CHAPTER 12 Managing Systems Support and Security

Chapter 12 describes systems support and security tasks that continue throughout the useful life of the system. In addition to user support, this chapter discusses maintenance, security, backup and disaster recovery, performance measurement, and system obsolescence.

INTRODUCTION

OBJECTIVES

When you finish this chapter, you will be able to:

- Explain the systems support and security phase
- Describe user support activities, including user training and help desks
- Define the four types of maintenance
- Explain various techniques for managing systems maintenance and support
- Describe techniques for measuring, managing, and planning system performance
- Explain risk management concepts
- Assess system security at six levels: physical security, network security, application security, file security, user security, and procedural security
- Describe backup and disaster recovery
- List factors indicating that a system has reached the end of its useful life
- Assess future challenges and opportunities for IT professionals
- Develop a strategic plan for career advancement and strong IT credentials

Managing systems support and security involves three main concerns: user expectations, system performance, and security requirements.

A systems analyst is like an internal consultant who provides guidance, support, and training. Successful systems often need the most support because users want to learn the features, try all the capabilities, and discover how the system can help them perform their tasks. In most organizations, more than half of all IT department effort goes into supporting existing systems.

This chapter begins with a discussion of systems support, including user training and help desks. You will study the four main types of maintenance: corrective, adaptive, perfective, and preventive. You also will learn how the IT group uses maintenance teams, configuration management, and maintenance releases, and you will examine system performance issues and maintenance tools. You will analyze the security system at each of the six security levels: physical security, network security, application security, file security, user security, and procedural security. You will also learn about data backup and recovery issues. Finally, you will learn how to recognize system obsolescence, and about some of the challenges and opportunities you are likely to face as an IT professional.

Chapter Introduction Case: Mountain View College Bookstore

Background: Wendy Lee, manager of college services at Mountain View College, wants a new information system that will improve efficiency and customer service at the three college bookstores.

In this part of the case, Tina Allen (systems analyst) and David Conroe (student intern) are talking about operation, support, and security issues for the new system.

Participants: Tina and David
Location: Tina's office, Friday afternoon, March 30, 2012
Project status: Tina and David successfully implemented the bookstore information system. Now they will discuss strategies for supporting, maintaining, and securing the new system.
Discussion topics: Support activities, training, maintenance, techniques for managing systems operation, enhancing system performance and security, and detecting system obsolescence

Tina: Well, we finally made it. The system is up and running and the users seem satisfied. Now we focus on supporting the system, ensuring that it delivers its full potential, and is properly secured and protected.

David: *How do we do that?*

Tina: First, we need to set up specific procedures for handling system support and maintenance. We'll set up a help desk that will offer user training, answer technical questions, and enhance user productivity.

David: *Sounds good. I'll set up a training package for new users who missed the initial training sessions.*

Tina: That's fine. You also should learn about the four types of maintenance. Users typically ask for help that requires corrective maintenance to fix problems or adaptive maintenance to add new features. As IT staff, we will be responsible for perfective maintenance, which makes the system more efficient, and preventive maintenance to avoid problems.

David: *Anything else for us to do?*

Tina: Yes, we'll need a system for managing maintenance requests from users. Also, we'll need to handle configuration management, maintenance releases, and version control. These tools will help us keep the system current and reduce unnecessary maintenance costs.

David: *What about keeping tabs on system performance issues?*

Tina: That's important, along with capacity planning to be sure the system can handle future growth.

David: *What about system security?*

Tina: Good question. We'll look at physical security, network security, application security, file security, user security, and procedural security. We'll also look at backup and disaster recovery issues.

David: *Sounds like we'll be busy for quite a while.*

Tina: Well, that depends on the system itself and user expectations. Every system has a useful life, including this one. We'll try to get a good return on our investment, but we'll also watch for signs of obsolescence. Here are some tasks we can work on:

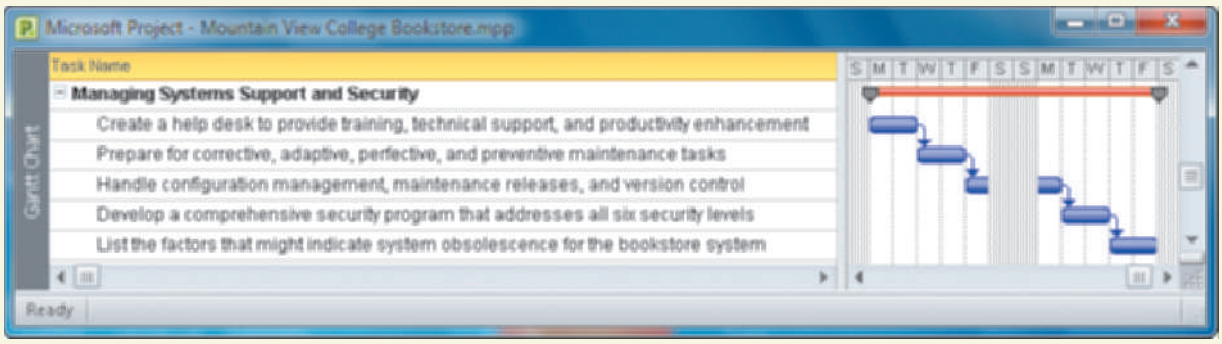


FIGURE 12-1 Typical systems support and security task list.

Overview

The systems support and security phase begins when a system becomes operational and continues until the system reaches the end of its useful life. Throughout the development process, the objective has been to create an information system that is efficient, easy to use, and affordable. After delivering the system, the IT team focuses on support and maintenance tasks.

The first part of this chapter covers four main topics. You will learn how to provide user support, maintain the system, manage the maintenance process, and handle system performance issues.

User Support

Companies provide user support in many forms, including user training and a help desk to provide technical support and assistance.

User Training

In Chapter 11, you learned about initial training that is performed when a new system is introduced. Additionally, new employees must be trained on the company's information systems. For example, a firm that produces electronic assemblies must train its new employees, as shown in Figure 12-2.

If significant changes take place in the existing system or if a new version is released, the IT department might develop a **user training package**. Depending on the nature of the changes, the package could include online support via e-mail, a special Web site, a revision to the user guide, a training manual supplement, or formal training sessions. Training users about system changes is similar to initial training. The main objective is to show users how the system can help them perform their jobs.

FIGURE 12-2 Whether a company is training manufacturing technicians, data entry personnel, or customer service representatives, employees need high-quality instruction to perform their jobs efficiently.

Help Desks

As systems and data structures become more complex, users need constant support and guidance. To make data more accessible and to empower users, many IT departments create help desks. A **help desk** is a centralized resource staffed by IT professionals who provide users with the support they need to do their jobs. A help desk has three main objectives: Show people how to use system resources more effectively, provide answers to technical or operational questions, and make users more productive by teaching them how to meet their own information needs. A help desk often is called an **information center** (**IC**) because it is the first place users turn when they need information or assistance.

A help desk does not replace traditional IT maintenance and support activities. Instead, help desks enhance productivity and improve utilization of a company's information resources.

Help desk representatives need strong interpersonal and technical skills plus a solid understanding of the business, because they interact with users in many departments.

ON THE WEB

To learn more about help desks, visit the Management Information Systems CourseMate Web site at **www.cengagebrain.com**, navigate to **On the Web Links** for this chapter, and locate the Help Desk link.

A help desk should document carefully all inquiries, support tasks, and activity levels. The information can identify trends and common problems and can help build a technical support knowledge base.

A help desk can boost its productivity by using **remote control software**, which allows IT staff to take over a user's workstation and provide support and troubleshooting. Popular examples of remote control software include Microsoft System Center Configuration Manager and DameWare Mini Remote Control.

During a typical day, the help desk staff member shown in Figure 12-3 might have to perform the following tasks:

FIGURE 12-3 A help desk, also called an information center (IC), provides guidance and assistance to system users. When a user contacts a help desk, the response should be prompt and effective.

- Show a user how to create a data query or report that displays specific business information
- Resolve network access or password problems
- Demonstrate an advanced feature of a system or a commercial package
- Help a user recover damaged data
- Offer tips for better operation
- Explain an undocumented software feature
- Show a user how to use Web conferencing
- Explain how to access the company's intranet or the Internet
- Assist a user in developing a simple database to track time spent on various projects
- Answer questions about software licensing and upgrades
- Provide information about system specifications and the cost of new hardware or software
- Recommend a system solution that integrates data from different locations to solve a business problem
- Provide hardware support by installing or reconfiguring devices such as scanners, printers, network cards, wireless devices, optical drives, backup devices, and multimedia systems
- Show users how to maintain data consistency and integrity among a desktop computer, a notebook computer, and a handheld computer or smart phone
- Troubleshoot software issues via remote control utilities

In addition to functioning as a valuable link between IT staff and users, the help desk is a central contact point for all IT maintenance activities. The help desk is where users report system problems, ask for maintenance, or submit new systems requests. A help desk can utilize many types of automated support, just as outside vendors do, including e-mail responses, on-demand fax capability, an online knowledge base, frequently asked questions (FAQs), discussion groups, bulletin boards, and automated voice mail. Many vendors now provide a live chat feature for online visitors. For example, as shown in Figure 12-4 on the next page, Dell invites its customers to chat interactively with a tech support person.

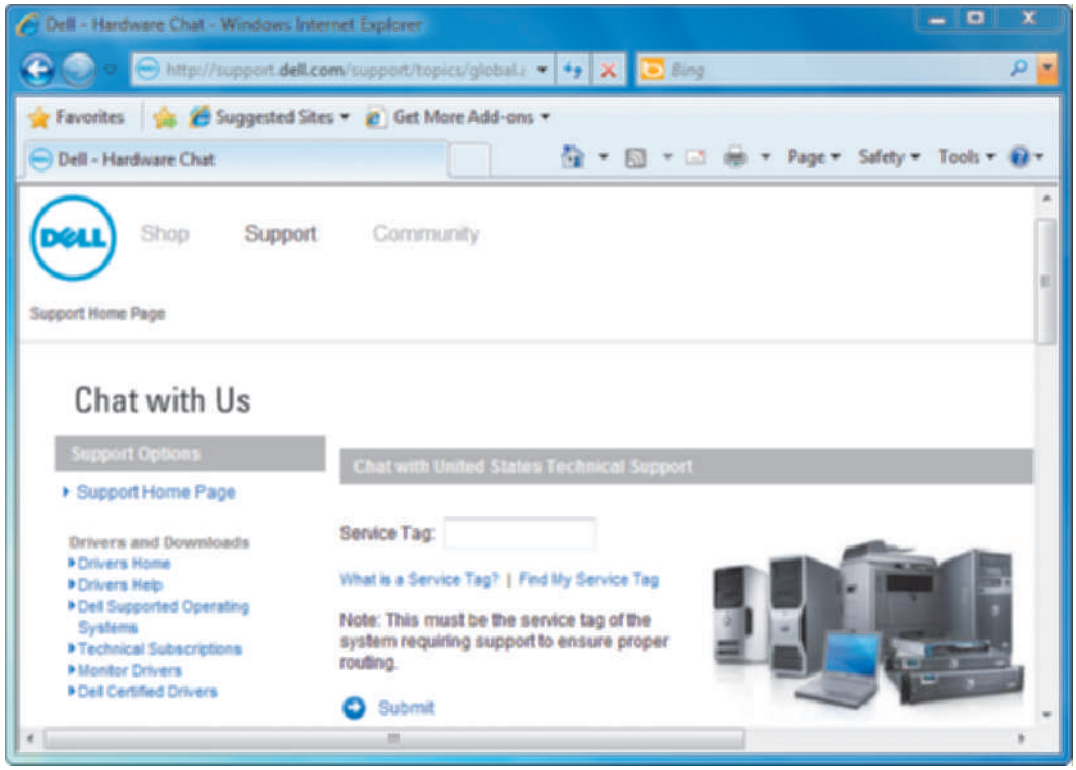


FIGURE 12-4 On its support site, Dell offers a variety of technical information and support options for customers.

Outsourcing Issues

As you learned in Chapter 7, many firms outsource various aspects of application development. This trend also includes outsourcing IT support and help desks. As with most business decisions, outsourcing has pros and cons. Typically, the main reason for outsourcing is cost reduction. Offshore call centers can trim expenses and free up valuable human resources for product development.

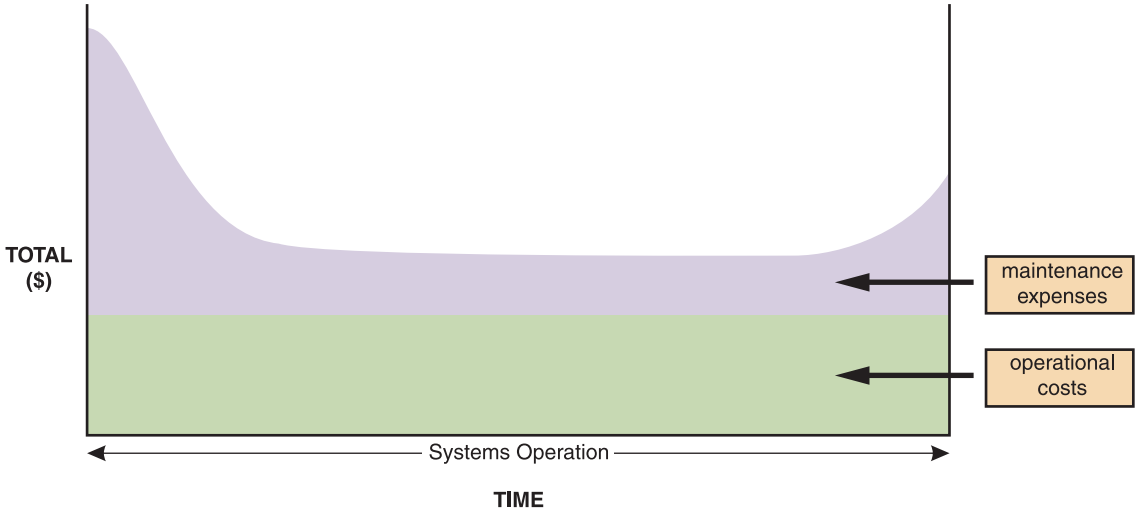
However, firms have learned that if tech support quality goes down, customers are likely to notice, and might shop elsewhere. Critical factors might include phone wait times, support staff performance, and online support tools. The real question is whether a company can achieve the desired savings without endangering its reputation and customer base. Risks can be limited, but only if a firm takes an active role in managing and monitoring support quality and consistency.

Maintenance Tasks

The systems support and security phase is an important component of TCO (total cost of ownership) because ongoing maintenance expenses can determine the economic life of a system.

Figure 12-5 shows a typical pattern of operational and maintenance expenses during the useful life of a system. **Operational costs** include items such as supplies, equipment rental, and software leases. Notice that the lower area shown in Figure 12-5 represents fixed operational expenses, while the upper area represents maintenance expenses.

Maintenance expenses vary significantly during the system's operational life and include spending to support maintenance activities. **Maintenance activities** include changing programs, procedures, or documentation to ensure correct system performance; adapting the system to changing requirements; and making the system operate more efficiently. Those needs are met by corrective, adaptive, perfective, and preventive maintenance.



TOOLKIT TIME

The Financial Analysis tools in Part C of the Systems Analyst's Toolkit can help you analyze and manage maintenance costs, and determine when a system is reaching the end of its useful life. To learn more about these tools, turn to Part C of the four-part Toolkit that follows Chapter 12.

FIGURE 12-5 The total cost of operating an information system includes operational and maintenance costs. Operational costs (green) are relatively constant, while maintenance expenses (purple) vary over time.

Although some overlap exists, four types of maintenance tasks can be identified, as shown by the examples in Figure 12-6. **Corrective maintenance** is performed to fix errors, **adaptive maintenance** adds new capability and enhancements, **perfective maintenance** improves efficiency, and **preventive maintenance** reduces the possibility of future system failure. Some analysts use the term *maintenance* to describe only corrective maintenance that fixes problems. It is helpful, however, to view the maintenance concept more broadly and identify the different types of tasks.

Maintenance expenses usually are high when a system is implemented because problems must be detected, investigated, and resolved by corrective maintenance. Once the system becomes stable, costs usually remain low and involve minor adaptive maintenance. Eventually, both adaptive and perfective maintenance activities increase in a dynamic business environment.

Near the end of a system's useful life, adaptive and corrective maintenance expenses increase rapidly, but perfective maintenance typically decreases when it becomes clear that the company plans to replace the system. Figure 12-7 on the next page shows the typical patterns for each of the four classifications of maintenance activities over a system's life span.

Examples of Maintenance Tasks

Corrective Maintenance
- Diagnose and fix logic errors
- Replace defective network cabling
- Restore proper configuration settings
- Debug program code
- Update drivers
- Install software patch

Adaptive Maintenance
- Add online capability
- Create new reports
- Add new data entry field to input screen
- Install links to Web site
- Create employee portal

Perfective Maintenance
- Install additional memory
- Write macros to handle repetitive tasks
- Compress system files
- Optimize user desktop settings
- Develop library for code reuse
- Install more powerful network server

Preventive Maintenance
- Install new antivirus software
- Develop standard backup schedule
- Implement regular defragmentation process
- Analyze problem report for patterns
- Tighten all cable connections

FIGURE 12-6 Corrective maintenance fixes errors and problems. Adaptive maintenance provides enhancements to a system. Perfective maintenance improves a system's efficiency, reliability, or maintainability. Preventive maintenance avoids future problems.

Corrective Maintenance

Corrective maintenance diagnoses and corrects errors in an operational system. To avoid introducing new problems, all maintenance work requires careful analysis before making changes. The best maintenance approach is a scaled-down version of the SDLC itself, where investigation, analysis, design, and testing are performed before implementing

	Immediately After Implementation	Early Operational Life	Middle Operational Life	Later Operational Life
Corrective Maintenance	High	Low	Low	High
Adaptive Maintenance (Minor Enhancements)	None	Medium	Medium	Medium
Adaptive Maintenance (Major Enhancements)	None	None	Medium to High	Medium to High
Perfective Maintenance	Low	Low to Medium	Medium	Low
Preventive Maintenance	Low	Medium	Medium	Low

FIGURE 12-7 Information systems maintenance depends on the type of maintenance and the age of the system.

any solution. Recall that in Chapter 11 you learned about the difference between a test environment and an operational environment. Any maintenance work that could affect the system must be performed first in the test environment, and then migrated to the operational system.

IT support staff respond to errors in various ways, depending on the nature and severity of the problem. Most organizations have standard procedures for minor errors, such as an incorrect report title or an improper format for a data element. In a typical procedure, a user submits a systems request that is evaluated, prioritized, and scheduled by the system administrator or the systems review committee. If the request is approved, the maintenance team designs, tests, documents, and implements a solution.

As you learned in Chapter 2, many organizations use a standard online form for systems requests. In smaller firms, the process might be an informal e-mail message. For more serious situations, such as incorrect report totals or inconsistent data, a user submits a systems request with supporting evidence. Those requests receive a high priority and a maintenance team begins work on the problem immediately.

The worst-case situation is a system failure. If an emergency occurs, the maintenance team bypasses the initial steps and tries to correct the problem immediately. This often requires a **patch**, which is a specially written software module that provides temporary repairs so operations can resume. Meanwhile, a written systems request is prepared by a user or a member of the IT department and added to the maintenance log. When the system is operational again, the maintenance team determines the cause, analyzes the problem, and designs a permanent solution. The IT response team updates the test data files, thoroughly tests the system, and prepares full documentation. Regardless of how the priorities are set, a standard ranking method can be helpful. For example, Figure 12-8 shows a three-level framework for IT support potential impact.

PRIORITY	IMPACT	TIMEFRAME
Level 1	Significant impact on IT operations, security, or business activity that requires immediate attention.	Implement patch as soon as possible.
Level 2	Some impact on IT operations, security, or business activity. Requires prompt attention, but operations can continue.	Patch as necessary and begin implementation prior to next release.
Level 3	Little or no impact on current IT operations, security, or business activity.	Implement in the next release.

FIGURE 12-8 This three-level ranking framework for IT support considers potential impact and response urgency.

The process of managing system support is described in more detail on page 578, including an overview of maintenance tasks and a procedural flowchart, which is shown in Figure 12-11 on page 581.

Adaptive Maintenance

Adaptive maintenance adds enhancements to an operational system and makes the system easier to use. An **enhancement** is a new feature or

capability. The need for adaptive maintenance usually arises from business environment changes such as new products or services, new manufacturing technology, or support for a new Web-based operation.

The procedure for minor adaptive maintenance is similar to routine corrective maintenance. A user submits a systems request that is evaluated and prioritized by the systems review committee. A maintenance team then analyzes, designs, tests, and implements the enhancement. Although the procedures for the two types of maintenance are alike, adaptive maintenance requires more IT department resources than minor corrective maintenance.

A major adaptive maintenance project is like a small-scale SDLC project because the development procedure is similar. Adaptive maintenance can be more difficult than new systems development because the enhancements must work within the constraints of an existing system.

Perfective Maintenance

Perfective maintenance involves changing an operational system to make it more efficient, reliable, or maintainable. Requests for corrective and adaptive maintenance normally come from users, while the IT department usually initiates perfective maintenance.

During system operation, changes in user activity or data patterns can cause a decline in efficiency, and perfective maintenance might be needed to restore performance. When users are concerned about performance, you should determine if a perfective maintenance project could improve response time and system efficiency.

Perfective maintenance also can improve system reliability. For example, input problems might cause a program to terminate abnormally. By modifying the data entry process, you can highlight errors and notify the users that they must enter proper data. When a system is easier to maintain, support is less costly and less risky. In many cases, you can simplify a complex program to improve maintainability.

In many organizations, perfective maintenance is not performed frequently enough. Companies with limited resources often consider new systems development, adaptive maintenance, and corrective maintenance more important than perfective maintenance. Managers and users constantly request new projects, so few resources are available for perfective maintenance work. As a practical matter, perfective maintenance can be performed as part of another project. For example, if a new function must be added to a program, you can include perfective maintenance in the adaptive maintenance project.

Perfective maintenance usually is cost effective during the middle of the system's operational life. Early in systems operation, perfective maintenance usually is not needed. Later, perfective maintenance might be necessary, but have a high cost. Perfective maintenance is less important if the company plans to discontinue the system.

When performing perfective maintenance, analysts often use a technique called software reengineering. **Software reengineering** uses analytical techniques to identify potential quality and performance improvements in an information system. In that sense, software reengineering is similar to business process reengineering, which seeks to simplify operations, reduce costs, and improve quality — as you learned in Chapter 1.

Programs that need a large number of maintenance changes usually are good candidates for reengineering. The more a program changes, the more likely it is to become inefficient and difficult to maintain. Detailed records of maintenance work can identify systems with a history of frequent corrective, adaptive, or perfective maintenance.

ON THE WEB

To learn more about software reengineering, visit the Management Information Systems CourseMate Web site at **www.cengagebrain.com**, navigate to **On the Web Links** for this chapter, and locate the Software Reengineering link.

Preventive Maintenance

To avoid problems, preventive maintenance requires analysis of areas where trouble is likely to occur. Like perfective maintenance, the IT department normally initiates preventive

FIGURE 12-9 Regardless of the type of system, high-quality maintenance must be performed by trained professionals.

maintenance. Preventive maintenance often results in increased user satisfaction, decreased downtime, and reduced TCO. Preventive maintenance competes for IT resources along with other projects, and sometimes does not receive the high priority that it deserves.

Regardless of the type of maintenance, computer systems must be supported by trained professionals, just as the aircraft shown in Figure 12-9 must be serviced by skilled technicians. In both cases, the quality of the maintenance will directly affect the organization's success.

CASE IN POINT 12.1: OUTBACK OUTSOURCING, INC.

You are a systems analyst at Outback Outsourcing, a firm that handles payroll processing for many large companies. Outback Outsourcing uses a combination of payroll package programs and in-house developed software to deliver custom-made payroll solutions for its clients. Lately, users have flooded you with requests for more new features and Web-based capability to meet customer expectations. Your boss, the IT manager, comes to you with a question. She wants to know when to stop trying to enhance the old software and develop a totally new version better suited to the new marketplace. How would you answer her?

MAINTENANCE MANAGEMENT

System maintenance requires effective management, quality assurance, and cost control. To achieve these goals, companies use various strategies, such as a maintenance team, a maintenance management program, a configuration management process, and a maintenance release procedure. In addition, firms use version control and baselines to track system releases and analyze the system's life cycle. These concepts are described in the following sections.

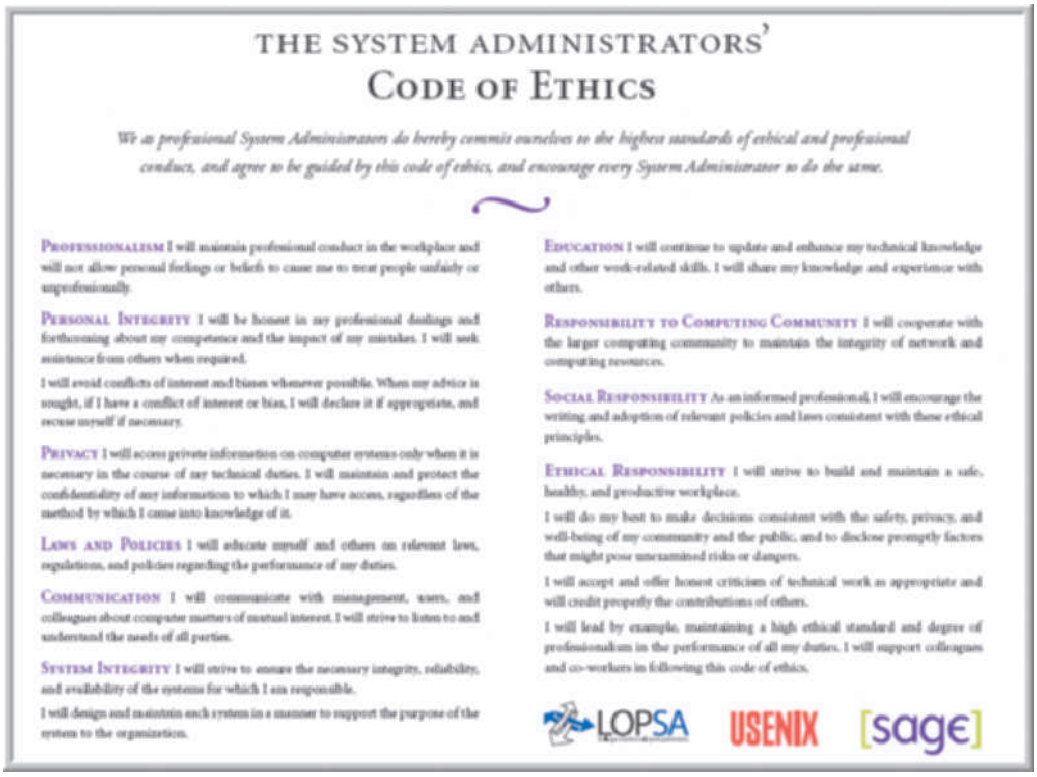
The Maintenance Team

A **maintenance team** includes a system administrator and one or more systems analysts and programmers. The system administrator should have solid technical expertise, and experience in troubleshooting and configuring operating systems and hardware. Successful analysts need a strong IT background, solid analytical abilities, good communication skills, and an overall understanding of business operations.

SYSTEM ADMINISTRATOR A **system administrator** manages computer and network systems. A system administrator must work well under pressure, have good organizational and communication skills, and be able to understand and resolve complex issues in a limited time frame. In most organizations, a system administrator has primary responsibility for the operation, configuration, and security of one or more systems. The system

administrator is responsible for routine maintenance, and usually is authorized to take preventive action to avoid an immediate emergency, such as a server crash, network outage, security incident, or hardware failure.

Systems administration is a vital function, and various professional associations, such as SAGE, which is shown in Figure 12-10, offer a wide variety of technical information and support for system administrators. Notice that SAGE members subscribe to a code of ethics that includes professionalism, integrity, privacy, and social responsibility, among other topics.



THE SYSTEM ADMINISTRATORS'
CODE OF ETHICS

We as professional System Administrators do hereby commit ourselves to the highest standards of ethical and professional conduct, and agree to be guided by this code of ethics, and encourage every System Administrator to do the same.

PROFESSIONALISM I will maintain professional conduct in the workplace and will not allow personal feelings or beliefs to cause me to treat people unfairly or unprofessionally.

PERSONAL INTEGRITY I will be honest in my professional dealings and forthcoming about my competence and the impact of my mistakes. I will seek assistance from others when required.

I will avoid conflicts of interest and biases whenever possible. When my advice is sought, if I have a conflict of interest or bias, I will declare it if appropriate, and recuse myself if necessary.

PRIVACY I will access private information on computer systems only when it is necessary in the course of my technical duties. I will maintain and protect the confidentiality of any information to which I may have access, regardless of the method by which I came into knowledge of it.

LAWS AND POLICIES I will educate myself and others on relevant laws, regulations, and policies regarding the performance of my duties.

COMMUNICATION I will communicate with management, users, and colleagues about computer matters of mutual interest. I will strive to listen to and understand the needs of all parties.

SYSTEM INTEGRITY I will strive to ensure the necessary integrity, reliability, and availability of the systems for which I am responsible.

I will design and maintain each system in a manner to support the purpose of the system to the organization.

EDUCATION I will continue to update and enhance my technical knowledge and other work-related skills. I will share my knowledge and experience with others.

RESPONSIBILITY TO COMPUTING COMMUNITY I will cooperate with the larger computing community to maintain the integrity of network and computing resources.

SOCIAL RESPONSIBILITY As an informed professional, I will encourage the writing and adoption of relevant policies and laws consistent with these ethical principles.

ETHICAL RESPONSIBILITY I will strive to build and maintain a safe, healthy, and productive workplace.

I will do my best to make decisions consistent with the safety, privacy, and well-being of my community and the public, and to disclose promptly factors that might pose unexamined risks or dangers.

I will accept and offer honest criticism of technical work as appropriate and will credit properly the contributions of others.

I will lead by example, maintaining a high ethical standard and degree of professionalism in the performance of all my duties. I will support colleagues and co-workers in following this code of ethics.

LOPSA USENIX [sage]

FIGURE 12-10 SAGE seeks to establish standards of professional excellence, improve the technical skills of its members, and promote a comprehensive code of ethics.

SYSTEMS ANALYSTS Systems analysts assigned to a maintenance team are like skilled detectives who investigate and rapidly locate the source of a problem by using analysis and synthesis skills. *Analysis* means examining the whole in order to learn about the individual elements, while *synthesis* involves studying the parts to understand the overall system. In addition to strong technical skills, an analyst must have a solid grasp of business operations and functions. Analysts also need effective interpersonal and communications skills and they must be creative, energetic, and eager for new knowledge.

PROGRAMMERS In a small organization, a programmer might be expected to handle a wide variety of tasks, but in larger firms, programming work tends to be more specialized. For example, typical job titles include an **applications programmer**, who works on new systems development and maintenance; a **systems programmer**, who concentrates on operating system software and utilities; and a **database programmer**, who focuses on creating and supporting large-scale database systems. Many IT departments also use a job title of **programmer/analyst** to designate positions that require a combination of systems analysis and programming skills.

ORGANIZATIONAL ISSUES IT managers often divide systems analysts and programmers into two groups: One group performs new system development, and the other group

handles maintenance. Some organizations use a more flexible approach and assign IT staff members to various projects as they occur. By integrating development and support work, the people developing the system assume responsibility for maintaining it. Because the team is familiar with the project, additional training or expense is unnecessary, and members are likely to have a sense of ownership from the onset.

Unfortunately, many analysts feel that maintenance is less interesting and creative than developing new systems. In addition, an analyst might find it challenging to troubleshoot and support someone else's work that might have been poorly documented and organized.

Some organizations that have separate maintenance and new systems groups rotate people from one assignment to the other. When analysts learn different skills, the organization is more versatile and people can shift to meet changing business needs. For instance, systems analysts working on maintenance projects learn why it is important to design easily maintainable systems. Similarly, analysts working on new systems get a better appreciation of the development process and the design compromises necessary to meet business objectives.

One disadvantage of rotation is that it increases overhead because time is lost when people move from one job to another. When systems analysts constantly shift between maintenance and new development, they have less opportunity to become highly skilled at any one job.

Newly hired and recently promoted IT staff members often are assigned to maintenance projects because their managers believe that the opportunity to study existing systems and documentation is a valuable experience. In addition, the mini-SDLC used in many adaptive maintenance projects is good training for the full-scale systems development life cycle. For a new systems analyst, however, maintenance work might be more difficult than systems development, and it might make sense to assign a new person to a development team where experienced analysts are available to provide training and guidance.

CASE IN POINT 12.2: BRIGHTSIDE INSURANCE, INC.

As IT manager at Brightside Insurance Company, you organized your IT staff into two separate groups — one team for maintenance projects and the other team for new systems work. That arrangement worked well in your last position at another company. Brightside, however, previously made systems assignments with no particular pattern.

At first, the systems analysts in your group did not comment about the team approach. Now, several of your best analysts have indicated that they enjoyed the mix of work and would not want to be assigned to a maintenance team. Before a problem develops, you have decided to rethink your organizational strategy. Should you go back to the way things were done previously at Brightside? Why or why not? Do other options exist? What are they?

Maintenance Requests

Typically, maintenance requests involve a series of steps, as shown in Figure 12-11. After a user submits a request, a system administrator determines whether immediate action is needed and whether the request is under a prescribed cost limit. In nonemergency requests that exceed the cost limit, a systems review committee assesses the request and either approves it, with a priority, or rejects it. The system administrator notifies affected users of the outcome.

Users submit most requests for corrective and adaptive maintenance when the system is not performing properly, or if they want new features. IT staff members usually initiate requests for perfective and preventive maintenance. To keep a complete maintenance log, all work must be covered by a specific request that users submit in writing or by e-mail.

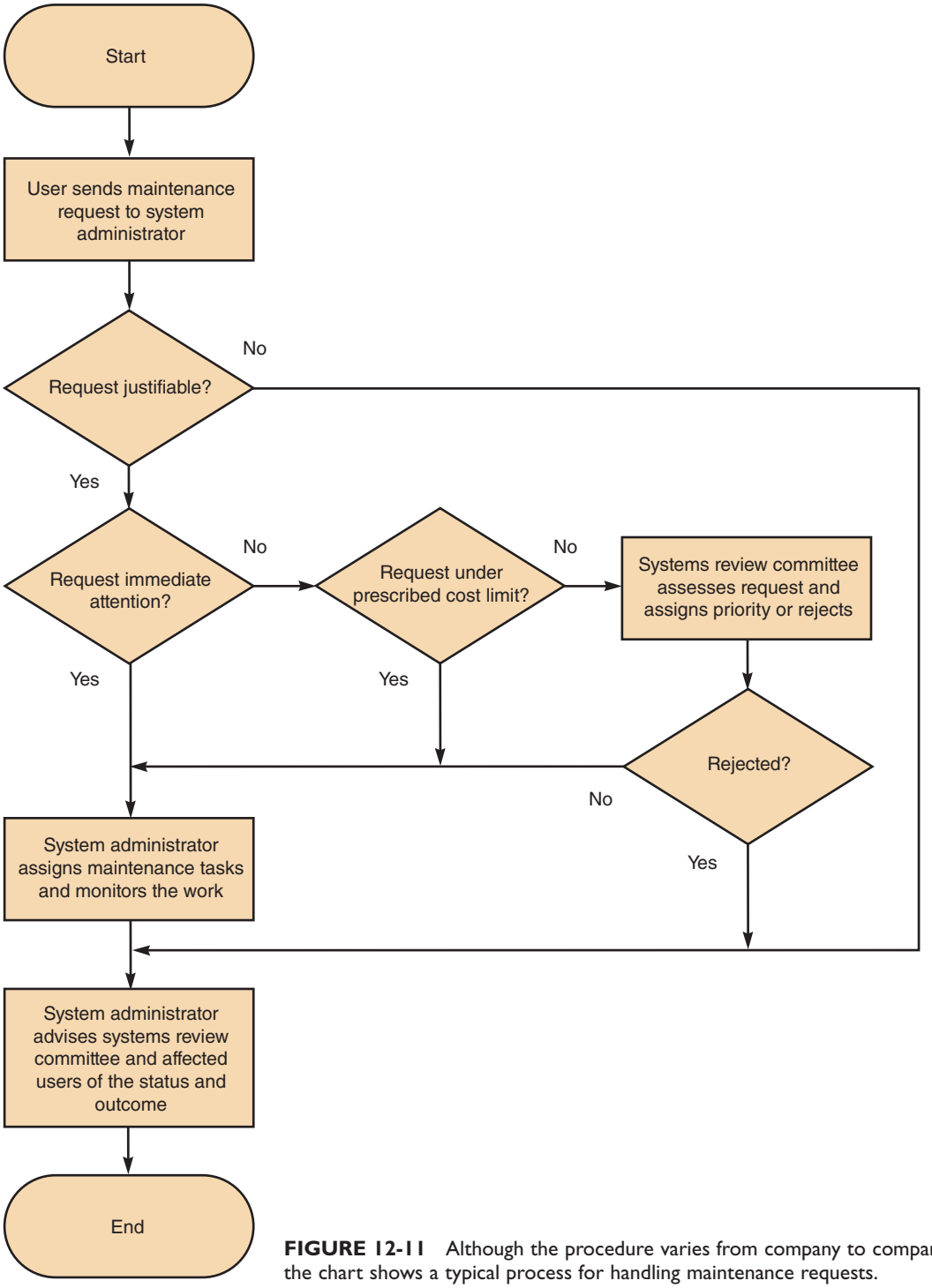


FIGURE 12-11 Although the procedure varies from company to company, the chart shows a typical process for handling maintenance requests.

INITIAL DETERMINATION When a user submits a maintenance request, the system administrator makes an initial determination. If the request is justifiable and involves a severe problem that requires immediate attention, the system administrator takes action at once. In justifiable, but noncritical, situations, the administrator determines whether the request can be performed within a preauthorized cost level. If so, he or she assigns the maintenance tasks and monitors the work.

THE SYSTEMS REVIEW COMMITTEE When a request exceeds a predetermined cost level or involves a major configuration change, the systems review committee either approves it and assigns a priority, or rejects it.

TASK COMPLETION The system administrator usually is responsible for assigning maintenance tasks to individuals or to a maintenance team. Depending on the situation and the company's policy, the system administrator might consider rotating assignments among the IT staff or limiting maintenance tasks to certain individuals or teams, as explained in the previous section.

USER NOTIFICATION Users who initiate maintenance requests expect a prompt response, especially if the situation directly affects their work. Even when corrective action cannot occur immediately, users appreciate feedback from the system administrator and should be kept informed of any decisions or actions that could affect them.

Establishing Priorities

ON THE WEB

To learn more about configuration management, visit the Management Information Systems CourseMate Web site at **www.cengagebrain.com**, navigate to **On the Web Links** for this chapter, and locate the Configuration Management link.

In many companies, the systems review committee separates maintenance and new development requests when setting priorities. In other organizations, all requests are considered together, and the most important project gets top priority, whether it is maintenance or new development.

Some IT managers believe that evaluating all projects together leads to the best possible decisions because maintenance and new development require similar IT department resources. In IT departments where maintenance and new development are not integrated, it might be better to evaluate requests separately. Another advantage of a separate approach is that maintenance is more likely to receive a proportional share of IT department resources.

The most important objective is to have a procedure that balances new development and necessary maintenance work to provide the best support for business requirements and priorities.

FIGURE 12-12 CM Crossroads provides a source of information and resources for configuration management professionals.

Configuration Management

Configuration management (CM), sometimes referred to as **change control** (CC), is a process for controlling changes in system requirements during software development. Configuration management also is an important tool for managing system changes and costs after a system becomes operational. Most companies establish a specific process that describes how system changes must be requested and documented.

As enterprise-wide information systems grow more complex, configuration management becomes critical. Industry standards have emerged, and many vendors offer configuration management software and techniques, as shown in Figure 12-12.

CM is especially important if a system has multiple versions that run in different hardware and software environments. Configuration management also helps to organize and handle documentation. An operational system has extensive documentation that covers development, modification, and maintenance for all versions of the installed system. Most documentation material, including the initial systems request, project management data, end-of-phase reports, data dictionary, and the IT operations and user manuals, is stored in the IT department.

Keeping track of all documentation and ensuring that updates are distributed properly are important aspects of configuration management.

Maintenance Releases

Keeping track of maintenance changes and updates can be difficult, especially for a complex system. When a **maintenance release methodology** is used, all noncritical changes are held until they can be implemented at the same time. Each change is documented and installed as a new version of the system called a **maintenance release**.

For an in-house developed system, the time between releases usually depends on the level of maintenance activity. A new release to correct a critical error, however, might be implemented immediately rather than saved for the next scheduled release.

When a release method is used, a numbering pattern distinguishes the different releases. In a typical system, the initial version of the system is 1.0, and the release that includes the first set of maintenance changes is version 1.1. A change, for example, from version 1.4 to 1.5 indicates relatively minor enhancements, while whole number changes, such as from version 1.0 to 2.0 or from version 3.4 to 4.0, indicate a significant upgrade.

The release methodology offers several advantages, especially if two teams perform maintenance work on the same system. When a release methodology is used, all changes are tested together before a new system version is released. This approach results in fewer versions, less expense, and less interruption for users. Using a release methodology also reduces the documentation burden, because all changes are coordinated and become effective simultaneously.

A release methodology also has some potential disadvantages. Users expect a rapid response to their problems and requests, but with a release methodology, new features or upgrades are available less often. Even when changes would improve system efficiency or user productivity, the potential savings must wait until the next release, which might increase operational costs.

Commercial software suppliers also provide maintenance releases, often called **service packs**, as shown in Figure 12-13. As Microsoft explains, a service pack contains all the fixes and enhancements that have been made available since the last program version or service pack.

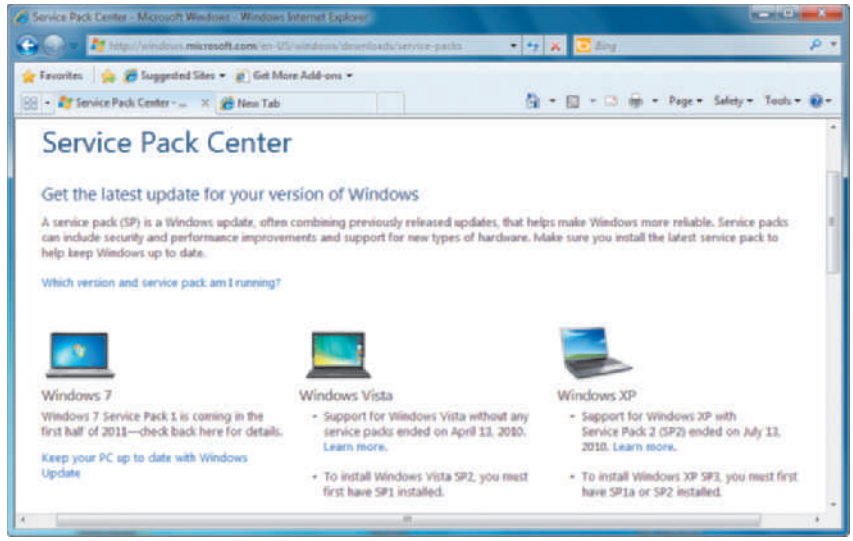


FIGURE 12-13 A Microsoft service pack provides access to up-to-date drivers, tools, security patches, and customer-requested product changes.

Version Control

Version control is the process of tracking system releases, or versions. When a new version of a system is installed, the prior release is **archived**, or stored. If a new version causes a system to fail, a company can reinstall the prior version to restore operations. In addition to tracking system versions, the IT staff is responsible for configuring systems that have several modules at various release stages. For example, an accounting system might have a one-year old accounts receivable module that must interface with a brand-new payroll module.

As systems grow more complex, version control becomes an essential part of system documentation. In addition to in-house version control procedures, companies can purchase software from vendors such as Serena, as shown in Figure 12-14 on the next page.

ON THE WEB

To learn more about version control, visit the Management Information Systems CourseMate Web site at **www.cengagebrain.com**, navigate to **On the Web Links** for this chapter, and locate the Version Control link.

FIGURE 12-14 Serena offers software called PVCS Version Manager that developers can use to manage projects.

Baselines

A **baseline** is a formal reference point that measures system characteristics at a specific time. Systems analysts use baselines as yardsticks to document features and performance during the systems development process. The three types of baselines are functional, allocated, and product.

The **functional baseline** is the configuration of the system documented at the beginning of the project. It consists of all the necessary system requirements and design constraints.

The **allocated baseline** documents the system at the end of the design phase and identifies any changes since the functional baseline. The allocated baseline includes testing and verification of all system requirements and features.

The **product baseline** describes the system at the beginning of system operation. The product baseline incorporates any changes made since the allocated baseline and includes the results of performance and acceptance tests for the operational system.

System Performance Management

Years ago, when most firms used a central computer for processing data, it was relatively simple to manage a system and measure its efficiency. Today, companies use complex networks and client/server systems to support business needs. A user at a client

workstation often interacts with an information system that depends on other clients, servers, networks, and data located throughout the company. Rather than a single computer, it is the integration of all those components that determines the system's capability and performance. In many situations, IT managers use automated software and CASE tools to manage complex systems.

To ensure satisfactory support for business operations, the IT department must manage system faults and interruptions, measure system performance and workload, and anticipate future needs. The following sections discuss these topics.

Fault Management

No matter how well it is designed, every system will experience some problems, such as hardware failures, software errors, user mistakes, and power outages. A system administrator must detect and resolve operational problems as quickly as possible. That task, often called **fault management**, includes monitoring the system for signs of trouble, logging all system failures, diagnosing the problem, and applying corrective action.

The more complex the system, the more difficult it can be to analyze symptoms and isolate a cause. In addition to addressing the immediate problem, it is important to evaluate performance patterns and trends. Windows 7 and Vista include a built-in fault management feature called Resource Monitor, which is shown in Figure 12-15. Resource Monitor can evaluate CPU, memory, disk, and network activity in real time, and save the data in a log file. In addition to automated notification, fault management software can identify underlying causes, speed up response time, and reduce service outages.

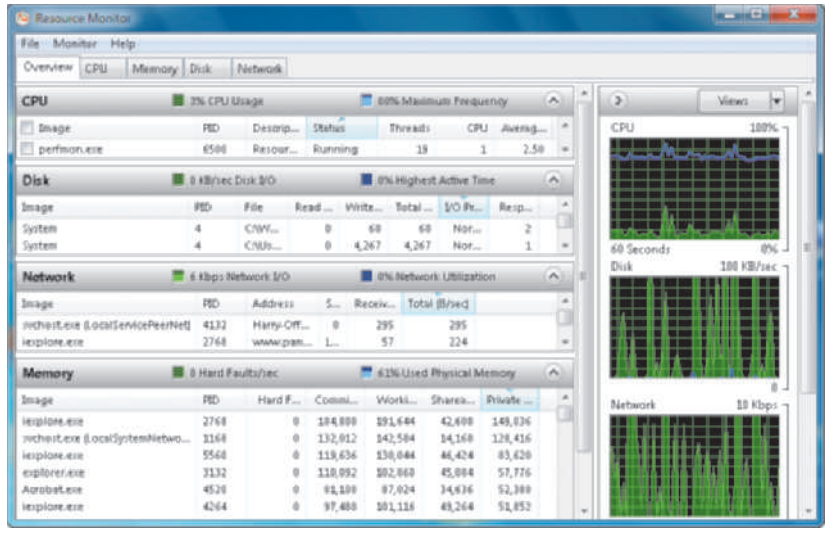


FIGURE 12-15 Windows Resource Monitor displays CPU, memory, disk, and network activity in real time.

Although system administrators must deal with system faults and interruptions as they arise, the best strategy is to prevent problems by monitoring system performance and workload.

Performance and Workload Measurement

In e-business, slow performance can be as devastating as no performance at all. Network delays and application bottlenecks affect customer satisfaction, user productivity, and business results. In fact, many IT managers believe that network delays do more damage than actual stoppages, because they occur more frequently and are difficult to predict, detect, and prevent. Customers expect reliable, fast response 24 hours a day, seven days a week. To support that level of service, companies use performance management software, such as Cisco Network Application Performance Analysis (NAPA), which is shown in Figure 12-16 on the next page.

To measure system performance, many firms use **benchmark testing**, which uses a set of standard tests to evaluate system performance and capacity. In addition to benchmark testing, performance measurements, called **metrics**, can monitor the number of transactions processed in a given time period, the number of records accessed, and the volume of online data. Network performance metrics include response time, bandwidth, throughput, and turnaround time, among others.

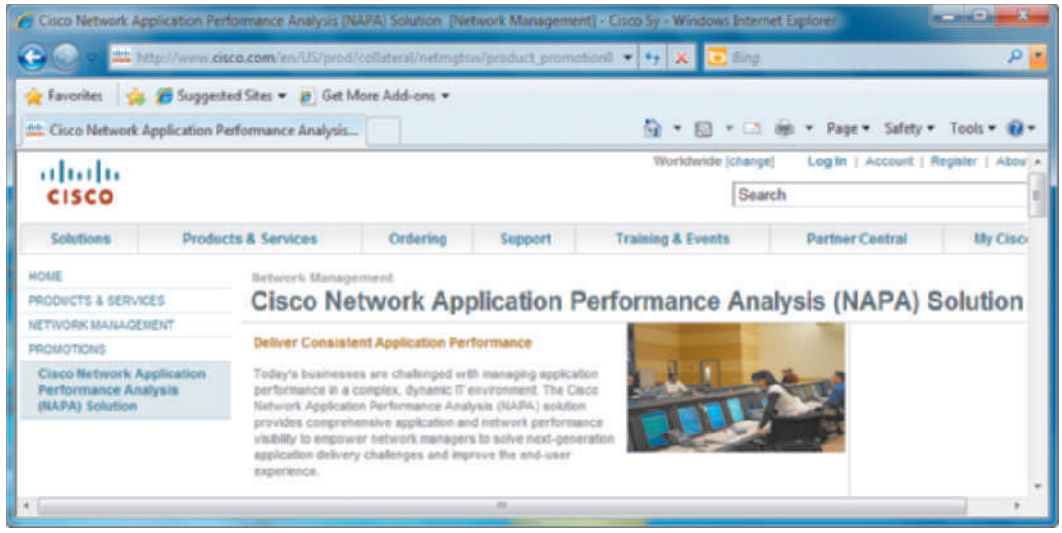


FIGURE 12-16 Network managers can use Cisco's NAPA to monitor performance and improve the end-user experience.

RESPONSE TIME **Response time** is the overall time between a request for system activity and the delivery of the response. In the typical online environment, response time is measured from the instant the user presses the ENTER key or clicks a mouse button until the requested screen display appears or printed output is ready. Response time is affected by the system design, capabilities, and processing methods. If the request involves network or Internet access, response time is affected by data communication factors.

Online users expect an immediate response, and they are frustrated by any apparent lag or delay. Of all performance measurements, response time is the one that users notice and complain about most.

BANDWIDTH AND THROUGHPUT Bandwidth and throughput are closely related terms, and many analysts use them interchangeably. **Bandwidth** describes the amount of data that the system can transfer in a fixed time period. Bandwidth requirements are expressed in bits per second. Depending on the system, you might measure bandwidth in **Kbps** (**kilobits per second**), **Mbps** (**megabits per second**), or **Gbps** (**gigabits per second**). Analyzing bandwidth is similar to forecasting the hourly number of vehicles that will use a highway in order to determine the number of lanes required.

Throughput measures actual system performance under specific circumstances and is affected by network loads and hardware efficiency. Throughput, like bandwidth, is expressed as a data transfer rate, such as Kbps, Mbps, or Gbps. Just as traffic jams delay highway traffic, throughput limitations can slow system performance and response time. That is especially true with graphics-intensive systems and Web-based systems that are subject to Internet-related conditions.

In addition to the performance metrics explained in the previous section, system administrators measure many other performance characteristics. Although no standard set of metrics exists, several typical examples are:

- Arrivals — The number of items that appear on a device during a given observation time.
- Busy — The time that a given resource is unavailable.
- Completions — The number of arrivals that are processed during a given observation period.
- Queue length — The number of requests pending for a service.
- Service time — The time it takes to process a given task once it reaches the front of the queue.

- Think time — The time it takes an application user to issue another request.
- Utilization — How much of a given resource was required to complete a task.
- Wait time — The time that requests must wait for a resource to become available.

The Computer Measurement Group (CMG®) maintains a site, shown in Figure 12-17, that provides support and assistance for IT professionals concerned with performance evaluation and capacity planning.

FIGURE 12-17 The Computer Measurement Group is a nonprofit organization that primarily is concerned with performance evaluation and capacity management.

TURNAROUND TIME **Turnaround time** applies to centralized batch processing operations, such as customer billing or credit card statement processing. Turnaround time measures the time between submitting a request for information and the fulfillment of the request. Turnaround time also can be used to measure the quality of IT support or services by measuring the time from a user request for help to the resolution of the problem.

The IT department often measures response time, bandwidth, throughput, and turnaround time to evaluate system performance both before and after changes to the system or business information requirements. Performance data also is used for cost-benefit analyses of proposed maintenance and to evaluate systems that are nearing the end of their economically useful lives.

Finally, management uses current performance and workload data as input for the capacity planning process.

Capacity Planning

Capacity planning is a process that monitors current activity and performance levels, anticipates future activity, and forecasts the resources needed to provide desired levels of service.

As the first step in capacity planning, you develop a current model based on the system's present workload and performance specifications. Then you project demand and user requirements over a one- to three-year time period and analyze the model to see what is needed to maintain satisfactory performance and meet requirements. To assist you in the process, you can use a technique called what-if analysis.

What-if analysis allows you to vary one or more elements in a model in order to measure the effect on other elements. For example, you might use what-if analysis to answer questions such as: How will response time be affected if we add more PC workstations to the network? Will our client/server system be able to handle the growth in sales from the new Web site? What will be the effect on server throughput if we add more memory?

Powerful spreadsheet tools also can assist you in performing what-if analysis. For example, Microsoft Excel contains a feature called Goal Seek that determines what changes are necessary in one value to produce a specific result for another value. In the example shown in Figure 12-18 on the next page, a capacity planning worksheet indicates that the system can handle 3,840 Web-based orders per day, at 22.5 seconds each. The user wants to know the effect on processing time if the number of transactions increases to 9,000. As the Goal Seek solution in the bottom figure shows, order processing will have to be performed in 9.6 seconds to achieve that goal.

ON THE WEB

To learn more about capacity planning, visit the Management Information Systems CourseMate Web site at **www.cengagebrain.com,** navigate to **On the Web Links** for this chapter, and locate the Capacity Planning link.

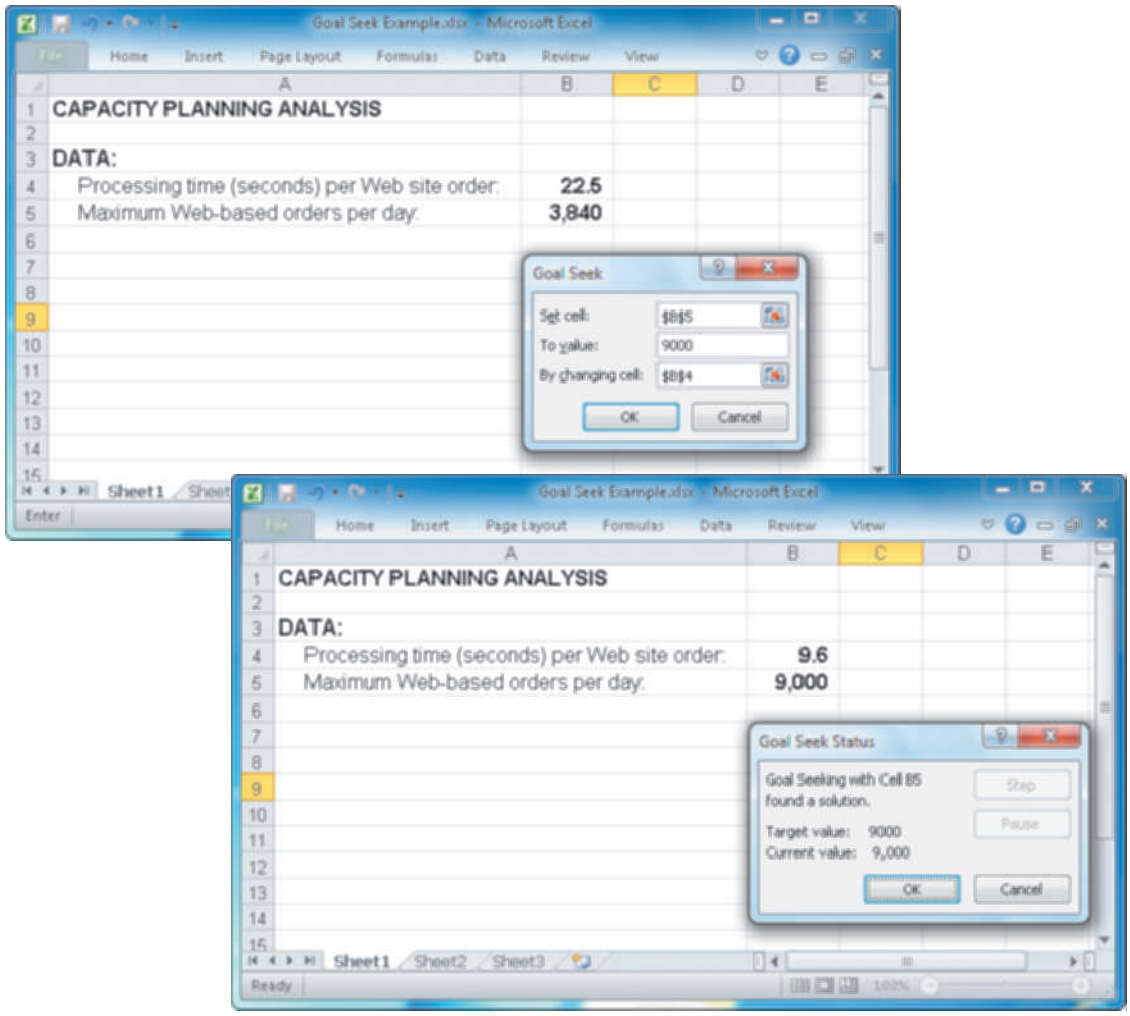


FIGURE 12-18 Microsoft Excel provides a Goal Seek feature that permits what-if analysis.

When you plan capacity, you need detailed information about the number of transactions; the daily, weekly, or monthly transaction patterns; the number of queries; and the number, type, and size of all generated reports. If the system involves a LAN, you need to estimate network traffic levels to determine whether or not the existing hardware and software can handle the load. If the system uses a client/server design, you need to examine performance and connectivity specifications for each platform.

Most important, you need an accurate forecast of future business activities. If new business functions or requirements are predicted, you should develop contingency plans based on input from users and management. The main objective is to ensure that the system meets all future demands and provides effective support for business operations. Some firms handle their own capacity planning, while others purchase software and services from companies such as Teamquest, shown in Figure 12-19.

TOOLKIT TIME

The CASE tools in Part B of the Systems Analyst's Toolkit can help you document business functions and processes, develop graphical models, and provide an overall framework for information system development. To learn more about these tools, turn to Part B of the four-part Toolkit that follows Chapter 12.

System Maintenance Tools

You can use automated tools that provide valuable assistance during the operation and support phase. Many CASE tools include system evaluation and maintenance features, including the following examples:

- Performance monitor that provides data on program execution times
- Program analyzer that scans source code, provides data element cross-reference information, and helps evaluate the impact of a program change

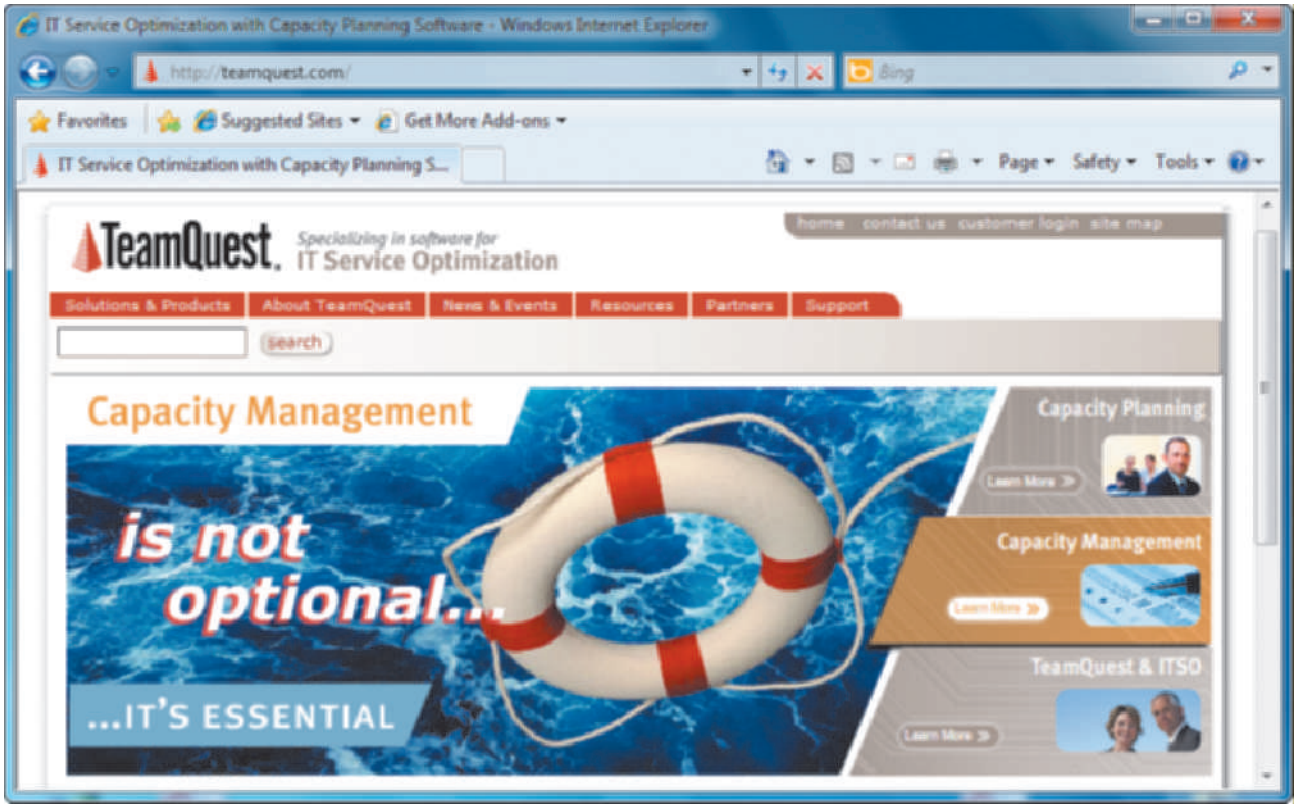


FIGURE 12-19 TeamQuest is an example of a firm that offers capacity planning software and services.

- Interactive debugging analyzer that locates the source of a programming error
- Reengineering tools
- Automated documentation
- Network activity monitor
- Workload forecasting tool

In addition to CASE tools, you also can use spreadsheet and presentation software to calculate trends, perform what-if analyses, and create attractive charts and graphs to display the results. Information technology planning is an essential part of the business planning process, and you probably will deliver presentations to management. You can review Part A of the Systems Analyst's Toolkit for more information on using spreadsheet and presentation software to help you communicate effectively.

System Security Overview

Security is a vital part of every information system. **Security** protects the system, and keeps it safe, free from danger, and reliable. In a global environment that includes many types of threats and attacks, security is more important than ever. This section includes a discussion of system security concepts, risk management, and common attacks against the system.

System Security Concepts

The **CIA triangle** in Figure 12-20 shows the three main elements of system security: confidentiality, integrity, and availability. **Confidentiality** protects information from unauthorized disclosure and safeguards privacy.

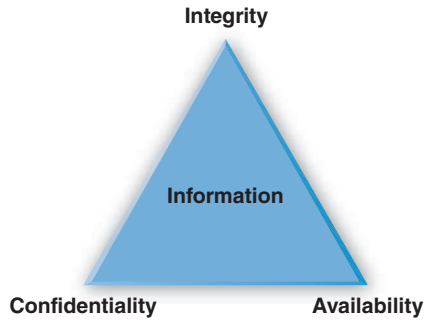


FIGURE 12-20 System security must provide information confidentiality, integrity, and availability.

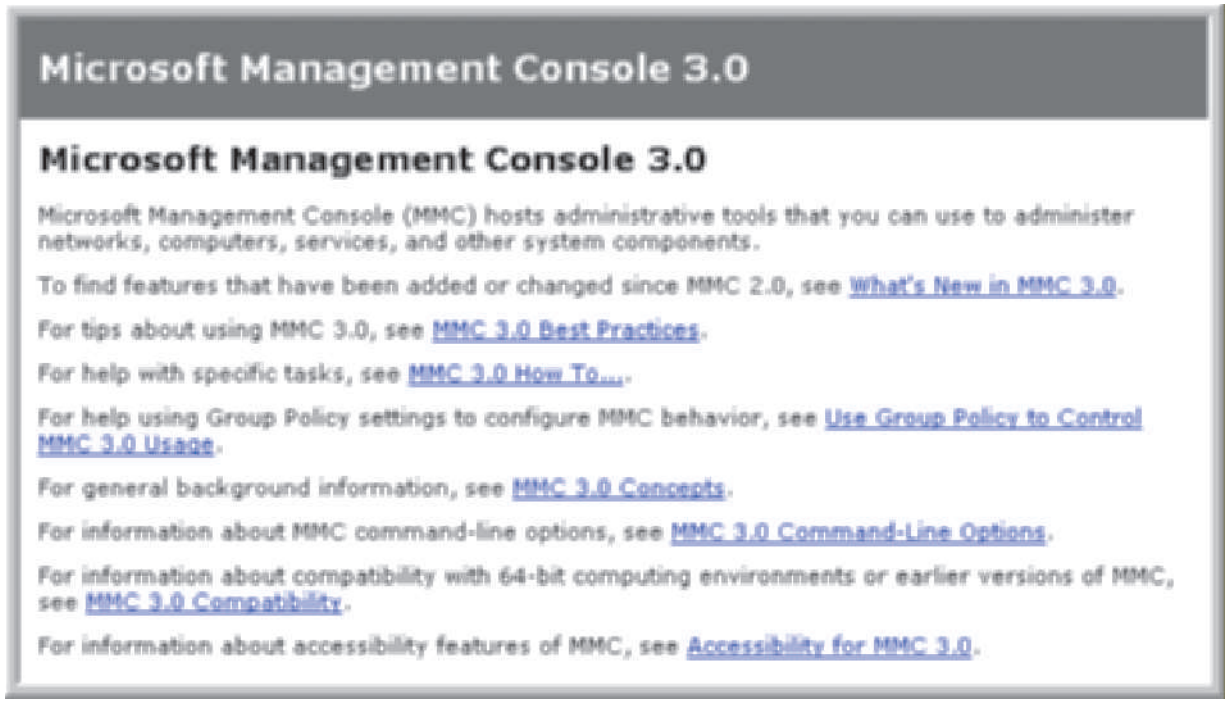


FIGURE 12-21 The Microsoft Management Console (MMC) includes built-in security tools, such as password and lockout policies, audit policies, user rights, and security configurations, among others.

Integrity prevents unauthorized users from creating, modifying, or deleting information. **Availability** ensures that authorized users have timely and reliable access to necessary information. The first step in managing IT security is to develop a **security policy** based on these three elements. Although it is beyond the scope of this chapter, the **Microsoft Management Console** (MMC) shown in Figure 12-21 is a portal to a broad array of built-in security tools and techniques.

FIGURE 12-22 Risk management requires continuous risk identification, assessment, and control.

Risk Management

In the real world, *absolute* security is not a realistic goal. Instead, managers must balance the value of the assets being protected, potential risks to the organization, and security costs. For example, it might not be worth installing an expensive video camera monitoring system to protect an empty warehouse. To achieve the best results, most firms use a **risk management** approach that involves constant attention to three interactive tasks: risk identification, risk assessment, and risk control, as shown in Figure 12-22.

Risk identification analyzes the organization's assets, threats, and vulnerabilities. **Risk assessment** measures risk likelihood and impact. **Risk control** develops safeguards that reduce risks and their impact.

RISK IDENTIFICATION The first step in risk identification is to list and classify business assets. An **asset** might include company hardware, software, data, networks, people, or procedures. For each asset, a risk manager rates the impact of an attack and analyzes possible threats. A **threat** is an internal or external entity that could endanger an asset. For example, threat categories might include natural disasters, software attacks, or theft, as shown in Figure 12-23.

Threat Categories and Examples

THREAT	CATEGORY
Extortion	Hacker steals trade secrets and threatens to release them if not paid.
Hardware and software failures	Router stops functioning, or software causes the application server to crash.
Human error or failure	Employee accidentally deletes a file.
Natural disasters	Flood destroys company building and networked systems.
Service failure	Electricity is disrupted and brings the entire system down for hours.
Software attack	A group plants destructive software, a virus, or a worm into a company network.
Technical obsolescence	Outdated software is slow, difficult to use, and vulnerable to attacks.
Theft of physical or intellectual property	Physical server is stolen, intellectual property is stolen or used without permission; may be physical or electronic.
Trespass and espionage	Employee enters unlocked server room and views the payroll data on a forbidden system.
Vandalism	Attacker defaces Web site logo, or destroys CEO's hard drive physically or electronically.

FIGURE 12-23 System threats can be grouped into several broad categories. Note the examples provided for each category.

ON THE WEB

To learn more about risk management, visit the Management Information Systems CourseMate Web site at **www.cengagebrain.com**, navigate to **On the Web Links** for this chapter, and locate the Risk Management link.

Next, the risk manager identifies vulnerabilities and how they might be exploited. A **vulnerability** is a security weakness or soft spot, and an **exploit** is an attack that takes advantage of a vulnerability. To identify vulnerabilities, a risk manager might ask questions like these: *Could hackers break through the proxy server? Could employees retrieve sensitive files without proper authorization? Could people enter the computer room and sabotage our servers?* Each vulnerability is rated and assigned a value. The output of risk identification is a list of assets, vulnerabilities, and ratings.

RISK ASSESSMENT In IT security terms, a **risk** is the impact of an attack multiplied by the likelihood of a vulnerability being exploited. For example, an impact value of 2 and a vulnerability rating of 10 would produce a risk of 20. On the other hand, an impact value of 5 and a vulnerability rating of 5 would produce a risk of 25. When risks arecalculated and prioritized, **critical risks** will head the list. Although ratings can be subjective, the overall process provides a consistent approach and framework.

RISK CONTROL After risks are identified and assessed, they must be controlled. Control measures might include the following examples: *We could place a firewall on the proxy server; We could assign permissions to sensitive files; We could install biometric devices to guard the computer room.* Typically, management chooses one of four risk control strategies: avoidance, mitigation, transference, or acceptance. **Avoidance** eliminates the risk by adding protective safeguards. For example, to prevent unauthorized access to LAN computers, a secure firewall might be installed. **Mitigation** reduces the impact of a risk by careful planning and preparation. For example, a company can prepare a disaster recovery plan in case a natural disaster occurs. **Transference** shifts the risk to another asset or party, such as an insurance company. **Acceptance** means that nothing is done. Companies usually accept a risk only when the protection clearly is not worth the expense.

The risk management process is iterative — risks constantly are identified, assessed, and controlled. To be effective, risk managers need a combination of business knowledge, IT skills, and experience with security tools and techniques.

Attacker Profiles and Attacks

An **attack** is a hostile act that targets the system, or the company itself. Thus, an attack might be launched by a disgruntled employee, or a hacker who is 10,000 miles away. Attackers break into a system to cause damage, steal information, or gain recognition, among other reasons. Attackers can be grouped into categories, as shown in Figure 12-24, while Figure 12-25 describes some common types of attacks.

Attacker Characteristics

ATTACKER	DESCRIPTION	SKILL SET
Cyberterrorist	Attacks to advance political, social, or ideological goals.	High
Employee	Uses unauthorized information or privileges to break into computer systems, steal information, or cause damage.	Varies
Hacker	Uses advanced skills to attack computer systems with malicious intent (black hat) or to expose flaws and improve security (white hat).	High
Hacktivist	Attacks to further a social or political cause; often involves shutting down or defacing Web sites.	Varies
Script kiddie	Inexperienced or juvenile hacker who uses readily available malicious software to disrupt or damage computer systems, and gain recognition.	Low
Spy	Non-employee who breaks into computer systems to steal information and sell it.	High

FIGURE 12-24 IT security professionals have coined labels for various types of attackers.

Types of Attacks and Examples

ATTACK	EXAMPLES
Back door	Attacker finds vulnerability in software package and exploits it.
Denial of service or distributed denial of service	One or more computers send a stream of connection requests to disable a Web server.
DNS poisoning	False DNS (Domain Name Server) information steers the user to the attacker's Web site. Attackers trick users into thinking they are visiting a legitimate site, such as a bank site, then attempt to obtain bank account numbers, usernames, and passwords.
Dumpster diving	Attacker scours the trash for valuable information that can be used to compromise the system.
Mail bombing	Enormous volumes of e-mail are sent to a target address.
Malicious code	Attacker sends infected e-mail to the target system. Attackers may use viruses, worms, Trojan horses, keystroke loggers, spyware, or scripts to destroy data, bog down systems, spy on users, or assume control of infected systems.
Man in the middle	The attacker intercepts traffic and poses as the recipient, sending the data to the legitimate recipient but only after reading the traffic or modifying it.
Password cracking	Hacker attempts to discover a password to gain entry into a secured system. This can be a dictionary attack, where numerous words are tried, or a brute force attack, where every combination of characters is attempted.
Privilege escalation	Employee tricks a computer into raising his or her account to the administrator level.
Sniffing	Network traffic is intercepted and scanned for valuable information.
Social engineering	An attacker calls the help desk posing as a legitimate user and requests that his or her password be changed.
Spam	Unwanted, useless e-mail is sent continuously to business e-mail accounts, wasting time and decreasing productivity.
Spoofing	IP address is forged to match a trusted host, and similar content may be displayed to simulate the real site for unlawful purposes.

FIGURE 12-25 Attacks can take many forms, as this table shows. IT security managers must be able to detect these attacks and respond with suitable countermeasures.

The following sections discuss how companies combat security threats and challenges by using a multilevel strategy.

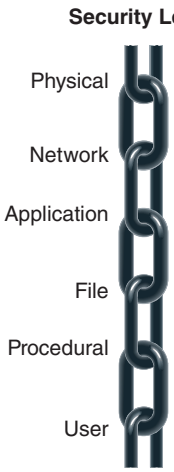


FIGURE 12-26
Each security link has a specific focus, and the overall chain is only as strong as the weakest link.

Security Levels

To provide system security, you must consider six separate but interrelated levels: physical security, network security, application security, file security, user security, and procedural security. Like the chain shown in Figure 12-26, system security is only as strong as the weakest link. The following sections describe these security levels, and the issues that must be addressed. Top management often makes the final strategic and budget decisions regarding security, but systems analysts should understand the overall picture in order to make informed recommendations.

Physical Security

The first level of system security concerns the physical environment, including IT resources and people throughout the company. Special attention must be paid to critical equipment located in operations centers, where servers, network hardware, and related equipment operate. Large companies usually have a dedicated room built specifically for IT operations. Smaller firms might use an office or storage area. Regardless of its size and shape, an operations center requires special protection from unwanted intrusion. In addition to centrally located equipment, all computers on the network must be secure, because each server or workstation can be a potential access point. Physical access to a computer represents an entry point into the system and must be controlled and protected.

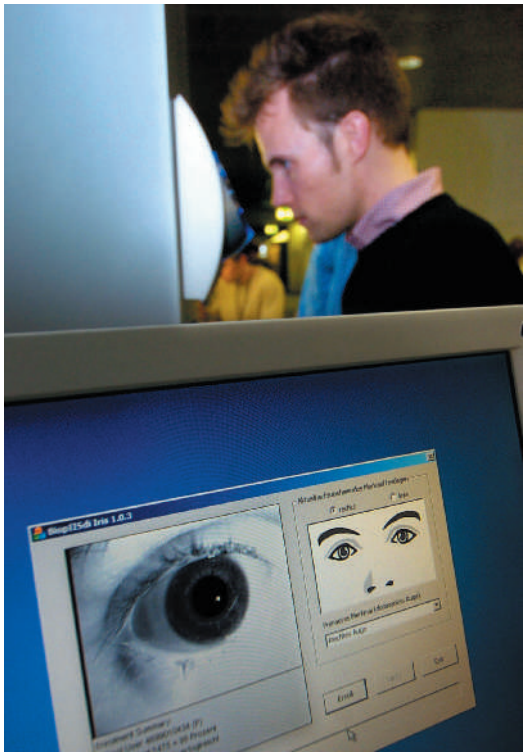


FIGURE 12-27 Companies use biometric scanning to analyze the features of the eye's iris, which has more than 200 points that can be measured and used for comparison.

OPERATIONS CENTER SECURITY Perimeter security is essential in any room or area where computer equipment is operated or maintained. Physical access must be controlled tightly, and each entrance must be equipped with a suitable security device. All access doors should have internal hinges and electromagnetic locks that are equipped with a battery backup system to provide standby power in the event of a power outage. When the battery power is exhausted, the doors should fail in a closed position, but it should be possible for someone locked inside the room to open the door with an emergency release.

To enhance security, many companies are installing **biometric scanning systems**, which map an individual's facial features, fingerprints, handprint, or eye characteristics, as shown in Figure 12-27. These hi-tech authentication systems replace magnetic identification badges, which can be lost, stolen, or altered.

Video cameras and motion sensors can be used to monitor computer room security and provide documentation of all physical activity in the area. A motion sensor uses infrared technology to detect movement, and can be configured to provide audible or silent alarms, and to send e-mail messages when it is triggered. Other types of sensors can monitor temperature and humidity in the computer room. Motion sensor alarms can be activated at times when there is no expected activity in the computer room, and authorized technicians should have codes to enable or disable the alarms.

SERVERS AND DESKTOP COMPUTERS If possible, server and desktop computer cases should be equipped with locks. This simple, but important, precaution might prevent an intruder from modifying the hardware configuration of a server, damaging the equipment, or removing a disk drive. Server racks should be locked, to avoid the unauthorized placement and retrieval of keystroke loggers. A **keystroke logger** is a device that can be inserted between a keyboard and a computer. Typically, the device resembles an ordinary cable plug, so it does not call attention to itself.

The device can record everything that is typed into the keyboard, including passwords, while the system continues to function normally. Keystroke loggers can be used legitimately to monitor, back up, and restore a system, but if placed by an intruder, a keystroke logger represents a serious security threat.

In addition to hardware devices, keystroke logging software also exists. A keystroke logging program can be disguised as legitimate software and downloaded from the Internet or a company network. The program remains invisible to the user as it records keystrokes and uploads the information to whoever installed the program. Such malicious software can be removed by antivirus and antispyware software, discussed later in the Application Security section.

Tamper-evident cases should be used where possible. A tamper-evident case is designed to show any attempt to open or unlock the case. In the event that a computer case has been opened, an indicator LED remains lit until it is cleared with a password. Tamper-evident cases do not prevent intrusion, but a security breach is more likely to be noticed. Many servers now are offered with tamper-evident cases as part of their standard configuration.

Monitor screen savers that hide the screen and require special passwords to clear should be used on any server or workstation that is left unattended. Locking the screen after a period of inactivity is another safeguard. Microsoft Windows 7 allows an administrator to include this feature in security policies. Also, you can use a **BIOS-level password**, also called a **boot-level password** or a **power-on password**, that must be entered before the computer can be started. A boot-level password can prevent an unauthorized person from booting a computer by using a CD-ROM or USB device.

Finally, companies must consider electric power issues. In mission-critical systems, large-scale backup power sources are essential to continue business operations. In other cases, computer systems and network devices should be plugged into an **uninterruptible power supply** (**UPS**) that includes battery backup with suitable capacity. The UPS should be able to handle short-term operations in order to permit an orderly backup and system shutdown.

NOTEBOOK COMPUTERS When assessing physical security issues, be sure to consider additional security provisions for notebook, laptop, and tablet computers. Because of their small size and high value, these computers are tempting targets for thieves and industrial spies. Although the following suggestions are intended as a checklist for notebook computer security, many of them also apply to desktop workstations.

- Select an operating system, such as Windows 7, that allows secure logons, BIOS-level passwords, and strong firewall protection. You can also select hardware that allows you to require BIOS-level passwords. Also, log on and work with a user account that has limited privileges rather than an administrator account, and mask the administrator account by giving it a different name that would be hard for a casual intruder to guess.
- Mark or engrave the computer's case with the company name and address, or attach a tamper-proof asset ID tag. Many hardware vendors allow corporate customers to add an asset ID tag in the BIOS. For example, after powering up, you might see the message: *Property of SCR Associates – Company Use Only*. These measures might not discourage a professional thief, but might deter a casual thief, or at least make your computer relatively less desirable because it would be more difficult to use or resell. Security experts also recommend that you use a generic carrying case, such as an attaché case, rather than a custom carrying case that calls attention to itself and its contents. Also be sure to complete and submit all manufacturer registration cards.
- Consider notebook models that have a built-in fingerprint reader, as shown in Figure 12-28.
- Many notebook computers have a **Universal Security Slot** (**USS**) that can be fastened to a cable lock or laptop alarm. Again, while these precautions might not deter professional thieves, they might discourage and deter casual thieves.

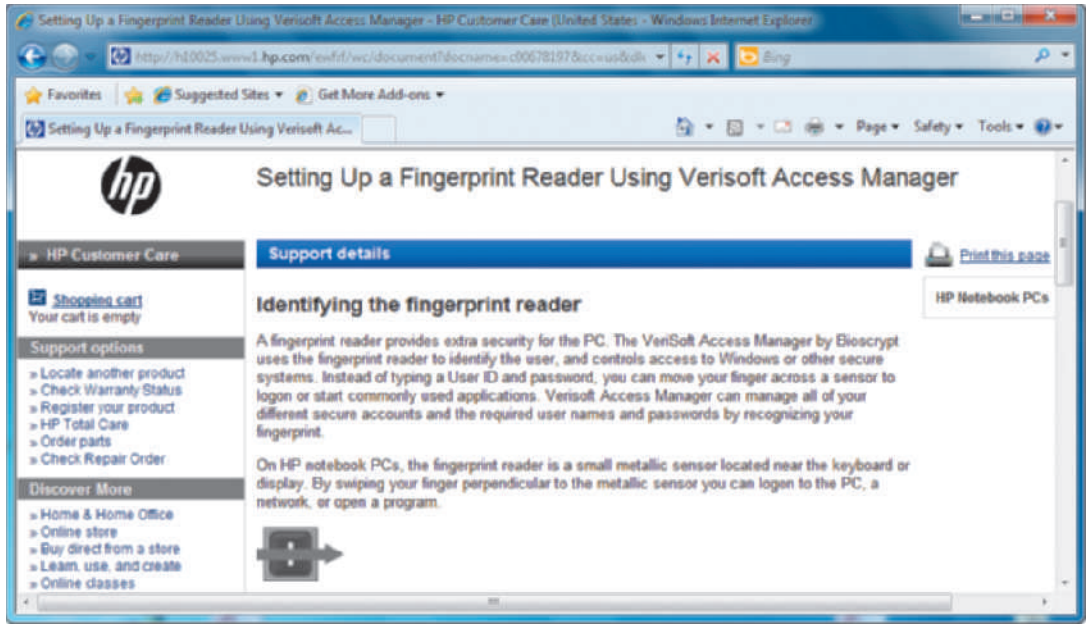


FIGURE 12-28 Some notebook computers feature a fingerprint reader, which is a small metallic sensor located near the keyboard or display.

- Back up all vital data before using the notebook computer outside the office. Also, instead of using your computer's hard drive, save and transport highly sensitive data on removable media, such as a flash memory device.
- Use tracking software that directs your laptop periodically to contact a security tracking center. If your notebook is stolen, the call-in identifies the computer and its physical location. Armed with this information, the security tracking center can alert law enforcement agencies and communications providers. As shown in Figure 12-29, Computrace sells a product called LoJack for Laptops, which offers call-in service, as well as a remote data erase capability. Some versions of the product even provide a payment if the firm does not recover your stolen laptop.

FIGURE 12-29 Many students use LoJack on their notebook computers. The product offers automated call-in identification and remote data erase capability.

- While traveling, try to be alert to potential high-risk situations, where a thief, or thieves, might attempt to distract your attention and snatch your computer. These situations often occur in crowded, noisy places like airport baggage claim areas, rental car counters, and security checkpoints. Also, when traveling by car, store your computer in a trunk or lockable compartment where it will not be visible.
- Establish stringent password protection policies that require minimum length and complexity, and set a limit on how many times an invalid password can be entered before the system locks itself down. In some situations, you might want to establish file encryption policies to protect extremely sensitive files.

CASE IN POINT 12.3: OUTER BANKS COUNTY

Outer Banks County is a 200-square-mile area in coastal North Carolina, and you are the IT manager. The county has about a hundred office employees who perform clerical tasks in various departments. A recent budget crisis has resulted in a wage and hiring freeze, and morale has declined. The county manager has asked you to install some type of keystroke logger to monitor employees and determine whether they are fully productive. After your conversation, you wonder whether there might be some potential privacy and security issues involved.

For example, does an employer have a duty to notify its employees that it is monitoring them? Should the employer notify them even if not required to do so? From a human resources viewpoint, what would be the best way to approach this issue? Also, does a potential security issue exist? If an unauthorized person gained possession of the keystroke log, he or she might be able to uncover passwords and other sensitive data.

What are your conclusions? Are these issues important, and how would you respond to the county manager's recommendation? Before you answer, you should go on the Internet and learn more about keystroke loggers generally, and specific products that currently are available.

Network Security

A **network** is defined as two or more devices that are connected for the purpose of sending, receiving, and sharing data, which is called network traffic. In order to connect to a network, a computer must have a **network interface**, which is a combination of hardware and software that allows the computer to interact with the network. To provide security for network traffic, data can be **encrypted**, which refers to a process of encoding the data so it cannot be accessed without authorization.

ENCRYPTING NETWORK TRAFFIC Network traffic can be intercepted and possibly altered, redirected, or recorded. For example, if an **unencrypted**, or **plain text**, password or credit card number is transmitted over a network connection, it can be stolen. When the traffic is encrypted, it still is visible, but its content and purpose are masked.

Figure 12-30 on the next page shows an example of encrypted traffic compared to plain text traffic. In the upper screen, the user has logged on to the SCR Associates case study, using a password of *sad9e*. Notice that anyone who gains access to this data easily could learn the user's password. In the lower screen, the user has logged on to an online bank account and used a password, but the encryption process has made it impossible to decipher the keystrokes.

Two commonly used encryption techniques are private key encryption and public key encryption. **Private key encryption** is symmetric, because a single key is used to encrypt and decrypt information. While this method is simple and fast, it poses a fundamental problem. To use symmetric encryption, both the sender and receiver must possess the same key beforehand, or it must be sent along with the message, which increases the risk of interception and disclosure.

In contrast, **public key encryption** (**PKE**) is asymmetric, because each user has a pair of keys: a public key and a private key, as shown in Figure 12-31 on the next page. Public keys are used to encrypt messages. Users can share their public keys freely, while keeping their private keys tightly guarded. Any message encrypted with a user's public key can only be decrypted with that user's private key. This method is commonly used in secure online shopping systems.

A recent Wikipedia article uses an interesting analogy for public key encryption. The article suggests that PKE is similar to a locked mailbox with a mail slot that is accessible to the public. The mailbox's location (street address) represents the public key. Anyone knowing the street address can drop a message through the slot. However, only a person with a key can open the box and read the message.

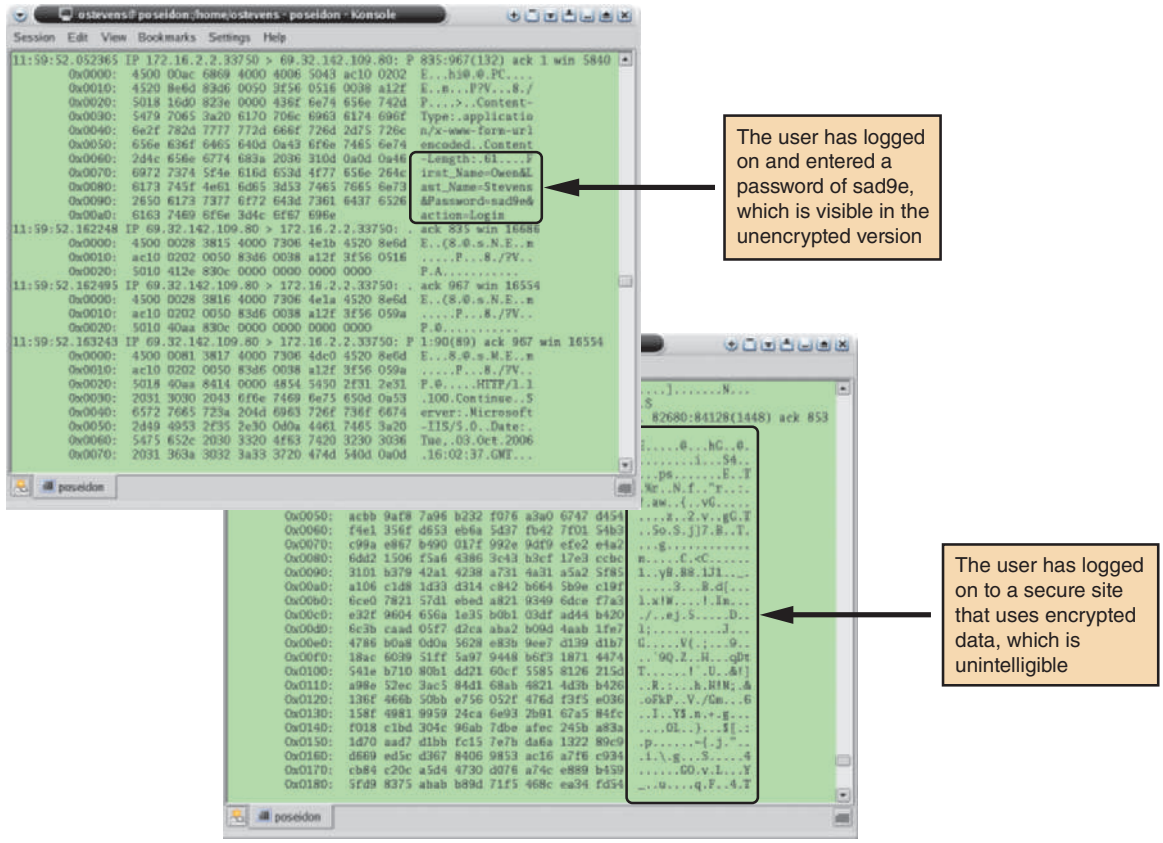


FIGURE 12-30 The upper screen shows an example of unencrypted text, which contains a visible password. In the lower screen, the encrypted text cannot be read.

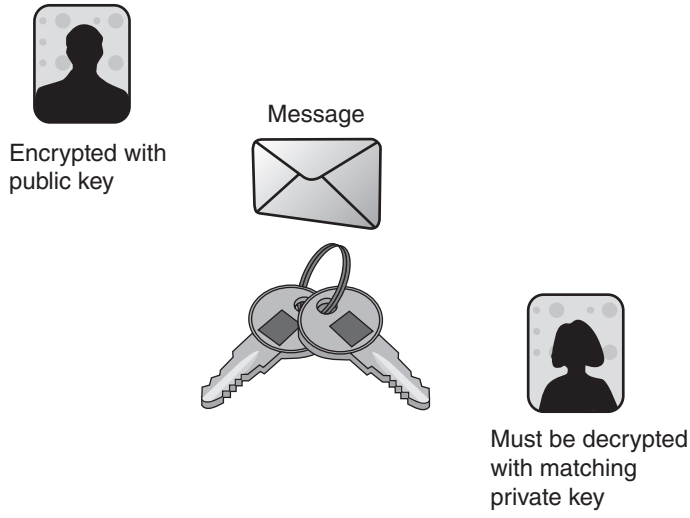


FIGURE 12-31 In a PKE environment, a message encrypted with a public key only can be decrypted with the matching private key.

WIRELESS NETWORKS As you learned in Chapter 10, wireless network security is a vital concern, because wireless transmission is much more vulnerable than traffic on a wired network. However, if wireless traffic is encrypted, any data that is intercepted by an unintended recipient will be useless to the intruder.

The earliest form of wireless security, called **Wired Equivalent Privacy (WEP)**, required each wireless client to use a special, preshared key. Although this method was used by many home and small office networks, it provided relatively weak protection.

WEP was replaced by **Wi-Fi Protected Access (WPA)**, which offered major security improvements based on protocols created by the Wi-Fi Alliance. The most recent wireless security enhancement, called **WPA2**, further strengthens the level of wireless protection. WPA2 is an extension of WPA based on a full implementation of the **IEEE 802.11i** standard. According to the WiFi Alliance, the WPA2 standard became mandatory for all new devices seeking Wi-Fi certification after 2006. WPA2 is compatible with WPA, so companies easily can migrate to the new security standard.

PRIVATE NETWORKS It is not always practical to secure all network traffic. Unfortunately, encrypting traffic increases the burden on a network, and can decrease network performance significantly. In situations where network speed is essential, such as a Web server linked to a database server, many firms use a private network to connect the computers. A **private network** is a dedicated connection, similar to a leased telephone line. Each computer on the private network must have a dedicated interface to the network, and no interface on the network should connect to any point outside the network. In this configuration, unencrypted traffic safely can be transmitted because it is not visible, and cannot be intercepted from outside the network.

VIRTUAL PRIVATE NETWORKS Private networks work well with a limited number of computers, but if a company wants to establish secure connections for a larger group, it can create a virtual private network (VPN). A **virtual private network (VPN)** uses a public network, such as the Internet or a company intranet, to connect remote users securely. Instead of using a dedicated connection, a VPN allows remote clients to use a special key exchange that must be authenticated by the VPN. Once authentication is complete, a secure network connection, called a **tunnel**, is established between the client and the access point of the local intranet. All traffic is encrypted through the VPN tunnel, which provides an additional level of encryption and security. As more companies allow employees to work from home, a VPN can provide acceptable levels of security and reliability.

PORTS AND SERVICES A **port**, which is identified by a number, is used to route incoming traffic to the correct application on a computer. In TCP/IP networks, such as the Internet, all traffic received by a computer contains a destination port. Because the destination port determines where the traffic will be routed, the computer sorts the traffic by port number, which is included in the transmitted data. An analogy might be a large apartment building with multiple mailboxes. Each mailbox has the same street address, but a different box number. Port security is critically important, because an attacker could use an open port to gain access to the system.

A **service** is an application that monitors, or listens on, a particular port. For example, a typical e-mail application listens on port 25. Any traffic received by that port is routed to the e-mail application. Services play an important role in computer security, and they can be affected by port scans and denial-of-service attacks.

- Port scans. **Port scans** attempt to detect the services running on a computer by trying to connect to various ports and recording the ports on which a connection was accepted. For example, the result of an open port 25 would indicate that a mail server is running. Port scans can be used to draw an accurate map of a network, and pinpoint possible weaknesses.
- Denial of service. A **denial of service (DoS)** attack occurs when an attacking computer makes repeated requests to a service or services running on certain ports. Because the target computer has to respond to each request, it can become bogged down and fail to respond to legitimate requests. A much more devastating attack based on this method is called a **distributed denial of service (DDoS)** attack. This attack involves multiple attacking computers that can synchronize DOS attacks and immobilize a server, as shown in Figure 12-32 on the next page. The seriousness of a DOS attack is evident in the National Cyber Alert System tip shown in Figure 12-33 on the next page.

FIREWALLS A **firewall** is the main line of defense between a local network, or intranet, and the Internet. A firewall must have at least one network interface with the Internet, and at least one network interface with a local network or intranet. Firewall software examines all network traffic sent to and from each network interface. Preset rules establish certain conditions that determine whether the firewall will allow the traffic to pass. When a

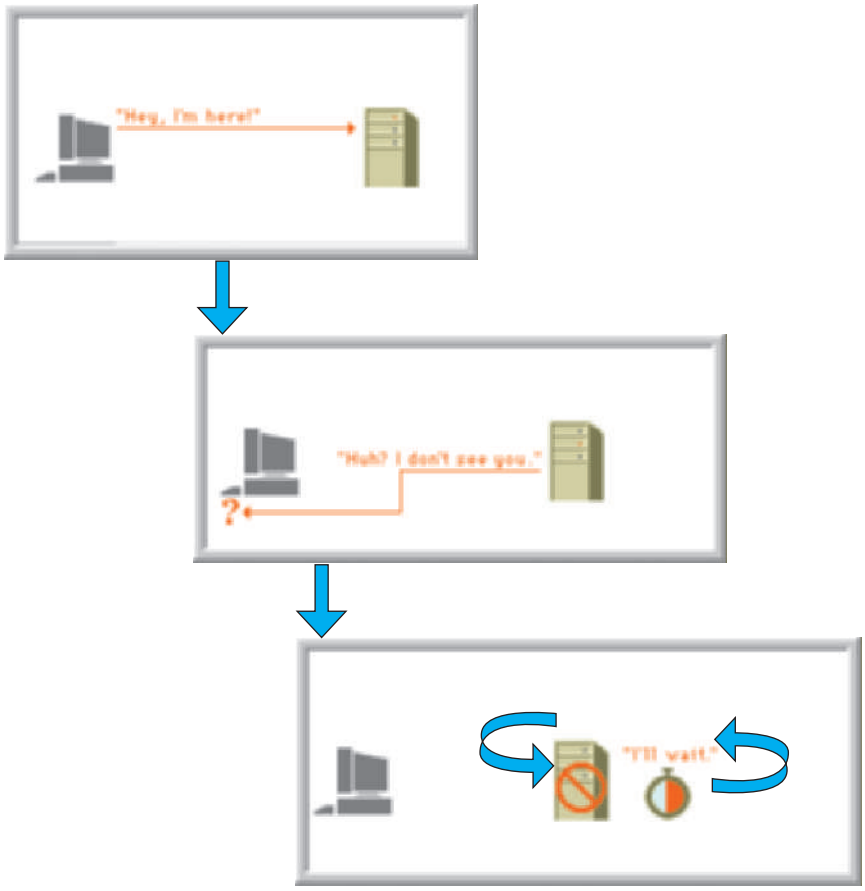


FIGURE 12-32 In a denial of service attack, an attacker sends numerous authentication requests with false return addresses. The server tries unsuccessfully to send authentication approval, and eventually is disabled by the flood of requests.

matching rule is found, the firewall automatically accepts, rejects, or drops the traffic. When a firewall rejects traffic, it sends a reply indicating that the traffic is not permissible. When a firewall drops traffic, no reply is sent. Firewalls can be configured to detect and respond to denial-of-service attacks, port scans, and other suspicious activity.

Figure 12-34 shows a basic set of firewall rules for a company that has a Web server and a mail server. In this example, the firewall would accept public Web server traffic only on ports 80 and 443, and public mail server traffic only on port 25. The firewall would allow private LAN traffic to any destination and port.

NETWORK INTRUSION DETECTION Suppose an intruder attempts to gain access to the system. Obviously, an intrusion alarm should be sounded when certain activity or known attack patterns are detected. A **network intrusion detection system** (NIDS) is like a burglar alarm that goes off when it detects a configuration violation. The NIDS also can alert the administrator when it detects suspicious network traffic patterns. A NIDS requires fine-tuning to detect the difference between legitimate network traffic and an

FIGURE 12-33 The United States Computer Emergency Readiness Team has published a security tip about DoS threats.

RULE	INTERFACE	SOURCE	DESTINATION	PORT	ACTION
1	Public	Any	Web Server	80	Accept
2	Public	Any	Web Server	443	Accept
3	Public	Any	Web Server	Any	Reject
4	Public	Any	Mail Server	25	Accept
5	Public	Any	Mail Server	Any	Reject
6	Public	Any	Any	Any	Drop
7	Private	LAN	Any	Any	Accept

FIGURE 12-34 Examples of rules that determine whether the firewall will allow traffic to pass.

attack. It is also important that a NIDS be placed on a switch or other network device that can monitor all network traffic. Although a NIDS requires some administrative overhead, it can be very helpful in documenting the efforts of attackers and analyzing network performance.

Application Security

In addition to securing the computer room and shielding network traffic, it is necessary to protect all server-based applications. To do so, you must analyze the application's functions, identify possible security concerns, and carefully study all available documentation. Application security requires an understanding of services, hardening, application permissions, input validation techniques, software patches and updates, and software logs.

SERVICES In the network security section, you learned that a service is an application that monitors, or listens, on a particular port. You can determine which services are running by using a port scan utility. If a particular application is not needed, it should be disabled. This will improve system security, performance, and reliability. An unnecessary or improperly configured service could create a vulnerability called a **security hole**. For example, if a loosely configured FTP (File Transfer Protocol) service is available to a hacker, he or she might be able to upload destructive code to the server.

HARDENING The **hardening** process makes a system more secure by removing unnecessary accounts, services, and features. Hardening is necessary because the default configuration of some software packages might create a vulnerability. For example, initial software settings might include relatively weak account permissions or file sharing controls. Hardening can be done manually or by using a configuration template, which speeds up the process in a large organization.

Hardening also includes additional protection such as antivirus and antispyware software. These programs can detect and remove **malware**, which is hostile software designed to infiltrate, damage, or deny service to a computer system. Malware includes worms, Trojan horses, keystroke loggers, and spyware, among others.

APPLICATION PERMISSIONS Typically, an application is configured to be run only by users who have specific rights. For example, an **administrator**, or **superuser** account, allows essentially unrestricted access. Other users might be allowed to enter data, but not to modify or delete existing data. To prevent unauthorized or destructive changes, the application should be configured so that nonprivileged users can access the program, but cannot make changes to built-in functions or configurations. **User rights**, also called **permissions**, are discussed in more detail in the file security section.

INPUT VALIDATION As you learned in Chapter 8, when designing the user interface, input validation can safeguard data integrity and security. For example, if an application requires a number from *1* to *10*, what happens if an alphabetic character or the number *31* is entered? If the application is designed properly, it will respond with an appropriate error message. Chapter 8 also explained data entry and validation checks, which are important techniques that can improve data integrity and quality. Failure to validate input data can result in output errors, increased maintenance expense, and erratic system behavior.

PATCHES AND UPDATES In an operational system, security holes or vulnerabilities might be discovered at any time. Patches can be used to repair these holes, reduce vulnerability, and update the system. Like any other new software, patches must be tested carefully. Before applying a patch, an effort should be made to determine the risks of *not* applying the patch, and the possibility that the patch might affect other areas of the system.

Many firms purchase software packages called **third-party software**. Patches released by third-party software vendors usually are safe, but any patch must be reviewed carefully before it is applied. Because researching and applying patches is time consuming and expensive, many software vendors offer an **automatic update service** that enables an application to contact the vendor's server and check for a needed patch or update. Depending on the configuration, available patches can be downloaded and installed without human intervention, or might require approval by IT managers. Although it is convenient, automatic updating carries substantial risks, and should be used only if changes can readily be undone if unexpected results or problems develop.

SOFTWARE LOGS Operating systems and applications typically maintain a **log** that documents all events, including dates, times, and other specific information. Logs can be important in understanding past attacks and preventing future intrusions. For example, a pattern of login errors might reveal the details of an intrusion attempt. A log also can include system error messages, login histories, file manipulation, and other information that could help track down unauthorized use. Software logs should be monitored constantly to determine if misuse or wrongdoing has occurred. As explained in the network security section, a network intrusion detection system (NIDS) can alert a system administrator whenever suspicious events occur. Windows Event Viewer, shown in Figure 12-35, is an example of a built-in software log.

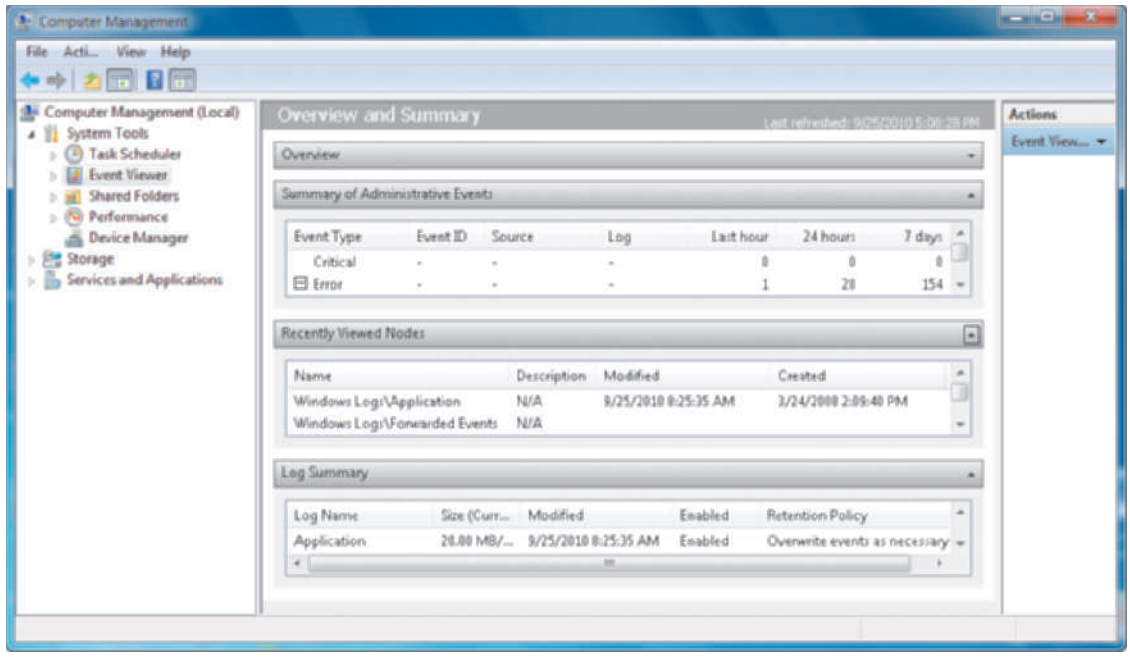


FIGURE 12-35 Windows Event Viewer can log application usage, security settings, and system changes.

File Security

Computer configuration settings, users' personal information, and other sensitive data are stored in files. The safety and protection of these files is a vital element in any computer security program, and a systems analyst needs to consider the importance of encryption, or encoding files to make them unreadable by unauthorized users, and permissions, which can be assigned to individual users or to user groups.

ENCRYPTION As you learned in the section on network security, encryption scrambles the contents of a file or document to protect it from unauthorized access. All corporate data must be protected, but encryption is especially important for sensitive material such as personnel or financial records. You can use the **Encrypting File System** (EFS), which is fully implemented on Windows 7 Professional, to encrypt and limit access to data. EFS can be enabled or disabled at the folder or the document level by simply changing the properties for that folder or document.

PERMISSIONS File security is based on establishing a set of permissions, which describe the rights a user has to a particular file or directory on a server. The most common permissions are read, write, and execute. Typical examples of permissions include the following:

- Read a file — The user can read the contents of the file.
- Write a file — The user can change the contents of the file.
- Execute a file — The user can run the file, if it is a program.
- Read a directory — The user can list the contents of the directory.
- Write a directory — The user can add and remove files in the directory.

When assigning file permissions, a system administrator should ensure that each user has only the minimum permissions necessary to perform his or her work — not more. In some firms, the system administrator has broad discretion in assigning these levels; in other companies, an appropriate level of management approval is required for any permissions above a standard user level. In any case, a well-documented and enforced permissions policy is necessary to promote file security and reduce system vulnerability.

USER GROUPS Individual users who need to collaborate and share files often request a higher level of permissions that would enable any of them to change file content. A better approach, from a system administrator's viewpoint, might be to create a user group, add specific users, and assign file permissions to the group, rather than to the individuals. Many firms use this approach, because it allows a user's rights to be determined by his or her work responsibilities, rather than by job title or rank. If a person is transferred, he or she leaves certain groups and joins others that reflect current job duties.

User Security

User security involves the identification of system users and consideration of user-related security issues. Regardless of other security precautions and features, security ultimately depends on system users and their habits, practices, and willingness to support security goals. Unfortunately, many system break-ins begin with a user account that is compromised in some way. Typically, an intruder accesses the system using the compromised account, and may attempt a **privilege escalation attack**, which is an unauthorized attempt to increase permission levels.

User security requires identity management, comprehensive password protection, defenses against social engineering, an effective means of overcoming user resistance, and consideration of new technologies. These topics are discussed in the following sections.

ON THE WEB

To learn more about identity management, visit the Management Information Systems CourseMate Web site at **www.cengagebrain.com**, navigate to **On the Web Links** for this chapter, and locate the Identity Management link.

IDENTITY MANAGEMENT **Identity management** refers to controls and procedures necessary to identify legitimate users and system components. An identity management strategy must balance technology, security, privacy, cost, and user productivity. Identity management is an evolving technology that is being pursued intensively by corporations, IT associations, and governments.

The Burton Group, a leading IT security consultant, has described identity management as a "set of electronic records that represent … people, machines, devices, applications, and services." This definition suggests that not just users, but each component in a system, must have a verifiable identity that is based on unique characteristics. For example, user authentication might be based on a combination of a password, a Social Security number, an employee number, a job title, and a physical location.

Because of the devastating consequences of intrusion, IT managers are giving top priority to identity management strategies and solutions.

PASSWORD PROTECTION As the section on physical security points out, a secure system must have a password policy that requires minimum length, complexity, and a limit on invalid login attempts. Although passwords are a key element in any security program, users often choose passwords that are easy to recall, and they sometimes resent having to remember complex passwords. Even so, IT managers should insist on passwords that have a minimum length, require a combination of case-sensitive letters and numbers, and must be changed periodically. Unfortunately, any password can be compromised if a user writes it down and stores it in an easily accessible location such as a desk, a bulletin board, or under the keyboard.

During a recent U.S. election campaign, a hacker made global headlines by gaining access to the e-mail account of a vice-presidential candidate. The intruder signed on as the candidate, requested a new password, guessed the answers to the security questions, and was able to enter the account. These actions were totally illegal, and constituted a serious felony under federal law.

SOCIAL ENGINEERING Even if users are protecting and securing their passwords, an intruder might attempt to gain unauthorized access to a system using a tactic called **social engineering**. In a social engineering attack, an intruder uses social interaction to gain access to a computer system. For example, the intruder might pretend to be a new employee, an outside technician, or a journalist. Through a series of questions, the intruder tries to obtain the information that he or she needs to compromise the system. A common ploy is for the attacker to contact several people in the same organization, and use some information from one source to gain credibility and entry to another source.

An intruder also might contact a help desk and say: "Hi. This is Anna Dressler from accounting. I seem to have forgotten my password. Could you give me a new one?" Although this request might be legitimate, it also might be an attacker trying to access the system. A password never should be given based solely on this telephone call. The user should be required to provide further information to validate his or her identity, such as a Social Security number, employee ID, telephone extension, and company e-mail address.

One highly publicized form of social engineering is called **pretexting**, which is a method of obtaining personal information under false pretenses. Pretexting, which is described in the Federal Trade Commission statement shown in Figure 12-36, is a very real threat. The best way to combat social engineering attacks is with employee education, more training, and a high level of awareness during day-to-day operations.

FIGURE 12-36 As the Federal Trade Commission points out, pretexting involves obtaining your personal information under false pretenses.

USER RESISTANCE Many users, including some senior managers, dislike tight security measures because they can be inconvenient and time consuming. Systems analysts should remind users that the company owes the best possible security to its customers, who have entrusted personal information to the firm; to its employees, who also have personal information stored in company files; and to its shareholders, who expect the company to have a suitable, effective, and comprehensive security program that will safeguard company assets and resources. When users understand this overall commitment to security and feel that they are part of it, they are more likely to choose better passwords, be more alert to security issues, and contribute to the overall success of the company's security program.

NEW TECHNOLOGIES In addition to traditional measures and biometric devices, technology can enhance security and prevent unauthorized access. For example, a **security token** is a physical device that authenticates a legitimate user. The Wikipedia image in Figure 12-37 shows several types of security tokens. Some firms provide employees with security tokens that generate a numeric validation code, which the employee enters in addition to his or her normal password.

Unfortunately, new technology sometimes creates new risks. For example, Google offers a desktop-based search engine, Google Desktop, with a powerful indexing feature that scans all the files, documents, e-mails, chats, and stored Web pages on a user's computer. Although the program provides a convenient way for users to locate and retrieve their data, it also can make it easier for an

FIGURE 12-37 Security tokens, which come is various forms, can provide an additional level of security.

intruder to obtain private information, especially in a multiuser environment, because the program can recall and display almost anything stored on the computer. Also, if an intruder uses the term *password* in a search, the program might be able to find password reminders that are stored anywhere on the computer. According to Google, the search index resides on the user's computer and is never sent or made accessible to Google or anyone else without explicit consent. However, to maintain privacy for multiuser computers, Google strongly recommends that each user have a separate account, with individual usernames and passwords.

Google Desktop also offers a way for users to search across multiple computers, and this option has caused some concern among IT managers and privacy advocates. To perform a multi-computer search, it is necessary to store a user's data temporarily on Google's servers. Some observers feel that this makes the data more vulnerable and possibly subject to examination by third parties, including government agencies. Google states that if you choose to enable the *Search Across Computers* feature, your shared data is encrypted and treated as personal information, in accordance with the Google Privacy Policy. Software such as Google Desktop is powerful, convenient, and fun to use. However, you should understand the possible risks involved before installing this type of software on personal or business workstations.

Procedural Security

Procedural security, also called **operational security**, is concerned with managerial policies and controls that ensure secure operations. In fact, many IT professionals believe that security depends more on managerial issues than technology. Management must work to establish a corporate culture that stresses the importance of security to the firm and its people. Procedural security defines how particular tasks are to be performed, from large-scale data backups to everyday tasks such as storing e-mails or forms. Other procedures might spell out how to update firewall software or how security personnel should treat suspected attackers.

All employees should understand that they have a personal responsibility for security. For example, an employee handbook might require that users log out of their system accounts, clear their desks, and secure all documents before leaving for the day. These policies reduce the risk of **dumpster diving** attacks, in which an intruder raids desks or trash bins for valuable information. In addition, paper shredders should be used to destroy sensitive documents.

Procedural security also includes safeguarding certain procedures that would be valuable to an attacker. The most common approach is a *need-to-know* concept, where access is limited to employees who need the information to perform security-related tasks. Many firms also apply a set of classification levels for access to company documents. For example, highly sensitive technical documents might be available only to the IT support team, while user-related materials would be available to most company employees. If classification levels are used, they should be identified clearly and enforced consistently.

CASE IN POINT 12.4: Chain Link Consulting, Inc.

Chain Link Consulting is an IT consulting firm that specializes in system security issues. The company's president has asked you to help her put together a presentation to a group of potential clients at a trade show meeting next month. First, she wants you to review system security issues, considering all six security levels. Then she wants you to come up with a list of ways that Chain Link could test a client's security practices, in order to get a real-world assessment of vulnerability.

To make matters more interesting, she told you it was OK to be creative in your recommendations, but not to propose any action that would be illegal or unethical. For example, it would be OK to pose as a job applicant with false references to see if they were being checked, but it would not be appropriate to pick a lock and enter the computer room.

Your report is due tomorrow. What will you suggest?

Procedural security must be supported by upper management and fully explained to all employees. The organization must provide training to explain the procedures and issue reminders from time to time that will make security issues a priority.

Backup and Recovery

Every system must provide for data backup and recovery. **Backup** refers to copying data at prescribed intervals, or continuously. **Recovery** involves restoring the data and restarting the system after an interruption. An overall backup and recovery plan that prepares for a potential disaster is called a **disaster recovery plan**.

The tragic events of September 11, 2001, and increased concern about global terrorism have led many companies to upgrade their backup and disaster recovery plans. Heightened focus on disaster recovery has spawned a whole new industry, which includes new tools and strategies. Many IT professionals feel that terrorism concerns have raised security awareness throughout the corporate world. Although they are separate topics, backup and disaster recovery issues usually are intertwined. The following sections cover these topics in more detail.

ON THE WEB

To learn more backup and disaster recovery, visit the Management Information Systems CourseMate Web site at **www.cengagebrain.com**, navigate to **On the Web Links** for this chapter, and locate the Backup and Disaster Recovery link.

Backup Policies

The cornerstone of business data protection is a **backup policy**, which contains detailed instructions and procedures. An effective backup policy can help a firm continue business operations and survive a catastrophe. The backup policy should specify backup media, backup types, and retention periods.

BACKUP MEDIA **Backup media** can include tape, hard drives, optical storage, and online storage. Physical backups must be carefully identified and stored in a secure location. **Offsiting** refers to the practice of storing backup media away from the main business location, in order to mitigate the risk of a catastrophic disaster such as a flood, fire, or earthquake. Even if the operating system includes a backup utility, many system administrators prefer to use specialized third-party software that offers more options and better controls for large-scale operations.

In addition to on-site data storage, many companies use Web-based data backup and retrieval services offered by vendors such as Rocky Mountain Software and IBM. For a small- or medium-sized firm, this option can be cost effective and reliable.

BACKUP TYPES Backups can be full, differential, incremental, or continuous. A **full backup** is a complete backup of every file on the system. Frequent full backups are time consuming and redundant if most files are unchanged since the last full backup. Instead of performing a full backup, another option is to perform a **differential backup**, which is faster because it backs up *only* the files that are new or changed since the last full backup. To restore the data to its original state, you restore the last full backup, and then restore the last differential backup. Many IT managers believe that a combination of full and differential backups is the best option, because it uses the least amount of storage space and is simple.

The fastest method, called an **incremental backup**, only includes recent files that never have been backed up by any method. This approach, however, requires multiple steps to restore the data — one for each incremental backup.

Most large systems use **continuous backup**, which is a real-time streaming method that records all system activity as it occurs. This method requires expensive hardware, software, and substantial network capacity. However, system restoration is rapid and effective because data is being captured in real time, as it occurs. Continuous backup often uses a **RAID** (**redundant array of independent disks**) system that mirrors the data. RAID systems are called **fault-tolerant**, because a failure of any one disk does not disable the system. Compared to one

large drive, a RAID design offers better performance, greater capacity, and improved reliability. When installed on a server, a RAID array of multiple drives appears to the computer as a single logical drive. Figure 12-38 shows a comparison of various backup methods.

Comparison of Backup Methods

BACKUP TYPE	CHARACTERISTICS	PROS AND CONS	TYPICAL FREQUENCY
Full	Backs up all files.	Slowest backup time and requires the most storage space. Rapid recovery because all files are restored in a single step.	Monthly or weekly.
Differential	Only backs up files that are new or changed since the last full backup.	Faster than a full backup and requires less storage space. All data can be restored in just two steps by using the last full backup and the last differential backup.	Weekly or daily.
Incremental	Only backs up files that are new or changed since the last backup of any kind.	Fastest backup and requires the least storage space because it only saves files that have never been backed up. However, requires many restore steps – one for each incremental backup.	Daily or more often.
Continuous	Real-time, streaming method that records all system activity.	Very expensive hardware, software, and network capacity. Recovery is very fast because system can be restored to just before an interruption.	Usually only used by large firms and network-based systems.

FIGURE 12-38 Comparison of full, differential, incremental, and continuous backup methods.

RETENTION PERIODS Backups are stored for a specific **retention period** after which they are either destroyed or the backup media is reused. Retention periods can be a specific number of months or years, depending on legal requirements and company policy. Stored media must be secured, protected, and inventoried periodically.

Business Continuity Issues

Global concern about terrorism has raised awareness levels and increased top management support for a business continuity strategy in the event of an emergency. A disaster recovery plan describes actions to be taken, specifies key individuals and rescue authorities to be notified, and spells out the role of employees in evacuation, mitigation, and recovery efforts. The disaster recovery plan should be accompanied by a **test plan**, which can simulate various levels of emergencies and record the responses, which can be analyzed and improved as necessary.

secure location. Afterward, the plan should focus on resuming business operations, including the salvaging or replacement of equipment and the recovery of backup data. The main objective of a disaster recovery plan is to restore business operations to pre-disaster levels.

Disaster recovery plans are often part of a larger **business continuity plan** (BCP), which goes beyond a recovery plan, and defines how critical business functions can continue in the event of a major disruption. Some BCPs specify the use of a hot site. A **hot site** is an alternate IT location, anywhere in the world, that can support critical systems in the event of a power outage, system crash, or physical catastrophe. A hot site requires **data replication**, which means that any transaction on the primary system must be mirrored on the hot site. If the primary system becomes unavailable, the hot site will have the latest data and can function seamlessly, with no downtime.

Although hot sites are attractive backup solutions, they are very expensive. However, a hot site provides the best insurance against major business interruptions. In addition to hot sites, business insurance can be important in a worst-case scenario. Although expensive, business insurance can offset the financial impact of system failure and business interruption.

System Obsolescence

At some point, every system becomes obsolete. For example, you might not remember punched cards, but they represented the cutting edge of data management back in the 1960s. Data was stored by punching holes at various positions, and was retrieved by machines that could sense the presence or absence of a punched hole. Most full-size cards stored only 80 characters, or bytes, so more than 12,000 cards would be needed to store a megabyte. Punched cards were even used as checks and utility bills. Today, this technology is virtually obsolete.

Constantly changing technology means that every system has a limited economic life span. Analysts and managers can anticipate system obsolescence in several ways and it never should come as a complete surprise.

A system becomes **obsolete** when it no longer supports user needs, or when the platform becomes outmoded. The most common reason for discontinuing a system is that it has reached the end of its economically useful life, as indicated by the following signs:

- The system's maintenance history indicates that adaptive and corrective maintenance are increasing steadily.
- Operational costs or execution times are increasing rapidly, and routine perfective maintenance does not reverse or slow the trend.
- A software package is available that provides the same or additional services faster, better, and less expensively than the current system.
- New technology offers a way to perform the same or additional functions more efficiently.
- Maintenance changes or additions are difficult and expensive to perform.
- Users request significant new features to support business requirements.

Systems operation and support continues until a replacement system is installed. Toward the end of a system's operational life, users are unlikely to submit new requests for adaptive maintenance because they are looking forward to the new release. Similarly, the IT staff usually does not perform much perfective or preventive maintenance because the system will not be around long enough to justify the cost. A system in its final stages requires corrective maintenance only to keep the system operational.

User satisfaction typically determines the life span of a system. The critical success factor for any system is whether or not it helps users achieve their operational and business goals. As an IT staff member, you should expect to receive input from users and managers throughout the systems development process. You should investigate and document all negative feedback, because it can be the first signal of system obsolescence.

At some point in a system's operational life, maintenance costs start to increase, users begin to ask for more features and capability, new systems requests are submitted, and the SDLC begins again.

Future Challenges and Opportunities

The only thing that is certain about the future is continuous change. Change itself is neither good nor bad — the real issue is how people and companies deal with the challenges and opportunities that are bound to occur.

No one would start a complex journey without a map and a plan. To navigate the future of information technology, companies require strategic plans, which were discussed in Chapter 2. An individual also needs a plan to reach to a specific goal or destination. This section discusses some predictions and stresses the importance of personal planning and development, including the acquisition of professional credentials.

Predictions

Although no one can foresee the future, it is safe to assume that companies will face intense competition and economic, social, and political uncertainty. Many IT experts believe that in this environment, the highest priorities will be the safety and security of corporate operations, environmental concerns, and bottom-line TCO.

Gartner Inc. is a leading consulting firm that is famous for accurate predictions of IT trends. Here is a summary of predictions that Gartner published in January, 2010:

- By 2012, 50% of traveling workers will use lighter, smaller Internet-centric devices rather than notebook computers. A new class of portable applications will enable users to re-create their work environment across multiple locations or systems.
- By 2012, 80% of commercial software will include open-source components. As open-source applications become mature, stable, and well supported, they will represent significant value opportunities for users.
- By 2012, one-third of business software spending will be for Software as a Service (SaaS).
- By 2012, 20% of businesses will use third parties to supply IT needs and will own no IT assets.
- By 2012, Facebook will become the hub for social network integration and Web socialization.
- By 2012, 60% of a new PC's total greenhouse gas emissions will have occurred before the user first turns the machine on.
- By 2013, mobile phones will overtake PCs as the most common Web access device worldwide.
- By 2014, most IT business cases will include carbon remediation costs.
- By 2014, over 3 billion adults worldwide will perform electronic transactions via mobile or Internet technology.
- By 2015, some aspects of online marketing will be regulated, which will affect more than $250 billion in Internet sales worldwide.

Gartner also predicted that large enterprises will require suppliers to certify their green credentials and sourcing policies. One issue might relate to the explosion of data storage and server farms, such as the one shown in Figure 12-39. In his 2008 book, *Planet Google*, author Randall Stross noted that the enormous amount of energy needed to drive cloud computing, including Google's servers, has raised serious environmental concerns. At the time he wrote the book, the author stated that data centers were already consuming more power in the United States than television sets.

FIGURE 12-39 The rapid growth of data centers and server farms has increased energy consumption significantly and raised environmental concerns.

Strategic Planning for IT Professionals

An IT professional should think of himself or herself as a business corporation that has certain assets, potential liabilities, and specific goals. Individuals, like companies, must have a strategic plan. The starting point is to formulate an answer to the following career planning question: What do I want to be doing three, five, or ten years from now?

Working backwards from your long-term goals, you can develop intermediate milestones and begin to manage your career just as you would manage an IT project. You can even use the project management tools described in Chapter 3 to construct a Gantt chart or a PERT/CPM chart using months (or years) as time units. Once the plan is developed, you would monitor it regularly to see whether you were still on schedule.

Planning a career is not unlike planting a tree that takes several years to reach a certain height. Once you know the desired height and the annual growth rate, you can determine when you must plant the tree. Similarly, if you want to possess a particular educational credential two years from now, and the credential takes two years to earn, then you need to start on it immediately if you want to adhere to stay on track.

IT Credentials and Certification

In recent years, technical credentials and certification have become extremely important to IT employers and employees. In a broad sense, **credentials** include formal degrees, diplomas, or certificates granted by learning institutions to show that a certain level of education has been achieved successfully. The term **certification** also has a special meaning that relates to specific hardware and software skills that can be measured and verified by examination. For example, a person might have a two- or four-year degree in Information Systems and possess an A+ certification, which attests to the person's computer hardware knowledge and skills.

Many IT industry leaders offer certification, including Microsoft, Cisco, Novell, Oracle, and Sun Microsystems.

About.com, shown in Figure 12-40 on the next page, offers hundreds of online guides and solutions for everyday questions and topics. The site includes descriptions of popular computer certifications, suggestions for choosing a certification, and tips on how to prepare for the exams.

Critical Thinking Skills

In additional to technical skills, IT professionals must have **soft skills**, such as communications, interpersonal, and perceptive abilities. IT professionals also need critical thinking skills to succeed in the workplace.

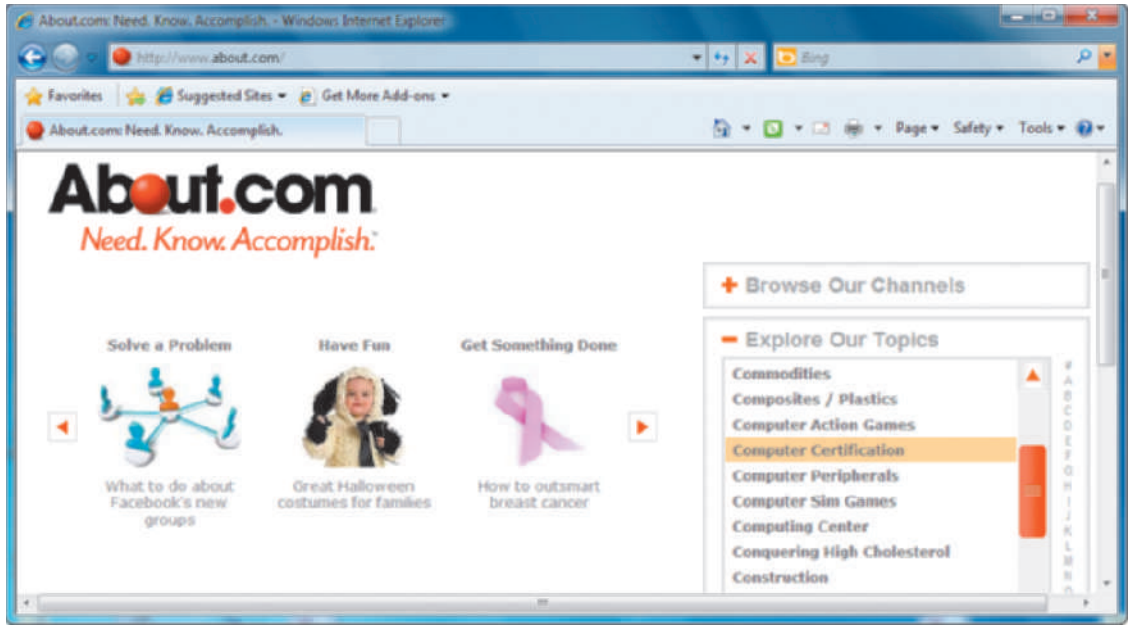


FIGURE 12-40 About.com offers online guides and solutions for everyday questions, including a section on computer certification.

Our digital society is inundated with massive amounts of data. Data mining, clever algorithms, and technical innovation are important, but the most valuable asset is an employee who can solve problems. The IT community has become interested in **critical thinking skills** that can help a person find, organize, analyze, and use the information he or she needs on the job. Many employers now seek critical thinkers who can locate data, identify important facts, and apply their knowledge in real-world decisions.

Many training courses exist for technical skills, but how do you develop your critical thinking skills? The best answer is to practice by performing tasks that resemble actual workplace tasks. As a future systems analyst, you already have an advantage — you know how to develop models, organize data, and recognize patterns. You can also complete the 12 *Ready for a Challenge* exercises at the end of each chapter. These exercises require critical thinking skills, and can help you learn, practice, and apply skills that you can take to the workplace.

Many instructors find that individual and team-based exercises can strengthen critical thinking skills. Examples include games, puzzles, brainstorming, creative problem-solving, decision tables, working with ethical questions, Boolean logic, Venn diagrams, and using cause-and-effect tools such as Pareto charts, X-Y diagrams, and fishbone diagrams, all of which can be found in this textbook.

A QUESTION OF ETHICS

Jamie just completed a routine security audit on the company's information systems, and she found several areas of vulnerability. For example, file permissions have not been updated in some time, no comprehensive password policy exists, and network traffic is not fully encrypted. She noted these areas, among others, in a report to Tamika, her supervisor. The report included specific recommendations to fix the problems.

Tamika responded by saying that budgets are tight right now, and she could not approve Jamie's requests to resolve these issues. As an IT professional, Jamie is very uncomfortable with the risk level, but she has been unable to sway Tamika. When Jamie discussed the situation with her friend, Ethan, he said, "Why worry about it? If it's good enough for Tamika, it should be good enough for you."

What do you think of Ethan's advice, and why? Is this an ethical question? If Jamie still is uncomfortable, what are her options?

Chapter Summary

Systems support and security covers the period from the implementation of an information system until the system no longer is used. A systems analyst's primary involvement with an operational system is to manage and solve user support requests.

Corrective maintenance includes changes to correct errors. Adaptive maintenance satisfies new systems requirements, and perfective maintenance makes the system more efficient. Adaptive and perfective maintenance changes often are called enhancements. Preventive maintenance is performed to avoid future problems.

The typical maintenance process resembles a miniature version of the systems development life cycle. A systems request for maintenance work is submitted and evaluated. If it is accepted, the request is prioritized and scheduled for the IT group. The maintenance team then follows a logical progression of investigation, analysis, design, development, testing, and implementation.

Corrective maintenance projects occur when a user or an IT staff member reports a problem. Standard maintenance procedures usually are followed for relatively minor errors, but work often begins immediately when users report significant errors.

In contrast to corrective maintenance, adaptive, perfective, and preventive maintenance projects always follow the organization's standard maintenance procedures. Adaptive maintenance projects occur in response to user requests for improvements to meet changes in the business or operating environments. The IT staff usually initiates perfective maintenance projects to improve performance or maintainability. Automated program restructuring and reengineering are forms of perfective maintenance. In order to avoid future problems, IT staff performs preventive maintenance, which involves analysis of areas where trouble is likely to occur.

A maintenance team consists of one or more systems analysts and programmers. Systems analysts need the same talents and abilities for maintenance work as they use when developing a new system. Many IT departments are organized into separate new development and maintenance groups where staff members are rotated from one group to the other.

Configuration management is necessary to handle maintenance requests, to manage different versions of the information system, and to distribute documentation changes. Maintenance changes can be implemented as they are completed or a release methodol-

ogy can be used in which all noncritical maintenance changes are collected and implemented simultaneously. A release methodology usually is cost effective and advantageous for users because they do not have to work with a constantly changing system. Systems analysts use functional, allocated, and product baselines as formal reference points to measure system characteristics at a specific time.

System performance measurements include response time, bandwidth, throughput, and turnaround time. Capacity management uses those measurements to forecast what is needed to provide future levels of service and support. Also, CASE tools that include system evaluation and maintenance features can be used during the systems operation, security, and support phase.

Security is a vital part of every computer system. System security is dependent upon a comprehensive security policy that defines how organizational assets are to be protected and how attacks are to be responded to.

Risk management creates a workable security policy by identifying, analyzing, anticipating, and reducing risks to an acceptable level. Because information systems face a wide array of threats and attacks, six separate but interrelated security levels should be analyzed: physical security, network security, application security, file security, user security, and procedural security. Physical security concerns the physical environment, including critical equipment located in a computer room, as well as safeguards for servers and desktops throughout the company. Network security involves encryption techniques, as well as private networks and other protective measures, especially where wireless transmissions are concerned. Application security requires an understanding of services, hardening, application permissions, input validation techniques, software patches and updates, and software logs. File security involves the use of encryption, and permissions, which can be assigned to individual users or to user groups. User security involves identity management techniques, a comprehensive password protection policy, an awareness of social engineering risks, and an effective means of overcoming user resistance. Procedural security involves managerial controls and policies that ensure secure operations.

Data backup and recovery issues include backup media, backup schedules, and retention periods, as well as backup designs such as RAID and Web-based backups.

All information systems eventually become obsolete. The end of a system's economic life usually is signaled by rapidly increasing maintenance or operating costs, the availability of new software or hardware, or new requirements that cannot be achieved easily by the existing system. When a certain point is reached, an information system must be replaced, and the entire systems development life cycle begins again.

Many IT experts predict intense competition in the future, along with economic, political, and social uncertainty. Facing these challenges, top IT priorities will be the safety and security of corporate operations, environmental concerns, and bottom-line TCO.

An IT professional should have a strategic career plan that includes long-term goals and intermediate milestones. An important element of a personal strategic plan is the acquisition of IT credentials and certifications that document specific knowledge and skills. Many IT industry leaders offer certification. In addition to technical ability, other skills, such as critical thinking skills, also are extremely valuable.

Key Terms and Phrases

acceptance *592*
adaptive maintenance *575*
administrator *601*
allocated baseline *584*
applications programmer *579*
archived *583*
asset *590*
attack *592*
automatic update service *602*
availability *590*
avoidance *592*
backup *607*
backup media *607*
backup policy *607*
bandwidth *586*
baseline *584*
benchmark testing *585*
biometric scanning systems *594*
BIOS-level password *595*
boot-level password *595*
business continuity plan (BCP) *609*
capacity planning *587*
certification *611*
change control (CC) *582*
CIA triangle *589*
confidentiality *589*
configuration management (CM) *582*
continuous backup *607*
corrective maintenance *575*
credentials *611*
critical risk *591*
critical thinking skills *612*
database programmer *579*
data replication *609*
denial of service (DOS) *599*
differential backup *607*
disaster recovery plan *607*
distributed denial of service (DDOS) *599*
dumpster diving *606*
encrypted *597*
Encrypting File System (EFS) *603*
enhancement *576*
exploit *591*
fault management *585*
fault tolerant *607*
firewall *599*
full backup *607*
functional baseline *584*
Gbps (gigabits per second) *586*
hardening *601*
help desk *572*
hot site *609*
identity management *604*
IEEE 802.11i *598*
incremental backup *607*
information center (IC) *572*
integrity *590*
Kbps (kilobits per second) *586*
keystroke logger *594*
log *602*
maintenance activities *574*
maintenance expenses *574*
maintenance release *583*
maintenance release methodology *583*
maintenance team *578*
malware *601*
Mbps (megabits per second) *586*
metrics *585*
Microsoft Management Console (MMC) *590*
mitigation *592*
network *597*
network interface *597*
network intrusion detection system (NIDS) *600*
obsolete *609*
offsiting *607*
operational costs *574*
operational security *606*
patches *576*
perfective maintenance *575*
permissions *601*
plain text *597*
port *599*
port scan *599*
power-on password *595*
pretexting *604*
preventive maintenance *575*
private key encryption *597*
private network *599*
privilege escalation attack *603*
procedural security *606*
product baseline *584*
programmer/analyst *579*
public key encryption (PKE) *597*
RAID (redundant array of independent disks) *607*
recovery *607*
remote control software *573*
response time *586*
retention period *608*
risk *591*
risk assessment *590*
risk control *590*
risk identification *590*
risk management *590*
security *589*
security hole *601*
security policy *590*
security token *605*
service *599*
service packs *583*
social engineering *604*
soft skills *611*
software reengineering *576*
superuser *601*
system administrator *578*
systems programmer *579*
tamper-evident cases *595*
test plan *608*
third-party software *602*
threat *590*
throughput *586*
transference *592*
tunnel *599*
turnaround time *587*
unencrypted *597*
uninterruptible power supply (UPS) *595*
Universal Security Slot (USS) *595*
user rights *601*
user training package *572*
version control *583*
virtual private network (VPN) *599*
vulnerability *591*
what-if analysis *587*
Wi-Fi Protected Access (WPA) *598*
Wired Equivalent Privacy (WEP) *598*
WPA2 *598*

Learn It Online

Instructions: To complete the Learn It Online exercises, visit the Management Information Systems CourseMate Web site at **www.cengagebrain.com**, navigate to the resources for this chapter, and click the link for the exercise you want to complete.

1 Chapter Reinforcement

TF, MC, and SA

Click one of the Chapter Reinforcement links for Multiple Choice, True/False, or Short Answer. Answer each question and submit to your instructor.

2 Flash Cards

Click the Flash Cards link and read the instructions. Type 20 (or a number specified by your instructor) in the Number of playing cards text box, type your name in the Enter your Name text box, and then click the Flip Card button. When the flash card is displayed, read the question and then click the ANSWER box arrow to select an answer. Flip through the Flash Cards. If your score is 15 (75%) correct or greater, click Print on the File menu to print your results. If your score is less than 15 (75%) correct, then redo this exercise by clicking the Replay button.

3 Practice Test

Click the Practice Test link. Answer each question, enter your first and last name at the bottom of the page, and then click the Grade Test button. When the graded practice test is displayed on your screen, click Print on the File menu to print a hard copy. Continue to take practice tests until you score 80% or better.

4 Who Wants To Be a Computer Genius?

Click the Computer Genius link. Read the instructions, enter your first and last name at the bottom of the page, and then click the Play button. When your score is displayed, click the PRINT RESULTS link to print a hard copy.

5 Wheel of Terms

Click the Wheel of Terms link. Read the instructions, and then enter your first and last name and your school name. Click the PLAY button. When your score is displayed on the screen, right-click the score and then click Print on the shortcut menu to print a hard copy.

6 Crossword Puzzle Challenge

Click the Crossword Puzzle Challenge link. Read the instructions, and then click the Continue button. Work the crossword puzzle. When you are finished, click the Submit button. When the crossword puzzle is redisplayed, submit it to your instructor.

SCR Associates Case Simulation Session 12: Managing Systems Support and Security

Overview

The SCR Associates case study is a Web-based simulation that allows you to practice your skills in a real-world environment. The case study transports you to SCR's intranet, where you complete 12 work sessions, each aligning with a chapter. As you work on the case, you will receive e-mail and voice mail messages, obtain information from SCR's online libraries, and perform various tasks.

How do I use the case?

- Review the SCR background material in Chapter 1.
- Read the Preview for this session and study the Task List.
- Visit the Management Information Systems CourseMate Web site at **www.cengagebrain.com**, navigate to the **SCR Case Simulation**, and locate the intranet link.
- Enter your name and the password **sad9e**. An opening screen will display the 12 sessions.
- Select this session. Check your e-mail and voice mail carefully, and then work on the tasks.

Preview: Session 12

You assisted your supervisor, Jesse Baker, in various implementation tasks, and the TIMS system is up and running. Now she wants you to focus on system operation, support, and security tasks. Specifically, she wants you to work on a help desk, version control, configuration management, capacity planning, and system security issues. She also wants you to create a checklist that will help SCR know when the TIMS system is reaching the end of its useful life.

Task List

1. *Jesse wants a recommendation about creating an SCR help desk. She said that I can find lots of information about help desks on the Internet.*
2. *At our meeting, Jesse asked me how SCR should manage the TIMS system in the future. I need to search the Internet to learn more about version control, configuration management, and capacity planning, and send her the results of my research.*
3. *Another important issue: Security! Jesse wants my thoughts on how SCR should manage IT security. She wants me to consider all six levels, and prepare an outline for a corporate security policy.*
4. *Jesse says that no one likes surprises or problems. She wants me to draft a checklist that SCR can use to detect TIMS obsolescence as early as possible. She also said that I might be receiving some interesting news very soon. Wonder what that's about?*

FIGURE 12-41 Task list: Session 12.

Chapter Exercises

Review Questions

1. Describe the four classifications of maintenance and provide an example of each type.
2. Why are newly hired systems analysts often assigned to maintenance projects?
3. What is configuration management and why is it important?
4. What is the purpose of capacity planning? How is what-if analysis used in capacity planning?
5. What is a release methodology and what are the pros and cons of this approach? What is the purpose of version control?
6. Define the following terms: response time, bandwidth, throughput, and turnaround time. How are the terms related?
7. What are some key issues that you must address when considering data backup and recovery?
8. Explain the concept of risk management, including risk identification, assessment, and control.
9. What are the six security levels? Name at least three specific issues that apply to each level. Also provide three examples of threat categories, attacker profiles, and types of attacks.
10. List six indications that an information system is approaching obsolescence.

Discussion Topics

1. Assume that your company uses a release methodology for its sales system. The current version is 4.5. Decide whether each of the following changes would justify a version 5.0 release, or be included in a version 4.6 update: (a) Add a new report, (b) add a Web interface, (c) add data validation checks, (d) add an interface to the marketing system, and (e) change the user interface.
2. The four types of IT system maintenance also apply to other industries. Suppose you were in charge of aircraft maintenance for a small airline. What would be an example of each type of maintenance — corrective, adaptive, perfective, and preventive?
3. An IT manager assigns programmers and systems analysts to maintenance projects if they have less than two years of experience or if they received an average or lower rating in their last performance evaluation. Do you agree with this practice?
4. What are the most important security issues facing companies today? Have these changed in the last five years, and will they continue to change? How should companies prepare themselves for security threats and problems in the future?

Projects

1. Using the Internet, locate a software package designed to automate version control. List the key features and describe your findings in a brief memo.
2. Develop a process for managing change requests and design a form to handle a generic change request. The process should include a contingency plan for changes that must be resolved immediately.
3. Visit the IT department at your school or at a local company and find out whether performance measurements are used. Write a brief report describing your findings.
4. Explain how to use the Goal Seek feature in Microsoft Excel, and create a worksheet that demonstrates this feature.

Apply Your Knowledge

The Apply Your Knowledge section contains four mini-cases. Each case describes a situation, explains your role in the case, and asks you to respond to questions. You can answer the questions by applying knowledge you learned in the chapter.

1 Premium Publishers

Situation:

Premium Publishers is a small publishing firm that specializes in reprinting classic literature. A year ago the IT staff developed a Web-based order entry system. The system has performed well, but the company would like to add more features and improve performance. So far, most of the maintenance has involved correcting minor errors.

1. What types of maintenance have the IT staff performed? What types of maintenance will they perform if the existing system is retained?
2. If new features are added, what methodology should the IT staff use to add new functions and enhancements?
3. What IT security measures should the firm adopt? Prepare a security checklist, and be sure to consider all six security levels.
4. Even though the new system is only a year old, e-commerce changes constantly. At what point should Premium Publishers consider replacing the Web-based system with a new system, and why?

2 Oceanside Furniture

Situation:

Oceanside Furniture produces indoor and outdoor wicker furniture. The company grew from one store in 2007 to eight locations today. Two years ago, the company's IT department developed an inventory control system to keep track of products and reorder out-of-stock items. The new system was well received by users, and inventory problems have decreased significantly. Since the inventory system became operational, however, users steadily have requested increased functionality and changes in screen forms and reports.

1. Should Oceanside have a specific process to manage future changes and enhancements? What should it be?
2. What about version control? Should Oceanside institute a maintenance release methodology? Why or why not?
3. Suppose that you had to assign specific IT staff members to maintain the inventory control system. How would you accomplish the task? Describe your strategy in a brief memo.
4. What should Oceanside watch for to detect possible obsolescence in the future? Develop a checklist with specific examples that Oceanside management could use.

3 Robin Hood Associates

Situation:

Robin Hood Associates is an IT consulting firm that develops new systems and maintains older systems for its clients. Robin Hood recently was awarded a contract to correct problems with an existing system. The system is three years old, and the consulting firm that initially designed the system did a poor job of documentation. The data dictionary, user manuals, and other reference material never have been updated, and no process exists for version control.

1. As one of the Robin Hood team members, how should you proceed? What steps would you take, and what would be your priorities?
2. Are CASE tools available that you could use on this assignment? What are they?
3. What advice would you give to the client regarding capacity planning for the future?
4. What steps should the client take to ensure that the system is secure? Prepare a checklist with at least 15 security items that the client should evaluate and monitor. Be sure to consider all six security levels.

4 Economy Travel

Situation:

Economy Travel specializes in personalized travel packages at popular prices, and the firm operates 12 offices in major U.S. cities. A key selling point is the firm's client management database, which includes preferences such as airline seating choices and favorite hotels. Economy Travel purchased the client management software as an off-the-shelf vendor package and modified the program to meet the company's needs. The package has been operational for one year and has performed well. Economy Travel, however, is in the process of expanding its operation to include six additional locations. You have been called in as a consultant to help the company make some decisions about IT support.

1. What performance and workload measurement issues should the company consider at the present time?
2. What capacity planning issues should the company consider at the present time?
3. Should the company establish a system baseline before the integration of the six new sites? Explain your answer.
4. As an IT consultant, you must understand the client's business. From that perspective, consider the impact of the Internet on the travel agency business. Investigate this topic using the Internet and other sources of information, and decide what issues to discuss with Economy Travel.

Case Studies

Case studies allow you to practice specific skills learned in the chapter. Each chapter contains several case studies that continue throughout the textbook, and a chapter capstone case.

New Century Health Clinic

New Century Health Clinic offers preventive medicine and traditional medical care. In your role as an IT consultant, you will help New Century develop a new information system.

Background

You implemented the new system at New Century Health Clinic successfully, and the staff has used the system for nearly four months. New Century is pleased with the improvements in efficiency, office productivity, and patient satisfaction.

Some problems have surfaced, however. The office staff members call you almost daily to request assistance and suggest changes in certain reports and forms. You try to be helpful, but now you are busy with a major project for a local distributor of exercise equipment. Actually, your contract with New Century required you to provide support only during the first three months of operation. Anita Davenport, New Century's office manager, reported that the system seems to slow down at certain times during the day, making it difficult for the staff to keep up with its workload. Also, you increasingly are concerned about system security. A recent article in the local newspaper described an incident where a disgruntled former employee was about to break into the computer system and destroy or alter data.

Assignments

1. You are willing to charge a lower rate for ongoing support services because you designed the system. You want New Century to use a specific procedure for requesting assistance and changes, however, so that you can plan your activities efficiently. Prepare a complete, written procedure for New Century Health Clinic maintenance change requests. Include appropriate forms with your procedure.
2. What could be causing the periodic slowdowns at New Century? If a problem does exist, which performance and workload measures would you monitor to pinpoint the problem?
3. At the end of the systems analysis phase, you studied the economic feasibility of the system and estimated the future costs and benefits. Now that the system is operational, should those costs and benefits be monitored? Why or why not?
4. You decide to prepare a security checklist for New Century. Prepare a list of security issues that the firm should evaluate and monitor. Be sure to organize the items into categories that match the six security levels.

PERSONAL TRAINER, INC.

Personal Trainer, Inc., owns and operates fitness centers in a dozen Midwestern cities. The centers have done well, and the company is planning an international expansion by opening a new "supercenter" in the Toronto area. Personal Trainer's president, Cassia Umi, hired an IT consultant, Susan Park, to help develop an information system for the new facility. During the project, Susan will work closely with Gray Lewis, who will manage the new operation.

Background

System changeover and data conversion were successful for the new Personal Trainer system. The post-implementation evaluation indicated that users were pleased with the system. The evaluation also confirmed that the system was operating properly. Several users commented, however, that system response seemed slow. Susan Park, the project consultant,

wants to meet with you to discuss operation, maintenance, and security issues affecting the new system.

Assignments

1. What might be causing the slow response time? Prepare a brief memo explaining system performance and workload measurement, using nontechnical language that Personal Trainer users can understand easily.
2. Personal Trainer's top management asked you to provide ongoing maintenance for the new system. In order to avoid any misunderstanding, you want to provide a brief description of the various types of maintenance. Prepare a brief memo that does this, and include at least two realistic examples of each type of maintenance.
3. Although the system has been operational for a short time, users already have submitted several requests for enhancements and noncritical changes. Should Personal Trainer use a maintenance release methodology to handle the requests? Why or why not?
4. What are the main security issues that Personal Trainer should address? Prepare a memo that lists the primary concerns and offers a specific recommendation for dealing with each issue.

TARHEEL INDUSTRIES

Tarheel Industries is a medium-sized sporting goods manufacturer located in North Carolina. Tarheel's online production support system was developed in-house and was implemented two months ago. The system runs 24 hours a day in Tarheel's three manufacturing facilities.

Background

Last Monday morning, the production support system developed a problem. When a screen display for certain parts was requested, the displayed values were garbled.

When she was alerted to the situation, Marsha Stryker, Tarheel's IT manager, immediately assigned a systems analyst to investigate the problem. Marsha instructed the analyst, Eric Wu, to resolve the problem and get the system up and running as soon as possible. Eric previously worked on two small maintenance projects for the production control system, so he was somewhat familiar with the application.

Eric worked all day on the problem, and by 6:30 p.m., he developed and implemented a fix. After verifying that the production support system was capable of producing correct part displays, Eric went home. Early the following morning, Marsha called Eric and two other members of the applications maintenance group to a meeting in her office, where she briefed them on a new adaptive maintenance project for another high-priority system. She asked them to begin work on the new project immediately.

Several nights later, the production control system crashed shortly after midnight. Every time the system was reactivated, it crashed again. Finally, around 2:30 a.m., all production lines were shut down and third-shift production workers were sent home. The production support system finally was corrected and full production was restored the following day, but by that time, Tarheel Industries had incurred thousands of dollars in lost production costs. The cause of the production support system crash was identified as a side effect of the fix that Eric made to the system.

Assignments

1. Is the second production support system failure entirely unexpected?
2. Who is most to blame for the second system failure?
3. What might Marsha have done differently to avoid the situation? What might Eric have done differently?
4. Outline a new set of maintenance procedures that will help Tarheel Industries avoid such problems in the future.

MILLS IMPORTS

Mills Imports is a successful importer of gourmet coffees, cheeses, and specialty foods from around the world. Mills Imports recently developed and implemented an online sales information system.

Background

Using a client/server design, the PCs in each of the firm's 12 retail stores were networked with a server located in the sales support center at the main office. Salespeople in the retail stores use the customer sales information system to record sales transactions; to open, close, or query customer accounts; and to print sales receipts, daily sales reports by salesperson, and daily sales reports by merchandise code. The sales support staff uses the system to query customer accounts and print various daily, weekly, and monthly reports.

When the customer sales system was implemented, the IT department conducted extensive training for the salespeople and the sales support center staff. One member of the systems development team also prepared a user manual, but users are familiar with the system so the manual rarely is used.

Two weeks ago, Mills opened two additional stores and hired six new sales representatives. A manager gave the user manual to the new sales representatives and asked them to read it and experiment with the system. Now, salespeople in both new stores are having major problems using the sales system. When a representative from the main office visited the stores to investigate the problem, she discovered that the new people could not understand the user manual. When she asked for examples of confusing instructions, several salespeople pointed to the following examples:

- *Obtaining the authorization of the store manager on Form RBK-23 is required before the system can activate a customer charge account.*
- *Care should be exercised to ensure that the BACKSPACE key is not pressed when the key on the numeric keypad with a left-facing arrow is the appropriate choice to accomplish nondestructive backspacing.*
- *To prevent report generation interruption, the existence of sufficient paper stock should be verified before any option that requires printing is selected. If not, the option must be reselected.*
- *The F2 key should be pressed in the event that a display of valid merchandise codes is required. That same key terminates the display.*

Assignments

1. What could Mills Imports have done to avoid the situation?
2. Should the sales support staff ask the IT department to rewrite the user manual as a maintenance project, or should they request a training session for the new salespeople? Can you offer any other suggestions?
3. Rewrite the user manual instructions so they are clear and understandable for new users. What steps might you take to ensure the accuracy of the new user manual instructions?
4. In the process of rewriting the user manual instructions, you discover that some of the instructions were not changed to reflect system maintenance and upgrade activities. A request form on the firm's intranet, for example, has replaced Form RBK-23. Mills also has phased out printed reports in favor of online reports, which users can view by entering a username and password. Rewrite the user manual instructions to reflect the changes.

CHAPTER CAPSTONE CASE: SoftWear, Limited

SoftWear, Limited (SWL), is a continuing case study that illustrates the knowledge and skills described in each chapter. In this case study, the student acts as a member of the SWL systems development team and performs various tasks.

Background

In mid-December 2012, five months after the post-implementation evaluation, the payroll package and the ESIP system were operating successfully and users seemed satisfied with both systems.

During that time, users requested minor changes in reports and screen displays, which the IT staff handled easily. Jane Rossman, manager of applications, continued to assign a mixture of new systems and maintenance tasks to the IT team, and the members indicated that they enjoyed the variety and challenge of both types of work.

Debra Williams, the payroll clerk who prints the ESIP checks, reported the only operational problem. She could not load and align the special check stock in the printer correctly. Becky Evans visited Debra to study the situation and then wrote a specific procedure to solve the problem.

No overtime had been paid in the payroll department since the new system was implemented, and errors in payroll deductions had stopped. Michael Jeremy, SWL's vice president of finance, who initiated the payroll and ESIP projects, is very pleased with the system's operation and output. He recently visited an IT department staff meeting to congratulate the entire group personally.

Some requests for enhancements also occurred. Mike Feiner recently submitted a systems request for the ESIP system to produce an annual employee benefits statement with the current value of all savings plan deductions, plus information on insurance coverage and other benefits data. Mike also indicated that the company would offer several new ESIP choices, including various mutual funds.

In mid-December, Pacific Software announced the latest release of its payroll package. The new version supported full integration of all payroll and human resources functions and data. Ann Hon, director of information systems, was interested in the announcement because she knew that Rob King, SWL's vice president of human resources, wanted a human resources information system (HRIS) to support SWL's long-term needs. At Ann's request, Jane Rossman assigned Becky Evans to analyze the new payroll package to determine if SWL could implement the latest version as a company-wide client/server application.

Becky began the preliminary investigation by reviewing the current system and meeting with Mike Feiner to learn more about the new ESIP options. Next, she met with Marty Hoctor, a representative from Pacific Software, to review the features of the new release. After describing the new software, Marty mentioned that a large Midwestern retail chain recently implemented the package, and he invited Becky to contact Sean Valine, director of IT at that company, to discuss the new release. Becky spoke with Sean, and he agreed to e-mail her a summary of comments that users had made about the new software.

Becky completed her preliminary investigation, including a cost-benefit analysis, and worked with Jane Rossman and Ann Hon to prepare a report and presentation to SWL's newly formed systems review committee, which was created at Ann's suggestion. In their presentation, the IT team recommended that SWL upgrade to the new release of the payroll package and build a client/server application for all of SWL's payroll and personnel functions, including the ESIP system. They also suggested that a team of IT and human resources people get together to study preliminary economic, technical, and operational factors involved in a human resources information system and report back to the systems review committee. They pointed out that if the project was approved, the same team could handle the systems development using JAD or RAD techniques. After the presentation, the committee approved the

CHAPTER CAPSTONE CASE: SoftWear, Limited (continued)

request and Ann called an IT department staff meeting for the next morning to start planning the systems analysis phase.

During the meeting, Ann and Jane thanked the entire department for its efforts on the payroll and ESIP projects. Ann pointed out that although the payroll package and the ESIP system support SWL's current needs, the business environment changes rapidly and a successful, growing company must investigate new information management technology constantly. At this point, the systems development life cycle for SWL begins again.

SWL Team Tasks

1. Now that the new ESIP system is operational, Jane Rossman wants you to track system performance using various measurements. At a minimum, she expects you to monitor operational costs, maintenance frequency, technical issues, and user satisfaction. You can add other items if you choose. Write a proposal for Jane that lists each factor you will measure, and make sure that you explain why the item is important and how you plan to obtain the information.
2. Jane assigned you to the SWL team that will study the feasibility of a human resources information system (HRIS). Using the Internet, identify several commercial packages and the names of firms or consultants who specialize in HRIS implementation. Write a brief memo to Jane with your findings.
3. Jane wants you to prepare a security audit procedure for SWL. Specifically, she wants you to prepare a checklist of security issues that need to be evaluated and rated. She said to consider all six security levels, and to include as many specific items as possible that should be assessed.
4. As Ann Hon pointed out in the last meeting, the business environment changes rapidly and a successful, growing company like SWL must investigate new information management technology constantly. Ann has asked you to describe trends in software and hardware that might affect SWL's future IT plans. Perform research on the Internet to identify several technology issues that might represent potential problems or opportunities for SWL, and present the results in a memo to Ann.

Manage the SWL Project

You have been asked to manage SWL's new information system project. One of your most important activities will be to identify project tasks and determine when they will be performed. Before you begin, you should review the SWL case in this chapter. Then list and analyze the tasks, as follows:

LIST THE TASKS Start by listing and numbering at least 10 tasks that the SWL team needs to perform to fulfill the objectives of this chapter. Your list can include SWL Team Tasks and any other tasks that are described in this chapter. For example, Task 3 might be to Perform necessary corrective maintenance and Task 6 might be to Identify perfective maintenance tasks.

ANALYZE THE TASKS Now study the tasks to determine the order in which they should be performed. First identify all concurrent tasks, which are not dependent on other tasks. In the example shown in Figure 12-42, Tasks 1, 2, 3, 4, and 5 are concurrent tasks, and could begin at the same time if resources were available.

CHAPTER CAPSTONE CASE: SoftWear, Limited (continued)

Other tasks are called dependent tasks, because they cannot be performed until one or more earlier tasks have been completed. For each dependent task, you must identify specific tasks that need to be completed before this task can begin. For example, you would to perform any necessary corrective maintenance before you could identify perfective maintenance tasks, so Task 6 cannot begin until Task 3 is completed, as Figure 12-42 shows.

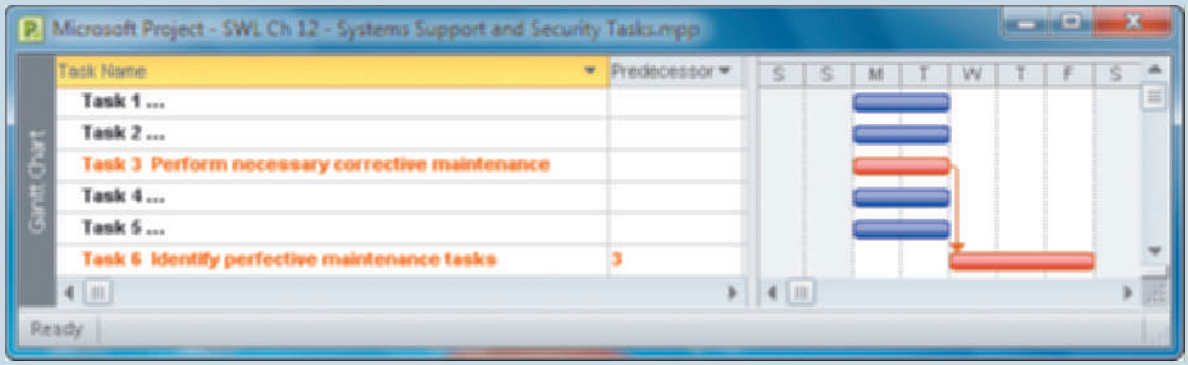


FIGURE 12-42 SWL Tasks 1, 2, 3, 4, and 5 are concurrent tasks that could be performed at the same time. Task 6 is a dependent task that cannot be performed until Task 3 has been completed.

Chapter 3 describes project management tools, techniques, and software. To learn more, you can use the Features section on your Student Study Tool CD-ROM, or visit the Management Information Systems CourseMate Web site at **www.cengagebrain.com** and locate the project management resources library for this book. On the Web, Microsoft offers demo versions, training, and tips for using Project 2010. You also can visit the OpenWorkbench.org site to learn more about this free, open-source software.

Ready for a Challenge?

In additional to technical skills, IT professionals need critical thinking skills such as perception, organization, analysis, problem-solving, and decision-making. The Ready for a Challenge feature can help you learn, practice, and apply critical thinking skills that you can take to the workplace.

Your team leader wants to develop a standard method for rating and ranking maintenance requests for the new C^3 system. The idea is to develop some type of grid that could suggest priorities based on the type of maintenance requested and the potential impact on operations. When you review your notes from your systems analysis textbook, you realize that you used a similar approach when you created a risk matrix in Chapter 3, developed an evaluation model in Chapter 7, and selected a changeover method in Chapter 11.

The team leader also wants to test IT security levels with a simulated attack, something like a fire drill. The planned exercise would include realistic threats that will allow the team to evaluate responses and security procedures.

Practice Tasks

Before you begin, review different techniques for showing multifactor grids. Also review the material on user support and types of maintenance. Then complete these tasks:

A. Develop the maintenance request grid, using the factors listed and any others you want to include. The design should enable requests to be rated or ranked, and the style is not important, as it will be refined later.
B. Draft a plan for the simulated attacks on IT security. Include at least five types of attacks. For each attack, provide an example and suggest a response or action that should be taken to counter the attack.

After you complete the Practice Tasks, to check your work and view sample answers, visit the Management Information Systems CourseMate Web site at **www.cengagebrain.com**, navigate to the resources for this chapter, and locate Ready for a Challenge?.

The Challenge

Your initial design was good, but the team leader wants you to try another approach. She put these questions to you: "Should corrective maintenance get a higher priority than other types of maintenance? Why or why not? Should cost-benefit issues be considered? If so, how would this be done?"

Also, your security plan was good, but did not go far enough. The team leader wants you to include at least five more types of attacks, with examples and suggested responses.

Challenge Tasks

A. Consider the team leader's questions carefully. When you reply, include a revised grid design as needed.
B. Revise the simulated attack plan by including five more types of attacks, with examples and suggested responses.