Systems Analysis and Design 11th Edition

Managing SystemsSupport and Security

Introduction

- Systems support and security phase begins when a system becomes operational
  - Continues until the system reaches the end of its life
- After delivering the system, the IT team focuses on support and maintenance tasks
  - Concerns in managing systems support and security
    - User expectations
    - System performance
    - Security requirements

User Support

- **User Training**
  - IT Department may develop a **user training package**
  - Training users about system changes is similar to initial training
  - Objective – To show users how the system can help them perform their jobs
- **Help** or **Service Desks**: Provide support and guidance

User Support (Cont. 1)

- Objectives
  - To show people how to use system resources more effectively and provide answers to technical or operational questions
  - To make users more productive by teaching them how to meet their own information needs
- Boost their productivity using remote control software
  - **Remote control software**: Allows IT staff to take over a user's workstation and provide support and troubleshooting

Mark Bowden/Getty Images

Figure 12-2 A help desk, also called a service desk, provides support to system users.

User Support (Cont. 2)

- **Outsourcing Issues**
  - Offshore call centers can trim expenses and free up valuable human resources for product development
  - Customers may shop elsewhere if the quality of tech support decreases
  - Critical factors
    - Phone wait times
    - Performance of support staff
    - Online support tools

Maintenance Tasks

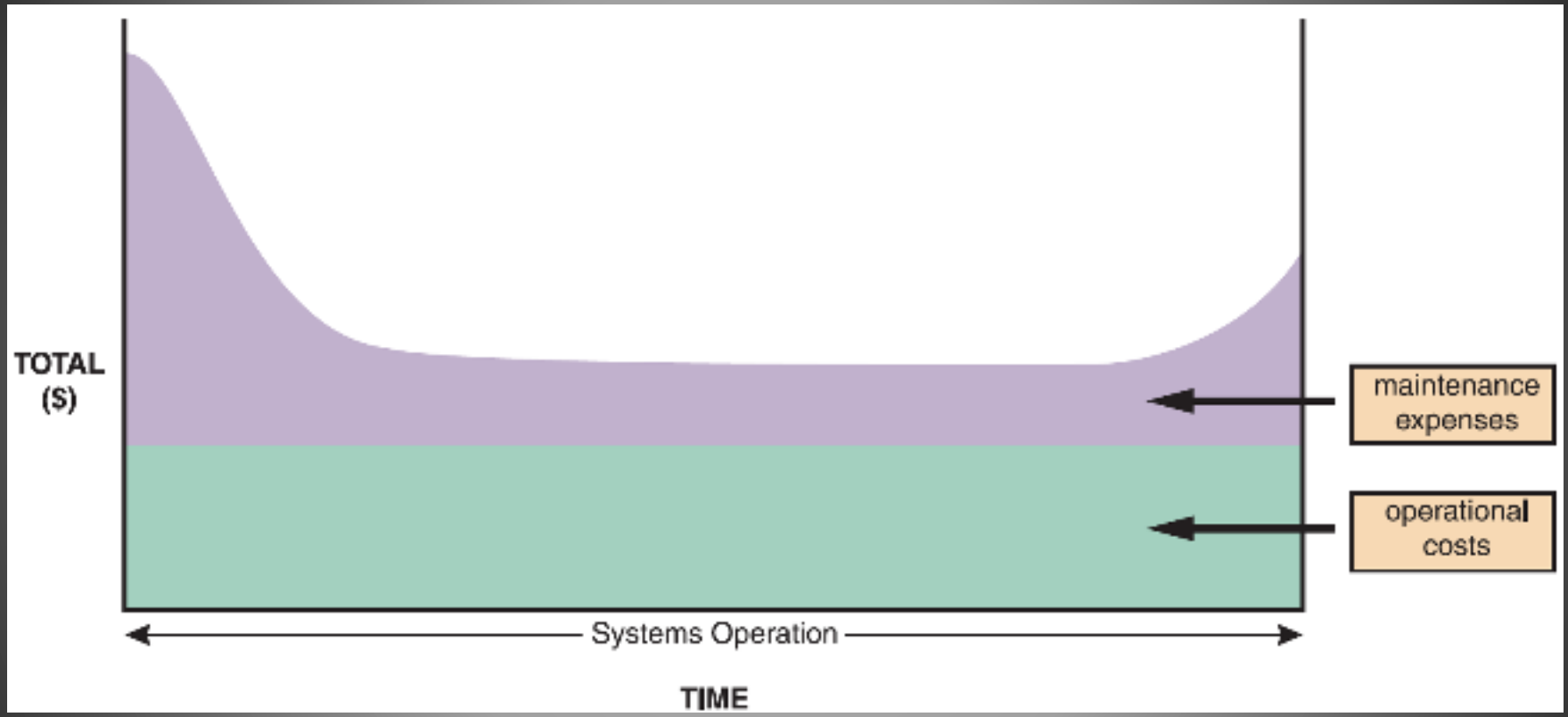

Figure 12-3 The total cost of operating an information system includes operational and maintenance costs. Operational costs (green) are relatively constant, while maintenance costs (purple) vary over time.

Maintenance Tasks (Cont. 1)

	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

maintenance expenses

operational costs

Figure 12-5 Information systems maintenance depends on the type of maintenance and the age of the system.

Maintenance Tasks (Cont. 2)

- **Corrective Maintenance**
  - Diagnoses and corrects errors in an operational system
  - Standard procedures are set for minor errors
  - Worst-case situation is a system failure
    - Requires a **patch**
    - When the system is operational again, the maintenance team determines the cause, analyzes the problem, and designs a permanent solution

Maintenance Tasks (Cont. 3)

PRIORITY	IMPACT	TIME FRAME
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 12-6 This three-level ranking framework for IT support considers potential impact and response urgency.

Maintenance Tasks (Cont. 4)

- **Adaptive Maintenance**
  - Adds **enhancements** to an operational system and makes the system easier to use
  - Procedure for minor adaptive maintenance is similar to routine corrective maintenance
    - Users submit requests that are evaluated and prioritized by the systems committee
  - Can be more difficult than new systems development
    - Enhancements must work within the constraints of an existing system

Maintenance Tasks (Cont. 5)

- **Perfective Maintenance**
  - Changing an operational system to make it more efficient, reliable, and maintainable
  - Cost-effective during the middle of the system's operational life
  - Performed using software reengineering
    - **Software reengineering**: Uses analytical techniques to identify potential quality and performance improvements in an information system
  - The more a program changes, the more likely it is to become inefficient and difficult to maintain

Maintenance Tasks (Cont. 6)

- **Preventive Maintenance**
  - Requires analysis of areas where trouble is likely to occur
  - IT department initiates preventive maintenance
  - Results in:
    - Increased user satisfaction
    - Decreased downtime
    - Reduced TCO
  - Competes for IT resources along with other projects

System Performance Management

- **Fault Management**
  - Includes monitoring the system for signs of trouble, logging all system failures, diagnosing the problem, and applying corrective action

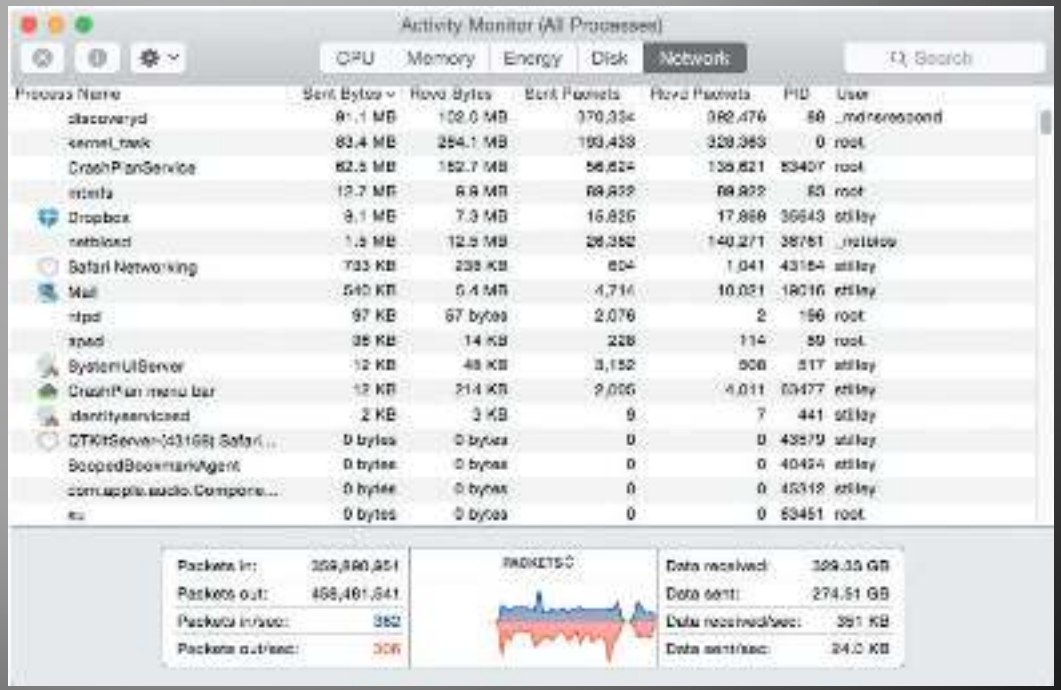

Figure 12-14 The Activity Monitor application on Apple's Mac OS X displays CPU, memory, energy, disk, and network activity of all running applications in real time.
Source: Apple

System Performance Management
(Cont. 1)

- **Performance and Workload Measurement**
  - System performance is measured using **benchmark testing** and **metrics**
  - **Response time**: Overall time between a request for system activity and the delivery of the response
  - Bandwidth and **throughput**
    - Can be measured in Kbps (kilobits per second), Mbps (megabits per second), and Gbps (gigabits per second)
  - Examples of standards of metrics
    - Arrivals – Number of items that appear on a device during a given observation time
    - Busy – Time that a given resource is unavailable

System Performance Management
(Cont. 2)

- Queue length – Number of requests pending for a service
- **Turnaround time**: Applies to centralized batch processing operations
  - Measures the time between submitting a request for information and the fulfillment of the request
  - Used to measure the quality of IT services
  - Management uses current performance and workload data as input for the capacity planning process

System Performance Management
(Cont. 3)

- **Capacity Planning**
  - Monitors current activity and performance levels
  - Anticipates future activity and forecasts resources required to provide desired levels of service
  - Uses what-if analysis
    - **What-if analysis**: Varies one or more elements to study their effect on other elements
  - Requires:
    - Detailed information
    - An accurate forecast of future business activities
  - Objective – To develop contingency plans based on input from users and management

System Performance Management

(Cont. 4)

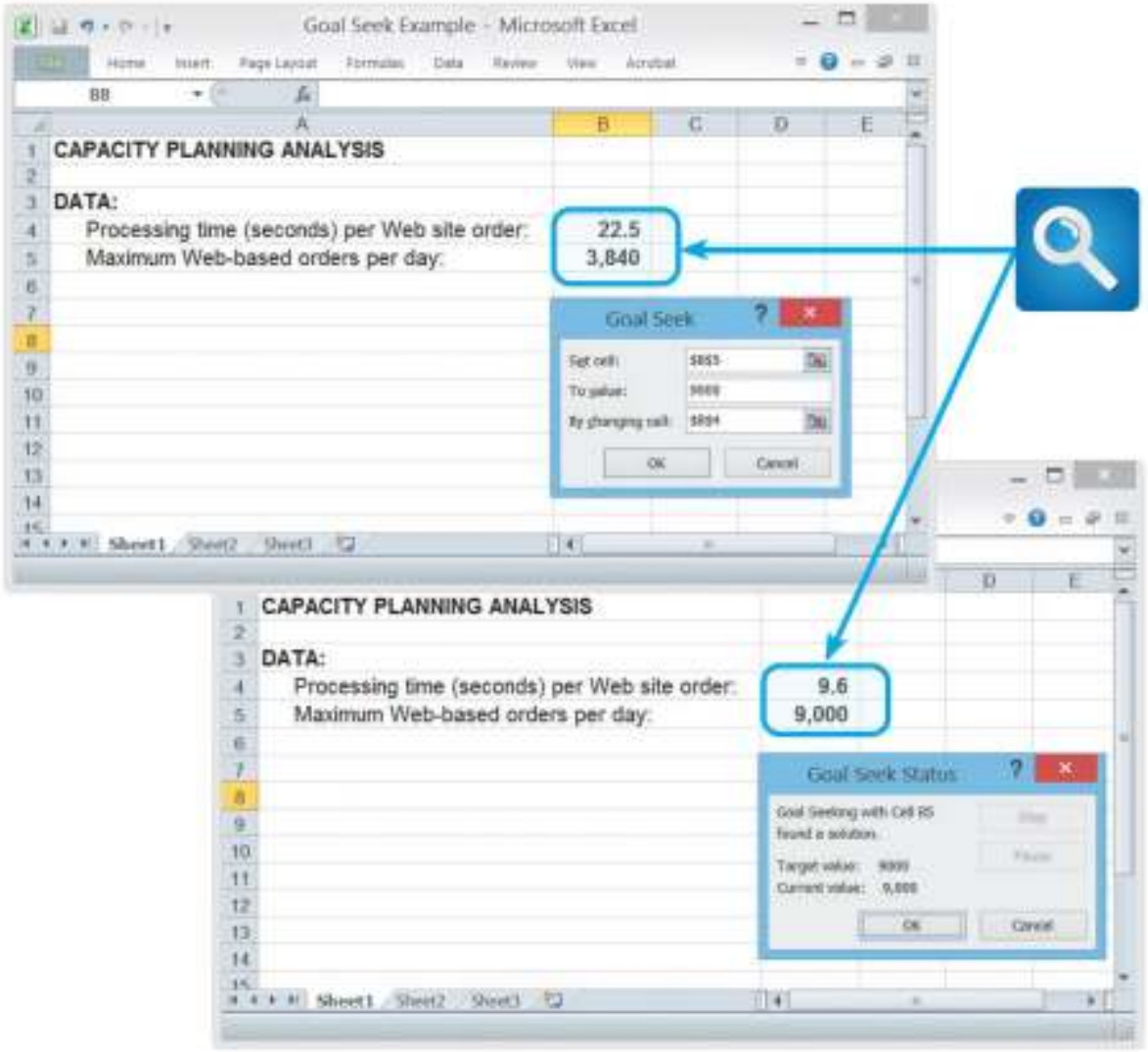

Figure 12-16 In this Goal Seek example, the user wants to know the effect on processing time if the number of daily transactions increases from 3,840 to 9,000.

System Performance Management
(Cont. 5)

- **System Maintenance Tools**
  - Many CASE tools include system evaluation and maintenance features
  - Spreadsheet and presentation software can be used to calculate trends, perform what-if analyses, and create charts and graphs

System Security Overview

- Security is a vital part of every computer system
- **System Security Concepts**
  - **CIA triangle**: Shows the main elements of system security
    - Elements are used to develop a security policy

Figure 12-18 System security must provide information confidentiality, integrity, and availability (CIA).

System Security Overview (Cont. 1)

- **Risk Management:** Involves:
  - **Risk identification**
    - List and classify **assets** and analyze possible **threats**
    - Identify **vulnerabilities** and how they might be **exploited**
  - **Risk assessment**
    - Risks need to be calculated and prioritized
  - **Risk control**
    - Strategies – **Avoidance**, **mitigation**, **transference**, and **acceptance**

Figure 12-19 Risk management requires continuous risk identification, assessment, and control.

System Security Overview (Cont. 2)

THREAT CATEGORY	EXAMPLE
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 website logo, or destroys CEO's hard drive physically or electronically.

Figure 12-20 System threats can be grouped into several broad categories.

System Security Overview (Cont. 3)

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 websites.	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 12-21 IT security professionals have names for various types of attackers.

System Security Overview (Cont. 4)

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.
Dumpster diving	Attacker scours the trash for valuable information that can be used to compromise the system.
Mail bombing	Enormous volumes of email are sent to a target address.
Malicious code	Attacker sends infected email 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.

Figure 12-22 Attacks can take many forms, as this table shows. IT security managers must be able to detect these attacks and respond with suitable countermeasures.

System Security Overview (Cont. 5)

ATTACK	EXAMPLES
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.
Phishing	False DNS (Domain Name Server) information steers the user to the attacker's website. 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.
Privilege escalation	Employee tricks a computer into raising his or her account to the administrator level.

Figure 12-22 Attacks can take many forms, as this table shows. IT security managers must be able to detect these attacks and respond with suitable countermeasures.

System Security Overview (Cont. 6)

ATTACK	EXAMPLES
Sniffing	Network traffic is intercepted and scanned for valuable information.
Social engineering	An attacker calls the service desk posing as a legitimate user and requests that his or her password be changed.
Spam	Unwanted, useless email is sent continuously to business email 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 12-22 Attacks can take many forms, as this table shows. IT security managers must be able to detect these attacks and respond with suitable countermeasures.

Backup and Recovery

- **Backup Policies**
  - **Backup media**: Includes tape, hard drives optical and online storage
    - **Offsiting**: Storing backup away from the business location
    - Cloud-based storage is growing rapidly
  - Types - **Full**, **differential**, **incremental**, and **continuous**
  - **Retention periods**: Backups are stored for a specific time beyond which they are either destroyed or reused

Backup and Recovery (Cont. 1)

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 12-34 Comparison of full, differential, incremental, and continuous backup methods.

Backup and Recovery (Cont. 2)

- **Business Continuity Issues**
  - A disaster recovery plan should be created along with a test plan
    - Often part of a business continuity plan (BCP)
      - **BCP**: Defines how critical business functions can continue during a major disruption
      - Specifies the use of a **hot site**, which requires **data replication**