11. Which of the following, if worded correctly, can protect companies from wrongful termination lawsuits?
    a. nondisclosure clauses
    b. acceptable use policies
    c. penalty clauses
    d. punitive clauses

12. A password policy might specify which of the following attributes for password selection?
    a. length requirements
    b. complexity requirements
    c. frequency for changing passwords
    d. all of the above

13. Which of the following provides employees with formal instructions about the organization's security strategy?
    a. acceptable use policy
    b. risk assessment
    c. strategy meeting
    d. security user awareness program

14. If organizations have employees who connect remotely, which of the following security concerns should be considered?
    a. the possibility of mobile devices being stolen
    b. virus infections spreading from home and mobile systems to corporate systems
    c. the use of updated, effective antivirus and firewall software on mobile devices or home systems that connect to the network
    d. all of the above

15. A password policy should be established in the _____ and enforced by _____ whenever possible.
    a. risk assessment process, management
    b. company Web site, network administrators
    c. security policy, software
    d. company employee handbook, security guards

Hands-On Projects

Hands-On Project 13-1: Calculating Replacement Costs

Time Required: 15 minutes

Objective: Use a risk analysis tool to calculate replacement costs for equipment.

Description: A software tool can help you perform risk analysis with consistency and objectivity. In this project, you download a trial version of a Windows tool called Project Risk Analysis (PRA) by Katmar Software. You then enter information about network resources in your school's lab and calculate the contingency funds needed to replace lab equipment if disaster strikes. You will need a file-archiving utility, such as WinZip. Enter values for computer equipment in your lab and estimate how much data is contained on each piece of equipment. You may need to research the cost of the network resources. The project specifies the names and costs of sample devices, but you can substitute the names and costs of your lab equipment. If you are not in your lab, you can use the information shown in the project steps.

1. Log on to either Windows Server 2008 or Windows 7.
2. Start your Web browser and go to **www.katmarsoftware.com/pra.htm**.
3. Read the description of the program, and then click **Download Now!**.
4. When you are prompted to open or save the Projrisk.zip file, click **Save** and then save the file to a folder in your file system.
5. When the download is finished, click **Close** in the Download Complete window. Exit your Web browser, and then double-click the file to open it with WinZip. Extract the files to the folder where you saved the .zip file you downloaded.
6. Double-click the **ProjRisk_Setup.exe** file, and follow the steps in the setup program to install the file on your computer.
7. Click **Start**, point to **All Programs**, point to **Risk Analysis**, and click **ProjRisk** to start the program. The first time you run the program, you see a window that states the terms under which the program can be run. (It runs 30 times as an evaluation.) Click **OK**, and then click **OK** again when you see a second shareware reminder.
8. Click **Add** to open the Add a Record at the End window. In the Description text box, type **Computers**.
9. In the Distribution section, click the **Normal** option button.
10. In the Likely Cost text box, type **15000**. Do not use commas when entering numbers. In the Low Cost text box, type **10000**.
11. Click **OK** to return to the main Project Risk Analysis window. Your estimate is entered in the first row.
12. Repeat Steps 8 through 11. Remember to click **Normal** in Step 9 each time. If you are not entering your own information, enter the following descriptions and costs:

Description: **Software**	Likely Cost: 5000	Low Cost: 3500
Description: **Printers**	Likely Cost: 500	Low Cost: 400
Description: **Switches**	Likely Cost: 150	Low Cost: 100
Description: **Cables**	Likely Cost: 100	Low Cost: 75
Description: **Monitors**	Likely Cost: 5000	Low Cost: 4000

13. In the main Project Risk Analysis window, click the **Analyze** button to see the Overall Cost Distribution graph. What are the Lowest Cost, Highest Cost, and Mean Cost?
14. Click the **Statistics** button. What is the mean cost in the Simulation Statistics Report window?
15. Close the Simulation Statistics Report window, and exit Project Risk Analysis. Leave your system running for the next project.

Hands-On Project 13-2: Conducting Security Policy Analysis

Time Required: 20 minutes

Objective: Evaluate security policy clauses, identify deficiencies, and update policies in response to events or changes.

Description: Security policies should be revised to address security breaches or new threats. In this project, you evaluate the theft of proprietary information and identify some obvious deficiencies in a security policy. Then you recommend changes to the security policy to prevent similar incidents from recurring.

A local branch office of a major national stock brokerage had no policy that required the termination of user ID and password privileges after employees leave. A senior trader left the brokerage and was hired by a competing brokerage. Shortly thereafter, the first brokerage lost two clients who said they were moving to a competing firm; their personal data files disappeared mysteriously from the company's databases. In addition, a year-end recommendations report that the senior trader had been preparing was released two weeks early by the competing brokerage. An investigation of the company's access logs revealed that the employee records file had been accessed by someone outside the company. The job records, however, did not reveal whether the report had been stolen because they had not been set up to record object accesses in a log.

The existing security policy states the following:

"On termination, employees shall surrender any laptops, disks, or computer manuals they have in their possession. They are no longer authorized to access the network, and they shall not take any hardware or software when they leave the office."

1. What changes would you make to the existing security policy so that security is improved after employees are terminated?
2. Brainstorm for ideas to develop a security policy clause that covers access of company records and helps track when files are accessed.

Hands-On Project 13-3: Collecting a Hardware and Software Inventory

Time Required: 15 minutes

Objective: Create a hardware and software inventory of your network and save it to a file.

spill. Be sure to look in all directions, including the ceiling. Be sure to note drop ceilings or false floors because they are a potential point of access for intruders.

4. Next, examine the probabilities of a threat occurring. Use the information in Table 13-2 as a guide. For example, if you listed a leaky roof as a threat and you live in an area with frequent rainfall, the probability of that threat occurring and causing damage is high. If you live in an arid desert climate, that probability is not as high.
5. Next, determine security controls to reduce threats. Beginning with your first asset, look for ways to manage risks to it, and write down safeguards. If the roof is leaking above an expensive computer, the cost of repairing the roof might be warranted, but simply moving the computer reduces the risk and is more cost effective. On the other hand, if the power supply to the server room is prone to fluctuations that could damage delicate electronics, investing in uninterruptible power supplies (UPSs) or a generator could be less expensive than replacing damaged equipment. Remember that the priority level determines the investment in security.
6. If time permits, share your findings with the class. Discuss the results and justify your assessments and recommendations. Were the results similar? Discuss similarities and differences in findings.

Case Projects

Case Project 13-1: Conducting Risk Assessment and Analysis

Risk assessment can be as simple as noting an unlocked door or a password written on a slip of paper, or it can be a complicated process that requires several team members and months to complete. A large enterprise environment probably has multiple locations, diverse activities, and a wide array of resources to evaluate. You do not need such a complicated network, however, to work through this case project. The main idea is to learn how to apply your knowledge in a methodical fashion to produce useful and accurate results. Approaching a task such as risk assessment without a strategy in place usually results in repeated steps, wasted resources, and mediocre results at best. Even worse, you might miss critical information.

In a real risk analysis, one of the first steps is to meet with all department managers, upper management, employee representatives, workers in the production environment, human resources staff, and other staff members to get their input. Such a meeting is not possible in this situation, so direct any questions to your instructor or do independent research to find your answers.

In this project, you conduct a risk assessment and analysis of a small e-commerce business. You decide what product or service the business sells over the Internet. Use the following files provided by your instructor:

- Facilities diagram
- Network diagram
- Asset identification worksheet

- Business process identification worksheet
- Threat identification and assessment worksheet
- Threat mitigation worksheet

1. Give your company a name.

   Company name: _____

   Products or services: _____

2. Identify the business processes that must continue for the organization to keep functioning—for example, collecting money from customers, receiving and processing sales, and developing new products. List major business processes that drive your company in the Business Process column of the business process identification worksheet. (Use your imagination and common sense to complete this step.) Assign a priority level to each process using the priority rankings in the following list. Write down the department that performs the process. Leave the Assets Used column blank for now.
   - *Critical*—Absolutely necessary for business operations to continue. Loss of a critical process halts business activities.
   - *Necessary*—Contributes to smooth, efficient operations. Loss of a necessary process doesn't halt business operations but degrades working conditions, slows production, or contributes to errors.
   - *Desirable*—Contributes to enhanced performance and productivity and helps create a more comfortable working environment, but loss of a desirable process doesn't halt or hurt operations.
3. Identify the organization's assets. Using the asset identification worksheet, list each asset, its location, and its approximate value, if known. For multiple identical assets, describe the asset and list the quantity instead of listing each asset. In organization-wide risk assessments, you would list all assets, including office furniture, industrial equipment, personnel, and other assets. For this project, stick to IT assets, such as computers, servers, and networking equipment. List all the equipment needed to build your network as well as any cabling in the facility. Assume that the facility is already wired for a computer network and has network drops for each computer. Remember to list items such as electricity and your Internet connection.
4. Next, determine which assets support each business process. On your business process identification worksheet, list the assets needed for each business process in the Assets Used column.
5. Document each process and assign a priority to it. Next, transfer the priority rankings to your asset identification worksheet. Now you know which assets are the most critical to restore and warrant the most expense and effort to secure. You also have the documentation to justify your security actions for each item.
6. Next, assess existing threats. Table 13-7 shows examples of evaluating types of threats and suggests ways to quantify them. On the threat identification and

assessment worksheet, list each possible threat. Be sure to consider threats from geographic and physical factors, personnel, malicious attacks or sabotage, and accidents. Also, examine the facilities diagram for flaws in the facility layout or structure that could pose a threat, such as an air-conditioning failure or loss of electrical service. For each threat, assess the probability of occurrence (POC) on a scale of 1 to 10, where 10 represents the highest probability. Enter the ratings in the POC column for each threat.

Type of threat	How to quantify
Severe rainstorm, tornado, hurricane, earthquake, wilderness fire, or flood	Collect data on frequency, severity, and proximity to facilities. Evaluate the past quality and speed of local and regional emergency response systems to determine whether they helped to minimize loss.
Train derailment, motor vehicle accident, toxic air pollution caused by accident, or plane crash	Collect data on the proximity of railroads, highways, and airports to facilities. Evaluate the construction quality of transportation systems and the rate of serious accidents on each system.
Building explosion or fire	Collect data on the frequency and severity of past incidents. Evaluate local emergency response to determine its effectiveness.
Militant group attacking facilities, riots, or civil unrest	Collect data on the political stability of the region where facilities are located. Compile and evaluate a list of groups that might have specific political or social issues with the organization.
Computer hacking (external) or computer fraud (internal)	Examine data on the frequency and severity of past incidents. Evaluate the effectiveness of computer security measures.

Table 13-7 Threat evaluation and quantification methods

7. Using the asset identification worksheet, determine which assets would be affected by each threat. List those assets in the Assets Affected column of the threat identification and assessment worksheet. For an electrical outage, for example, list all assets that require electricity to operate. For a hardware failure, list all assets that a hardware failure would disrupt, damage, or destroy.
8. In the Consequence column, enter the consequences of the threat occurring. Use the following designations:
   - *Catastrophic (C)*—Total loss of business processes or functions for one week or more; potential complete failure of business
   - *Severe (S)*—Business would be unable to continue functioning for 24 to 48 hours; loss of revenue, damage to reputation or confidence, reduction of productivity, complete loss of critical data or systems

- *Moderate (M)*—Business could continue after an interruption of no more than four hours; some loss of productivity and damage or destruction of important information or systems
- *Insignificant (I)*—Business could continue functioning without interruption; some cost incurred for repairs or recovery; minor equipment or facility damage; minor productivity loss and little or no loss of important data

9. Rate the severity of each threat in the Severity column. Use the same designations as in Step 8 (C, S, M, or I). You derive these ratings by combining the probability of occurrence, the asset's priority ranking, and the potential consequences of a threat occurring. For example, if an asset has a Critical (C) priority ranking and a Catastrophic (C) consequence rating, it has a Catastrophic (C) severity rating. If you have mixed or contradictory ratings, you need to reevaluate the asset and use common sense to determine the severity rating. A terrorist attack that destroys the facility might have a POC of 1, depending on your location, but the consequences would definitely be catastrophic. Even so, because of the low POC, you wouldn't necessarily rank its severity as catastrophic.
10. On the threat mitigation worksheet, list assets that are ranked as the most critical and are threatened with the highest severity. In the Mitigation Techniques column, list recommendations for mitigating threats to those assets. For example, to mitigate the threat of an electrical outage damaging a critical server, you might suggest a high-end UPS.
11. Review your work, and submit it to your instructor.

11. Before installing new signatures for an IDPS, what do you need to do?
    a. Back up the IDPS.
    b. Stop the IDPS.
    c. Change passwords.
    d. Double-check to verify whether new signatures are necessary.
12. What can happen if you change a security configuration too abruptly and without proper authorization? (Choose all that apply.)
    a. Employees might ignore the change.
    b. The change might surprise other security managers.
    c. You might be flooded with protests from employees.
    d. You could face disciplinary action.
13. The change management process might apply when which of the following occurs? (Choose all that apply.)
    a. New password logon procedures are needed.
    b. You need to block access to DMZ servers.
    c. A new VPN gateway is installed.
    d. You need to change a fragmentation rule in a packet filter.
14. Security auditing involves which of the following? (Choose all that apply.)
    a. reviewing log files
    b. reviewing hardware and software costs
    c. testing defenses
    d. rotating firewall logs
15. What is nonrepudiation?
    a. the ability of a system to authenticate users
    b. the ability to rely on information gained through a security audit
    c. a legal defense used by employees whose privacy has allegedly been violated
    d. the ability to validate transactions through electronic documentation

Hands-On Projects

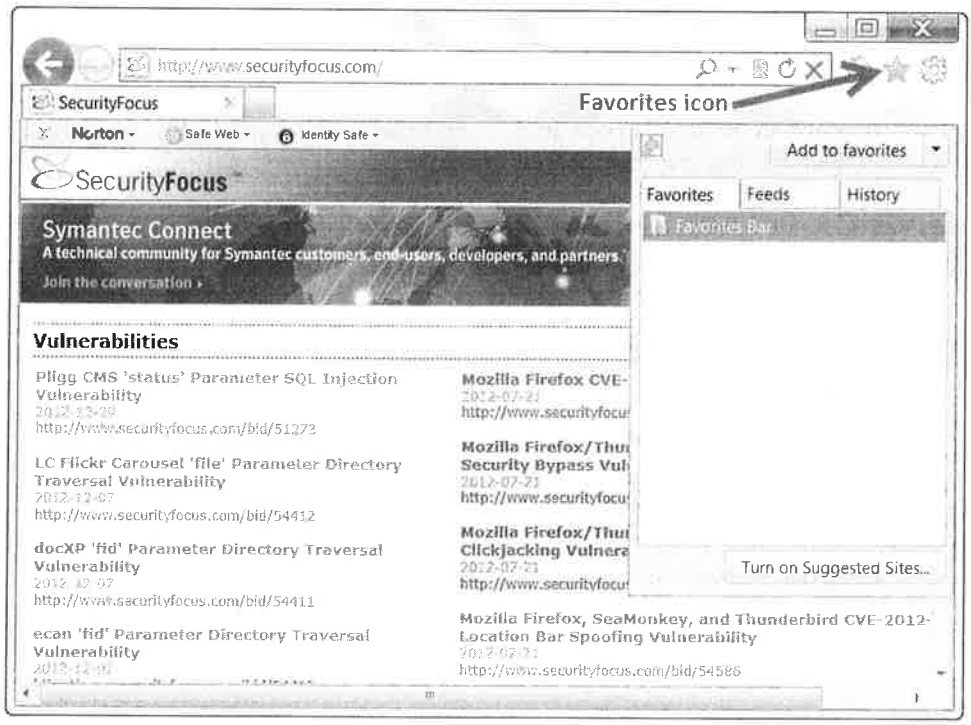
Hands-On Project 14-1: Assembling Security-Related Bookmarks for Web Pages

Time Required: 20 minutes

Objective: Create a list of Web sites to use as resources for staying updated on the latest developments in security.

Description: As part of your ongoing security management program, you need to consult dedicated Web sites and other resources to remain informed about network defense issues. One way to ensure that you check these resources regularly is to assemble a list of bookmarks that you can access quickly. You can then set up an e-mail reminder to check for updated software and other security-related news. For this activity, you need a computer with an Internet connection and Internet Explorer 9 installed.

1. Start your browser and go to ***www.securityfocus.com***.
2. Click the **Favorites** icon (see Figure 14-5), click the **Add to favorites** arrow, and click **Organize favorites**.



Source: Symantec Corp.

Figure 14-5 Internet Explorer favorites

3. Click **New Folder**, replace "New Folder" with the name **Security**, and then press **Enter**.
4. Click **New Folder**, replace "New Folder" with the name **News**, and then press **Enter**.
5. Click **Move**, click the **Security** folder, and then click **OK**.
6. Repeat Steps 4 and 5 to create two more new folders named **Conversations** and **Other Resources**.
7. Click **Close**.

8. Add the Security Focus home page to the News folder. Click the **Favorites** icon, click **Add to favorites**, click the **Create in** arrow, click **News**, and click **Add**.
9. Near the top of the Security Focus home page, click **Join the conversation**. Add this page to the Conversations folder using the procedures in Step 8.
10. Scroll down the Security Focus home page to the Mailing Lists section. You could choose to subscribe to mailing lists, but in this step you add a mailing list to your favorites. Find the Penetration Testing heading and click **Complete Archive** below it.
11. Click the **Favorites** icon, click **Add to favorites**, and enter **Penetration Testing** in the Name text box over the default name. Verify that the Create in text box is set to Conversations, and click **Add**.
12. Return to the Security Focus home page, and repeat Steps 10 and 11 to add two more mailing list sites to the Conversations folder.
13. As an optional final step, add the URLs listed earlier in this chapter to the appropriate folders in your Security favorites folder. Specifically, add the URLs listed in the "Staying Informed About Security Trends" section.

Hands-On Project 14-2: Assembling Security-Related Bookmarks for RSS Feeds

Time Required: 20 minutes

Objective: Create a list of RSS feeds to use as resources for staying updated on the latest developments in security.

Description: Rich Site Summary (RSS) feeds allow publishers to syndicate blogs, news, and other types of content that might change frequently. You can obtain specific clients and RSS reader software or view feeds in Internet Explorer and other browsers. For this activity, you need a computer with an Internet connection and Internet Explorer 9 installed.

1. Start your browser and go to ***http://searchsecurity.techtarget.com/rss***.
2. On the SearchSecurity Web page under Security Wire Daily News, click the RSS icon shown in Figure 14-6.

Source: Mozilla Foundation

Figure 14-6 RSS feed icon

3. In the SearchSecurity: Security Wire Daily News window, click **Subscribe Now**. In the next window, click **Subscribe**.
4. You can now access this RSS feed from the Favorites icon in the Feeds tab.
5. Search the Internet for three more RSS feeds associated with topics in this book. Add the feeds to your feeds list.

Case Projects

Case Project 14-1: Information Security Certifications

To ensure that information technology workers maintain up-to-date knowledge about information security, many employers require periodic certification. An ever-growing list of information security certifications is offered by a variety of vendors. Some commonly sought certifications are administered by ISC^2, SANS, and CompTIA. U.S. Department of Defense directive DoD 8570 includes certification requirements for both DoD workers and support contractors. The directive defines employee position levels and certifications required at these levels. As of this writing, the latest version of the directive is 8570.01-M (*www.dtic.mil/whs/directives/corres/pdf/857001m.pdf*).

For this project, summarize the requirements of DoD 8570 in your own words. Include a definition of the three IAT (Information Assurance Technical) position levels. Describe the typical tasks performed by these workers, list the certification requirements for these levels, and include a summary of the objectives of each certification required at these levels.