ISYS2110
Analysis and Design of Web Information Systems

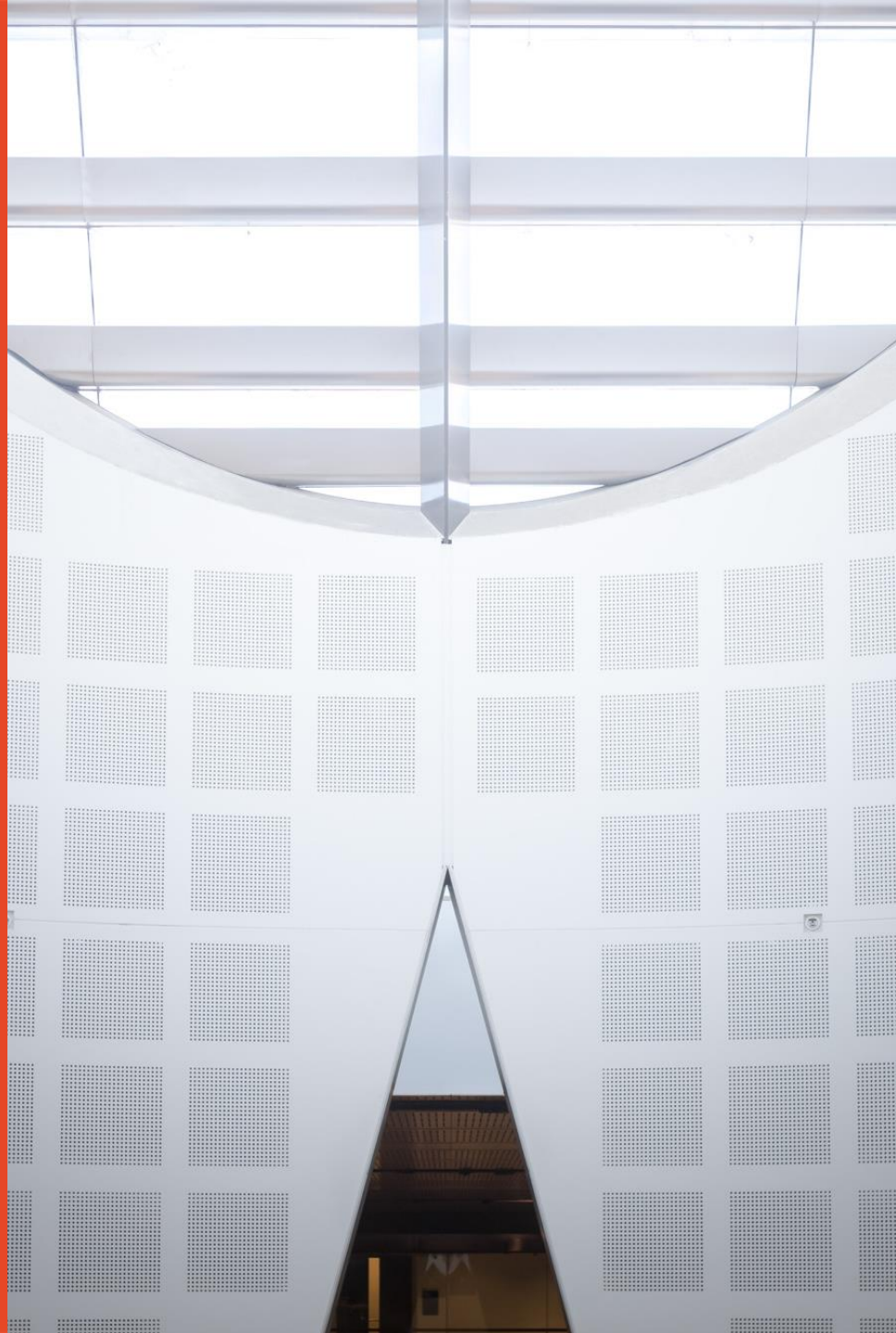
Lecture 12

Documentation & Systems Support

Semester 1, 2018

Dr Rabiul Hasan

THE UNIVERSITY OF SYDNEY



Recapture From Lecture 11

What we have covered on the topic: Systems Implementation

- Implementation
- Testing
- Training

What Will We Do Today ?

- Lecture
  - Documentation
  - System support (User support, system maintenance, system performance, and system security)
  - Code of ethics

- Class activities
  - Critical Thinking / No Problem Solving Today
  - https://padlet.com
  - https://answergarden.ch

- Tutorial: ?
- Assessment ?
- Announcement (if any):

Learning Objectives

- Explain the documentation, systems support and security phase
- Define the four types of maintenance
- Explain various techniques for managing systems maintenance and support
- Describe backup and disaster recovery
- Assess future challenges and opportunities for IT professionals

Documentation

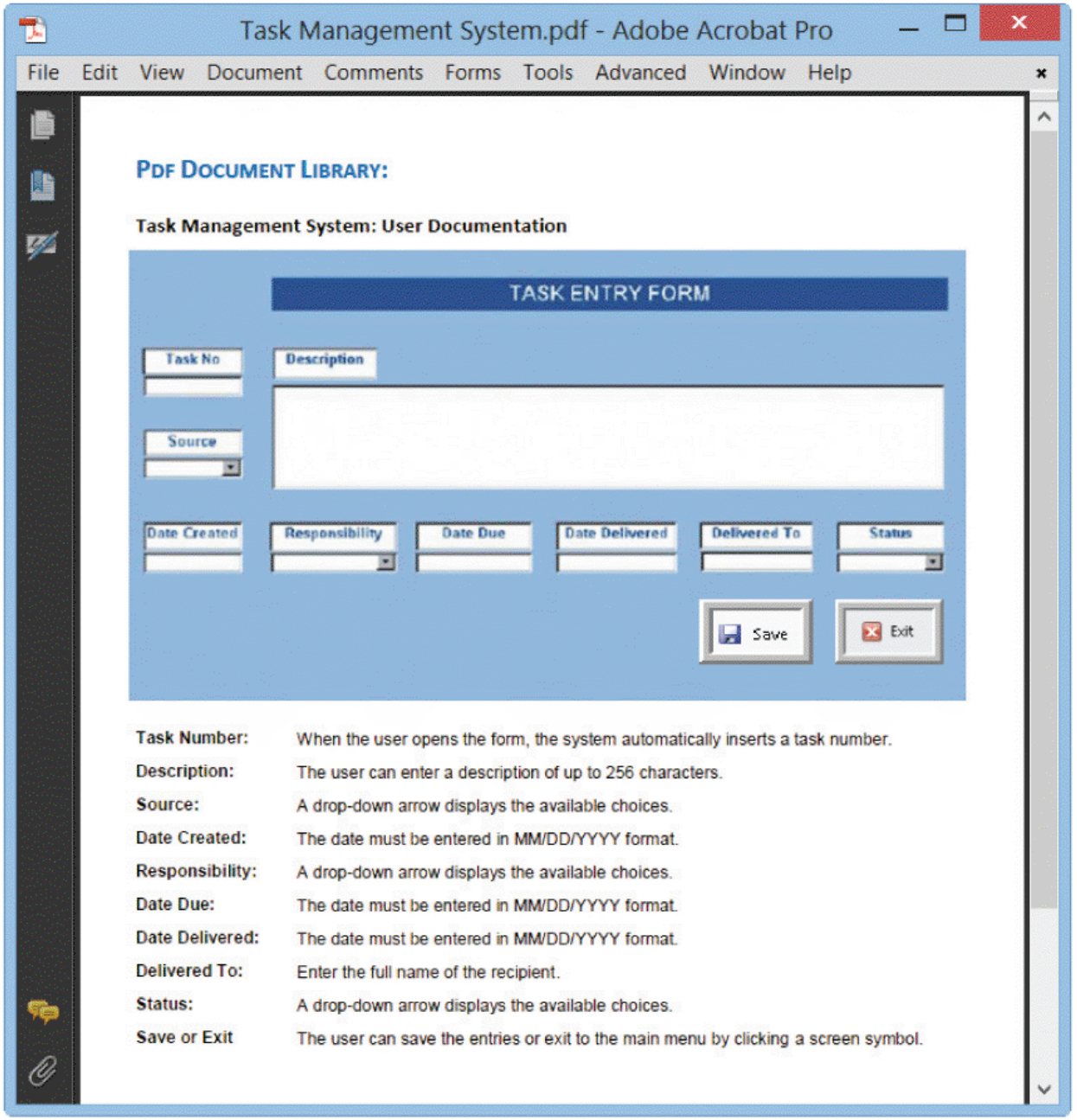
- **Program Documentation**
  - Describes the inputs, outputs, and processing logic for all program modules
  - Process starts in the systems analysis phase and continues during systems implementation
  - Overall documentation is prepared early in the SDLC
- **System Documentation**
  - Describes the system's functions and how they are implemented
- **Operations Documentation**
  - Contains the information needed for processing and distributing online and printed output
- **User Documentation**
  - Consists of instructions and information for users who will interact with the system

Documentation

- **Online Documentation**
  - Provides immediate help when users have questions or encounter problems

The Cisco Support Community invites users to contribute valuable experience and documentation using social media. **Source:** Cisco Support Community

Documentation



A sample page from a user manual. The instructions explain how to add a new task to the system.

Systems Project Closure – Documentation

- It provides confirmation that project documentation has been completed, that outputs have been delivered, and includes any outstanding issues with recommendations on how they should be resolved.

Adapted from Carr, S. (2014)

Systems Project Closure – Documentation

- The contents of the system project closure document includes:
  - Project summary
  - Project team
  - Project outcome
  - Lessons learned summary
  - Transition to operations
  - Recommendations for future system projects
  - Post projects or outstanding tasks and issues
  - Project closure approval
  - Appendix

Adapted from Carr, S. (2014)

Systems Support

- Systems support 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

- **Help** or **Service Desks**: Provide support and guidance
  - 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

User Support (Cont. 1)

- 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

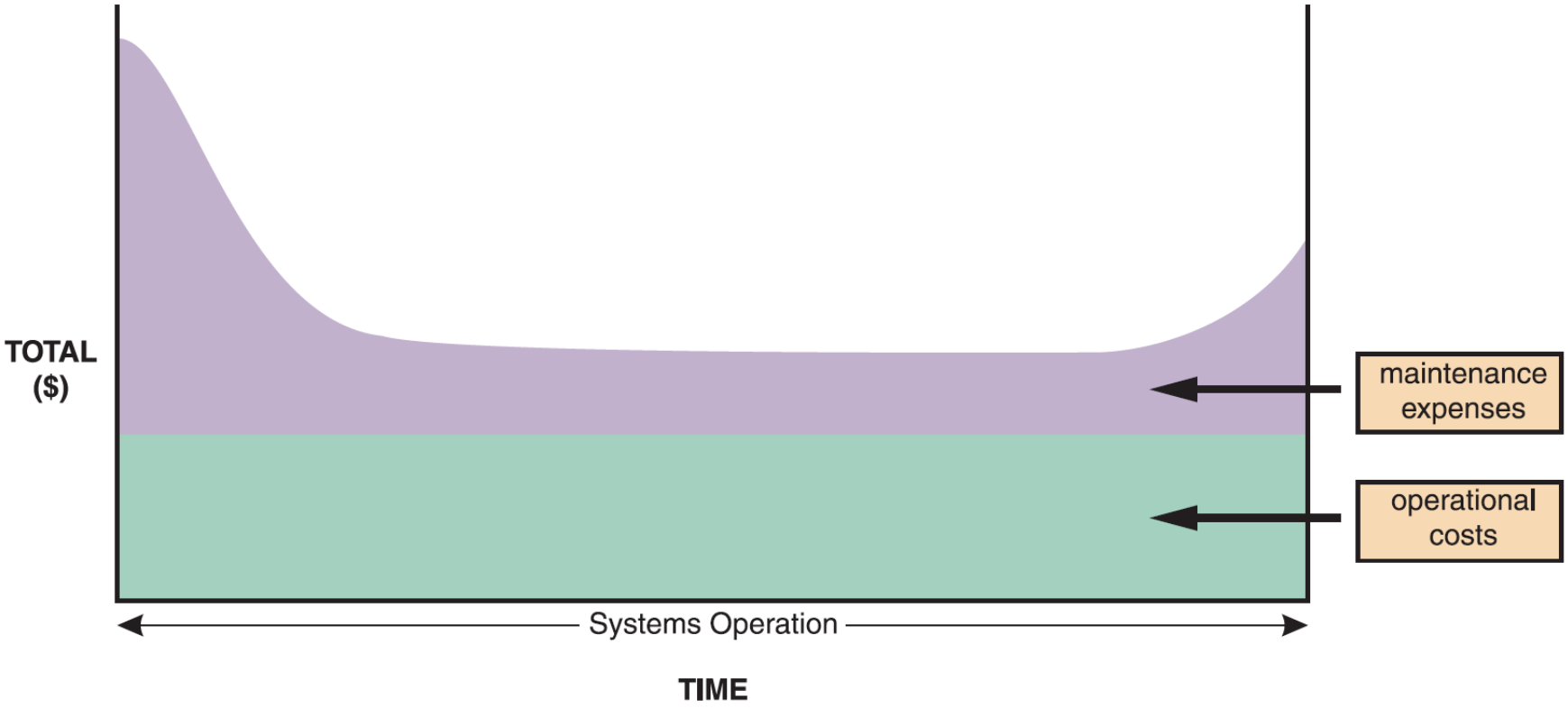
Mark Bowden/Getty Images

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



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

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.

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

Class Exercise – Critical Thinking

- 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.

- Q1: How would you answer her?
- Q2: As a newly hired systems analysts, would you prefer the role of maintaining the systems? Why/Why not?

Maintenance Management

- **The Maintenance Team**
  - **System administrator:** Manages computer and network systems
  - **Systems analysts -** Investigate and locate the source of a problem using analysis and synthesis skills
  - **Programmers -** Include **applications programmers, systems programmers,** and **database programmers**
  - Organizational issues
    - Organizations have groups that perform maintenance and new systems development
    - May rotate people from one assignment to the other

Maintenance Management

- **Maintenance Requests**
  - Involve a series of steps
    - Initial determination
    - Consideration by the systems review committee
    - Task completion and user notification

- **Establishing Priorities**
  - Systems review committees may either separate maintenance requests from new systems development requests or evaluate all projects together
  - Objective - To have a procedure that balances new development and necessary maintenance work

Maintenance Management

- **Change Control (CC)**
  - Becomes critical as enterprise-wide information systems grow more complex
    - Important to systems with multiple versions running in different hardware and software environments
  - Helps in organizing and handling documentation

Maintenance Management

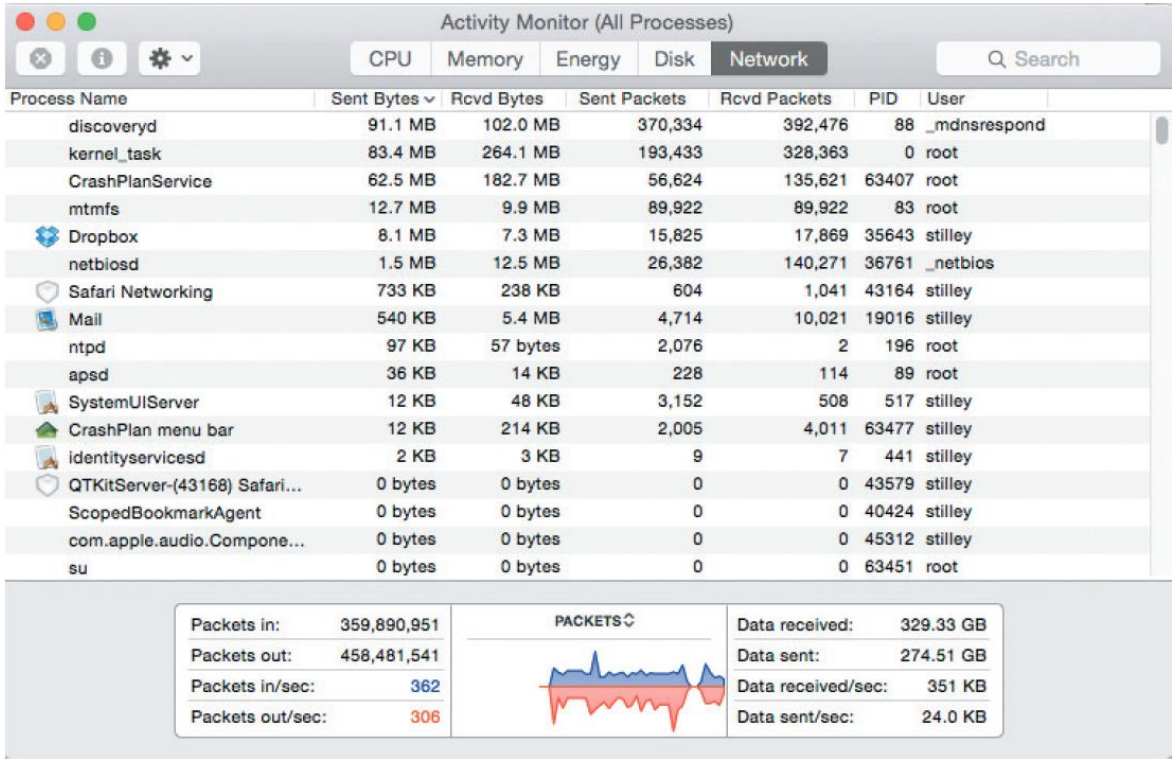
- **Maintenance Releases**
  - Documents and installs changes as a new version
  - **Maintenance release methodology:** Retains all noncritical changes and implement them simultaneously
    - Advantage - All changes are tested together, resulting in fewer versions and lesser expense
    - Disadvantage - New features of upgrades are available less often
  - **Service packs:** Maintenance releases provided by commercial software suppliers

Maintenance Management

- **Version Control**
  - Process of tracking system releases or versions
    - Prior release is **archived** and restored in case the new version fails
  - Firms use commercial applications that handle version control for complex systems
- **Baselines**
  - Measure system characteristics at a specific time
  - Types **- Functional, allocated,** and **product**

System Performance Management

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



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

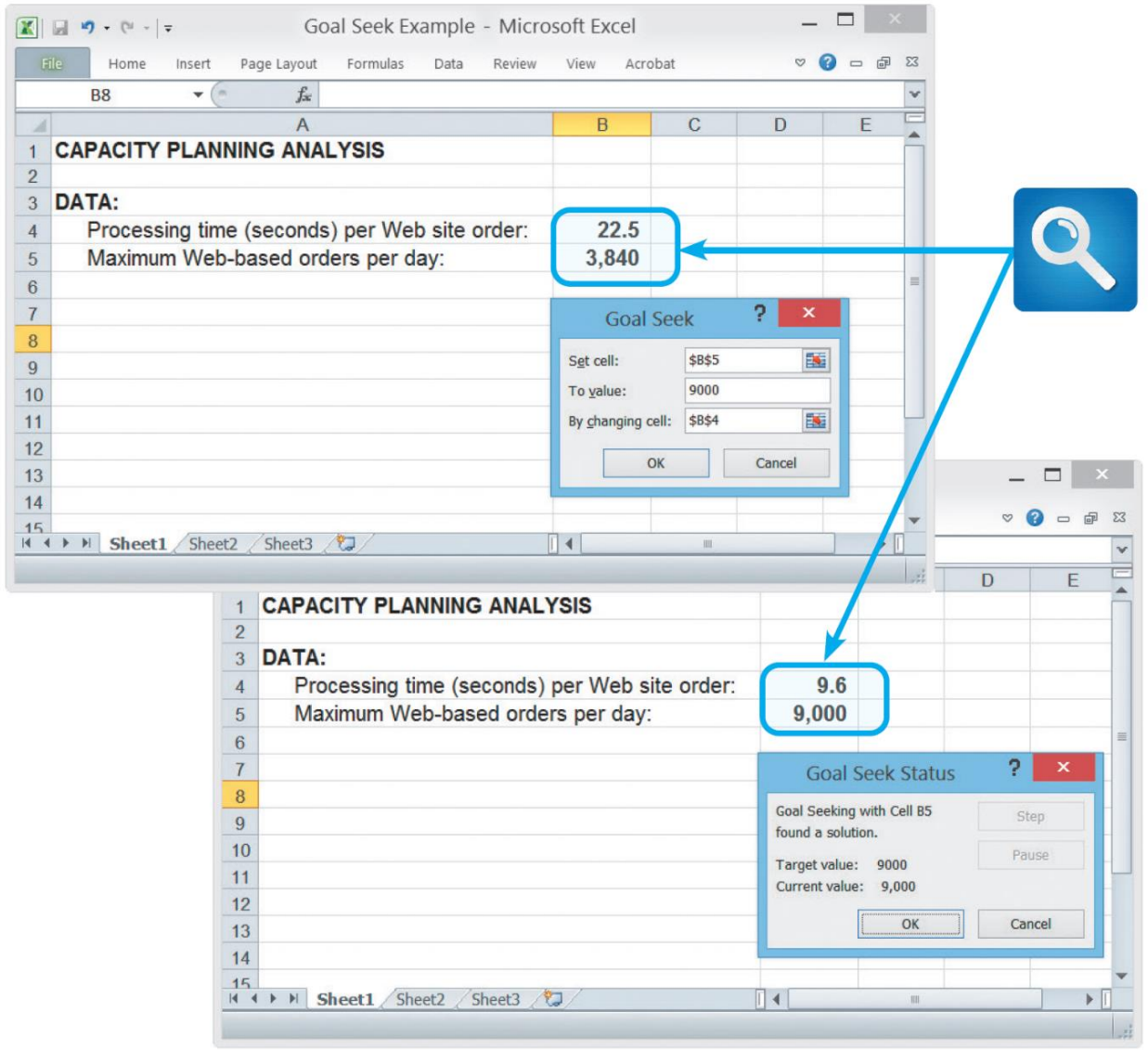
System Performance Management

- **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
    - Queue length - Number of requests pending for a service

System Performance Management

- **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



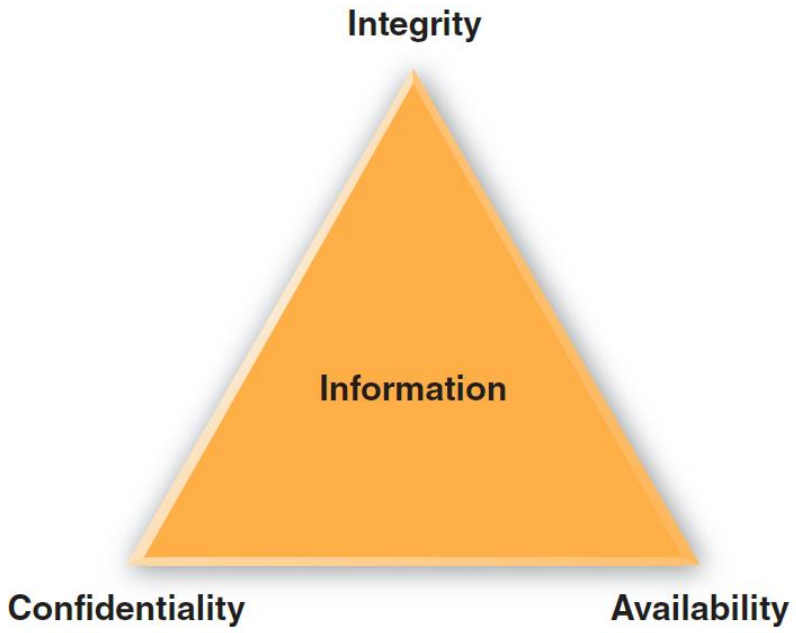
In this Goal Seek example, the user wants to know the effect on processing time if the number of daily transactions increases from 3,840 to 9,000.

System Performance Management

- **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



System security must provide information confidentiality, integrity, and availability (CIA).

System Security Overview (Cont. 2)

System threats can be grouped into several broad categories.

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.

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

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.

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.

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

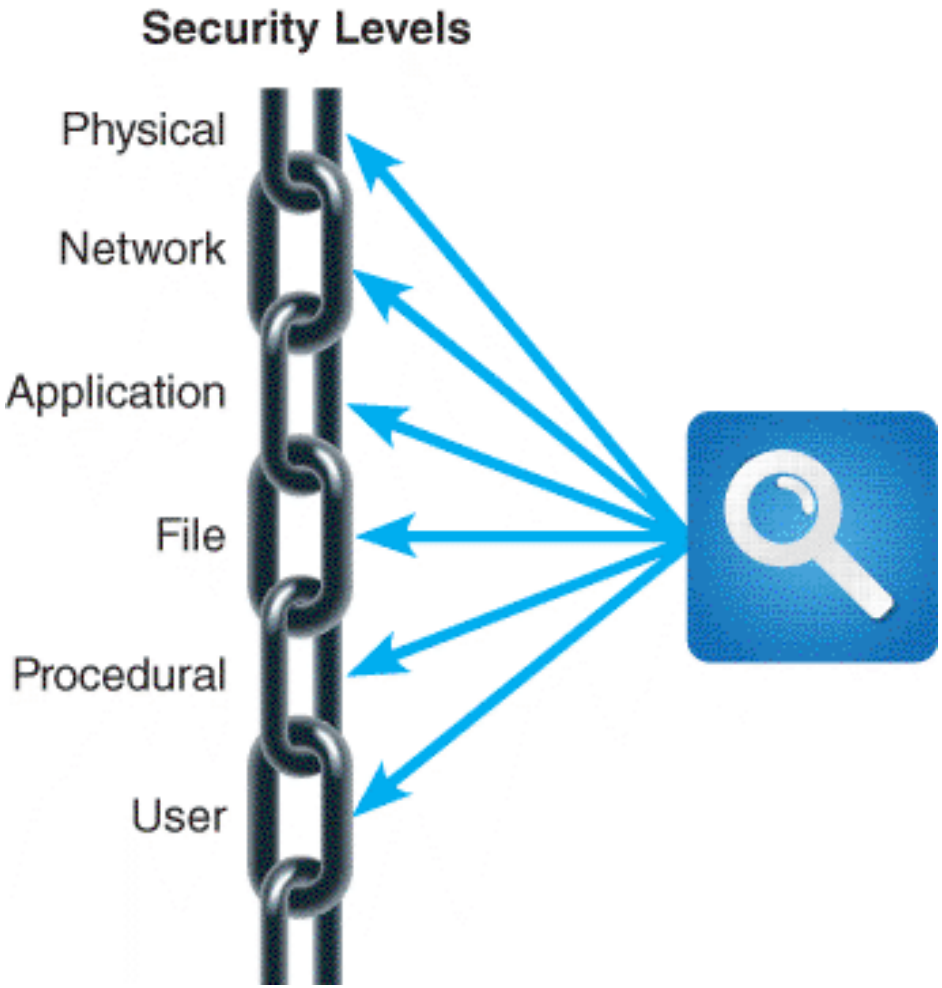
System Security Overview (Cont. 6)

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.

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

Security Levels

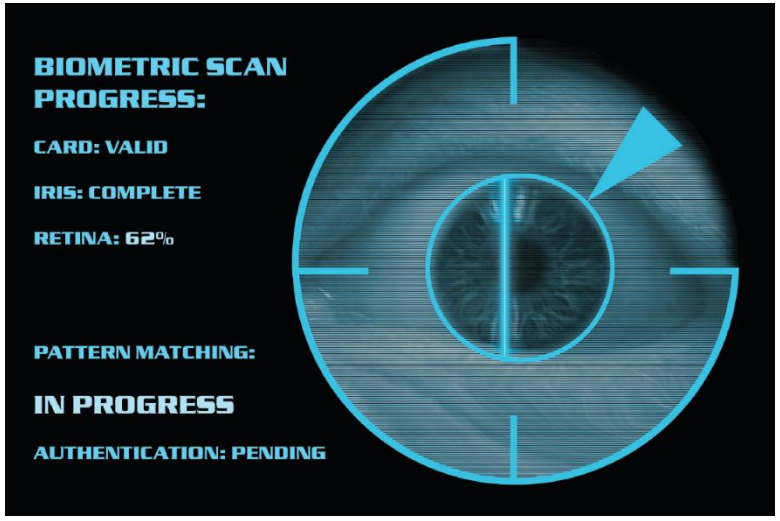
- System security involves six separated but interrelated levels



Each security link has a specific focus.

Security Levels

- **Physical Security**
  - Operations center security - Each entrance must be equipped with a suitable security device
  - Servers and desktop computers
    - Install locks on server racks to avoid unauthorized placement of **keystroke loggers**
    - **Tamper evident cases** and **BIOS-level passwords** can be used



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

Andy Piatt/Shutterstock.com

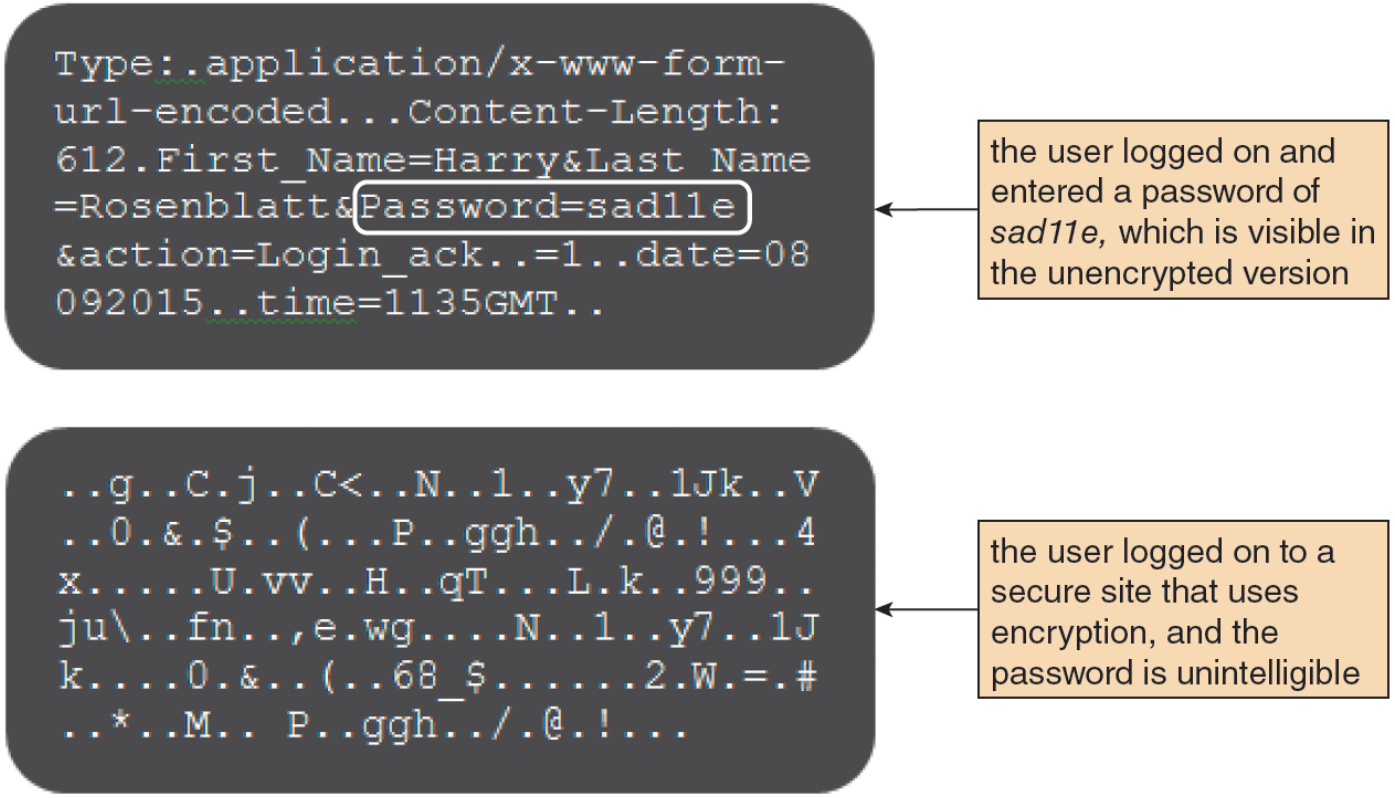
Security Levels

- Portable computers
  - Select an operating system with strong protection
  - Mark the computer's case with the company name and address
  - Consider devices that have a built-in fingerprint reader and use the Universal Security Slot (USS) if available
  - Back up all vital data before using the computer outside the office and link the system to a tracking software
  - Be alert to high-risk situations while traveling
  - Establish stringent password protection policies

Security Levels

- **Network security**
  - Encrypt network traffic
  - Wireless networks - Wi-Fi Protected Access 2 (WPA2) strengthens the level of wireless protection
  - Private networks can be used when speed is necessary
  - Virtual Private Networks (VPN) establish secure connections for a large number of computers
  - Firewalls allow or block network traffic from each network interface based on preset rules
  - Network intrusion detection system (NDIS) alerts the administrator when it detects suspicious network traffic patterns

Security Levels



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

Security Levels

- **Application Security**
  - Services that are not needed must be disabled
    - Unnecessary or improperly configured service could create a security hole
  - Hardening: Removes unnecessary accounts, services, and features
  - Application permissions
    - To provide unauthorized changes applications must be configured to be run by users who have specific rights
  - Input validation helps safeguard data integrity and security
  - Patches and updates - Used to repair security holes, reduce vulnerabilities, and update the system
  - Software logs document all events
    - Help understand past attacks and prevent future intrusions

Security Levels

- **File Security**
  - Encryption - Scrambles the contents of a file or document to protect it from unauthorized access
  - Permissions - Describe the rights a user has to a particular file or directory on a server
  - Administrators can create user groups and assign file permissions

Security Levels

- **User Security**
  - **Identity management:** Controls and procedures necessary to identify legitimate users and system components
    - Strategy must balance technology, security, privacy, cost, and user productivity
  - **Password protection**
    - Password policies need to specify a set minimum length, complexity, and a limit on invalid attempts
  - **Social engineering:** Intruder uses social interaction to gain unauthorized access to a computer system
    - Includes pretexting

Security Levels

- **User resistance**
  - Users need to understand and be a part of the organization's commitment to security
- **New technologies** can be used to enhance security and prevent unauthorized access

Security tokens, which come in various forms, can provide an additional level of security. Lim Yong Hian/Shutterstock.com

Security Levels

- **Procedural Security (Operational Security)**
  - Defines how particular tasks are to be performed
  - Includes safeguarding procedures that would be valuable to an attacker
  - Organization must explain procedures and issue reminders that will make security issues a priority

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)

Comparison of full, differential, incremental, and continuous 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.

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**

System Obsolescence

- Factors indicating obsolescence
  - Adaptive and corrective maintenance are increasing steadily
  - Operational costs or execution times are increasing rapidly
  - A software package is available that provides the same or additional services more efficiently
  - 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

Future Challenges and Opportunities

- **Trends and Predictions**
  - Cybercrime will increase significantly
  - Smartphones and tablets will become the dominant computing platform
  - Software-as-a-service will become the norm, which will affect business models and consumer costs
  - Cloud computing will become the principal computing infrastructure for the enterprise
  - Insourcing will increase due to economic factors
  - Large enterprises may require suppliers to certify their green credentials and sourcing policies

Future Challenges and Opportunities

- **Strategic Planning for IT Professionals**
  - System analysts should work backwards from goals in order to develop intermediate milestones
- **IT Credentials and Certification**
  - Professional organizations and IT industry leaders offer continuing educational courses and credentialed certifications
- **Critical Thinking Skills and CyberEthics**
  - System analysts should:
    - Possess **soft skills** and **critical thinking skills**
    - Be able to address ethical, social, and legal aspects of IT

Code of Ethics for System Professionals

- Professionalism – maintaining professional conduct at workplace and not allowing personal feelings
- Personal integrity – being honest in professional dealings.

- Privacy – accessing private information on computer systems only when it is necessary in the course of technical duties
- Law and policies – learning relevant laws and regulations

- Ethical responsibility – Doing best to make decisions consistent with safety, privacy and well-being of community and the public.

Class Exercise – Critical Thinking

- Blake works for a large IT company. The company is presented with a legal directive from the federal government to divulge personal data regarding some of the company's customers who are suspected of wrongdoing.
- Blake feels that this is a violation of the customers' privacy and is reluctant to comply with the request. His boss tells him the company has no choice; it must follow the law. Blake is told he can always choose to resign from the company if he feels so strongly about the situation.
- Instead of complying or resigning, Blake goes public. He uses the media to advocate his point of view for freedom and privacy, even while knowing that his actions will have far-reaching consequences. Instead of just losing his job, Blake risks losing his freedom and his future.

- Did Blake do the right thing?
- Is he a hero of free speech or a criminal (and possibly even a traitor)?
- What other options were available to him?
- What should the company have done when Blake went public? What should the government do?

Class Exercise – Critical Thinking

- Assume that you are a system consultant in a company. In your understanding, security is a key concern for any systems to build. However, the top management has decided to go for low cost option where security is less.

- What would you do in this situation?

Lecture Summary

- Systems support and security cover the period from the implementation of an information system until the system no longer is used
- Corrective, adaptive, perfective and preventative are types of system maintenance
- A maintenance team consists of systems analysts and programmers
- Security is a vital part of every computer system
- Data backup and recovery plans are essential
- All information systems eventually become obsolete