security risks. The disks and backup plans are specific assets in these categories.
3. D. The policy would reflect that the sales staff will store files on their laptops and that the only real means of protecting sensitive information on laptops is through the use of encryption. A strong password policy and smart cards can be overcome simply by installing another version of Windows on the drive and using it to access the files. Strong passwords really provide security to network resources that are physically secure. The company could choose not to save data to laptops to be secure, but the sales force needs offline access to the data.
4. B. Elliott will need to establish the physical security of his servers. Data encryption and password policies will not protect against theft or vandalism at the physical level. Logical security would represent the software security mechanisms like passwords and access rights.
5. C. This is an example of technical constraints that may affect security on a network. Because the Unix server does not support Active Directory, it would have no information on the network's password policy. The policy would have to be configured separately on the Unix Server and it might not support the same options as Windows Server 2003.
6. D. The biggest cost to the small firm would be from penalties set in government regulations if it is not compliant. Therefore, although a backup plan, password policy, and protection of data on the laptops would also be prudent, government regulation will most likely cost the most in the short term.
7. B. The bank's strongest concern is the privacy of the customer's data sent over the Internet. If this information is not secure, it can cost them in fraud, lost customers, and image.
8. D. Dave should be concerned about a denial of service attack that will prevent legitimate users from accessing the web application. Man in the middle and spoofing involve changing information en route to the server, which may be a concern to Dave but are not his primary focus. Dave is probably not concerned with somebody using him as a spamming server because he is not running an SMTP server.
9. B, D. Using the Security Configuration And Analysis snap-in in combination with the Security Templates snap-in allows Lenin to enforce many aspects of the security policy and to verify that the configured server is still in compliance at a later time. You could push the policy out with Group Policy through Active Directory.
10. C. The data needs to be recoverable if it is to be secure, which means having a backup strategy that will successfully capture the data at regular intervals based on what the service level agreement defines as how much data can be lost. This will minimize the risk of deletion and corruption of the data. The type of data, access patterns, and data synchronization with mobile users are usually indirectly related to access control and encryption.

## Case Study

You should give yourself 20 minutes to review this testlet and complete the questions.

### Background

Infinite Horizons is a human resources consulting firm. It is located in Rochester, NY. It has been growing at the rate of 20 percent a year and currently has 200 employees at its headquarters in Rochester. Approximately 175 of the 200 employees are consultants. The consultants often work at many of the customers' sites.

### Computers

The network headquarters consist of 13 Windows Server 2003 machines and 200 Windows XP Professional workstations. Of the 200 workstations, 175 are laptop users. One of the servers is running SQL Server 2000 to support a Customer Relationship Manager (CRM) for the sales department. The company maintains a firewall. All the users have been granted dial-in permissions. The company maintains a VPN server and dial-up access because most of the employees connect from remote locations to the network. Employees can also use Outlook Web Access (OWA) to check their e-mail via a web browser.

### WAN Connectivity

The company has a DSL connection to the Internet at 1.5Mbps.

### LAN Connectivity

The LAN runs on a 100Mbps network.

### Security

The folks at Infinite Horizons pride themselves in maintaining confidentiality of all customers' data; therefore, security is very important to them. They have implemented password policies and their internal network is protected by a firewall. They have had laptops stolen that contained customer data in the past. They have also had some internal security lapses where shares had the incorrect permissions and employees had access to confidential customer data.

Infinite Horizons needs to protect data between its customers and its corporate headquarters.

## Network Usage and Roles

**Human Resources Department** The HR department uses a database application to maintain resumes and employee information. It also has a file server that stores additional employee confidential information like annual reviews.

**IT Department** The IT department maintains and supports the network. Members of this department implement physical and network security.

The help desk resolves first-level support issues and issues with employees' computers.

The server administrators group builds the network and resolves the company's server and network issues.

**Sales Department** The sales staff stores shared documents in a share called SALES and personnel sales documents on their local computers. They also need access to a SQL Server 2000 server that hosts their customer relations application and a lead-tracking system. They need to store some of the data on their laptops so it is available whenever they are not connected to the network.

**Consultants** Consultants use the network to communicate with each other. They are required to fill out forms in the intranet-based time tracking application. They also need to get access to proposals that certain managers are working on to help author them, and they need secure access to their e-mail through the Web.

## Security Policy

All users must securely authenticate on the network.

Data that is stored on laptop computers must be secure.

## Case Study Questions

1. What are the two primary risks to security for Infinite Horizons?
  - A. Customer data on stolen laptop computers
  - B. Denial of service attack on the Outlook Web Access server
  - C. Unauthorized access of the network via the dial-in server
  - D. Unauthorized access by employees to network data
  - E. Unauthorized access by employees to the customer relationship database
  - F. Unauthorized capturing and reading data being transmitted over the VPN connection to the company
  
2. What are the four security priorities of Infinite Horizons?
  - A. Preventing denial of service attacks on the Outlook Web Access server
  - B. Preventing unauthorized network access
  - C. Securing communications to client sites
  - D. Protecting employee data on laptop computers
  - E. Isolating the HR network from the rest of the network via an internal firewall
  - F. Providing SSL access to intranet resources
  - G. Secure authentication of all users
  - H. Enabling Windows Only authentication on SQL Server
  
3. What kind of technology would you use to secure data on the laptop computers?
  - A. NTFS permissions
  - B. Encrypting file system
  - C. Biometric scanner for reading employee fingerprints
  - D. A strong password policy
  
4. What technologies would you implement to guard against data corruption? (Choose all that apply.)
  - A. Virus scanner
  - B. Backups
  - C. Access control
  - D. Smart card reads
  - E. Data Encryption

- 32** Chapter 1 • Analyzing Security Policies, Procedures, and Requirements
5. What security policy statement would apply to Infinite Horizons?
    - A. Employees must use strong passwords to access the network as defined by the network administration group.
    - B. Employees must not lend their smart card to anyone.
    - C. Employees will not store company data on their laptops.
    - D. Hardware that requires user interaction must support a smart card reader.
  6. What technology should Infinite Horizons employ to make sure data moving between it and its clients is secure?
    - A. TCP/IP
    - B. Firewall
    - C. Encryption
    - D. Dial-up
  7. What technological limitation will Infinite Horizons face with regard to implementing security?
    - A. Password policy cannot be enforced.
    - B. Consultants may not be able to connect securely from client sites.
    - C. Laptop data will not be secure.
    - D. Data exchanged with clients will not be secure.
  8. What compromises will Infinite Horizons have to make to integrate security with a customer's network? (Choose all that apply.)
    - A. Different password policies
    - B. Data not confidentially exchanged
    - C. Separate passwords, no single login capability
    - D. No access control of the data
  9. What is the most important goal when securing assets that Infinite Horizons needs to address in its security policy?
    - A. Integrity of the SQL Server 2000 database
    - B. Confidentiality of customer data
    - C. Physical security of the laptop computers
    - D. Availability of the Outlook Web Access server
  10. What would be included in the security baseline for a laptop computer at Infinite Horizons?
    - A. Employees must use a smart card to log on to the laptop.
    - B. Back up the SQL Server database's transaction logs every three hours and perform a full backup every night.
    - C. Passwords must have at least eight characters and be complex.
    - D. Confidential customer data must be encrypted on a laptop.

## Answers to Case Study Questions

1. A, D. All of the answers describe possible risks to the Infinite Horizons network, but you need to consider probability when determining primary risks to the network. Because the company has had laptops with customer data on them stolen in the past and has had issues with employees having unauthorized access to network data, these two options have a higher probability of occurring and need to be mitigated.
2. B, C, D, G. You need to pay attention to any primary security risks that you have identified and the new security features that the customer would like implemented when deciding the security priorities of a company. Infinite Horizons wants to secure communications to client sites and, through strong password policies, secure authentication of users. It also recognized that data is compromised when laptops are stolen or employees have unauthorized access to resources.
3. B. Encryption would afford the best protection to the company's data if it was stolen or lost, which Infinite Horizons considers a risk because it has experienced it in the past. Another option would be to just not allow certain data to be stored on a laptop. NTFS permissions can protect data through access control and are important, but if someone has physical access to the hardware, NTFS permissions can be easily overcome. Likewise, a biometric scanner and strong passwords can be defeated if an attacker has physical access. In the case of Windows, an attacker can just install another copy and use the built-in administrator to access the data, and it is not too difficult to write a program that will read raw data off a hard drive.
4. A, B, C. Virus scanning helps prevent data corruption due to viruses, Trojan horses, and worms. Controlling access to data will prevent unauthorized users from corrupting or deleting the data. However, because neither virus scanning nor access control is one hundred percent successful, you will need to make sure that you have good backups and can successfully restore them when needed. Smart card readers and data encryption don't protect the data from corruption. Smart card readers are used to authenticate the user. This information is certainly useful when creating access control lists, but it is not directly related to preventing data corruption. Data encryption guards against a compromise in confidentiality of the data. Encrypted data can still be corrupted.
5. A. Option A is the only statement that applies to Infinite Horizons according to the scenario. Infinite Horizons does not use smart card technology, so its policy would not mention smart cards. Infinite Horizons allows company data to be stored on laptops and, according to the scenario, wants to address the issue of protecting it because laptops have been stolen.
6. C. Encryption is the way to secure data that is moving through a public network like the Internet. TCP/IP is the protocol of the Internet, but it does nothing to secure data. A firewall can prevent certain data from entering or leaving the company, but once the data is out on the Internet, a firewall is of little use. Dial-up access is usually over a public network and data would still need to be protected with encryption.
7. B. The consultants work at client sites much of the time and may not be able to use a VPN or other secure method to access their company resources. Password policy can be enforced with the Windows Server 2003 Security Configuration And Analysis snap-in. Laptop data can be secured with the Encrypting File System (EFS). Data can be exchanged with clients over an agreed-upon technology like HTTP-S or IPSec.

**34** Chapter 1 • Analyzing Security Policies, Procedures, and Requirements

- 8.** A, C. Infinite Horizons will not use the same technology for authentication as its customers use so, due to technical constraints, will need separate passwords for the customer's network. This may lead to employees at Infinite Horizons having to deal with different password policies. Confidential exchange and control of data is a requirement for integration, so no compromises will be made in these areas.
- 9.** B. While all these goals are important to Infinite Horizons, the company has stated that the confidentiality of customer data is the most important directive. If there are trade-offs to security due to technical limitations or resources, confidentiality of data will be the priority.
- 10.** D. The security baseline would include all of the procedures necessary to implement the security policy for the technology in question. The security policy for Infinite Horizons does not mention smart cards, so smart cards would not be necessary to access laptops. Performing backups of the SQL Server database would be part of the SQL Server baseline but not the baseline for the laptops. The security baseline for accounts would mention the password policy, but again this does not apply to laptop users.