Securing Information Systems

You’ re on LinkedIn? Watch Out!

- Problem: Massive data breach; using old security practices
- Solution: Initiative to use minimal up-to-date industry practices, for example, salting passwords
- Illustrates the need for security practices to keep up with current standards and threats
- Demonstrates the lack of regulation for corporate computer security and social network data security; poor data protection by many companies

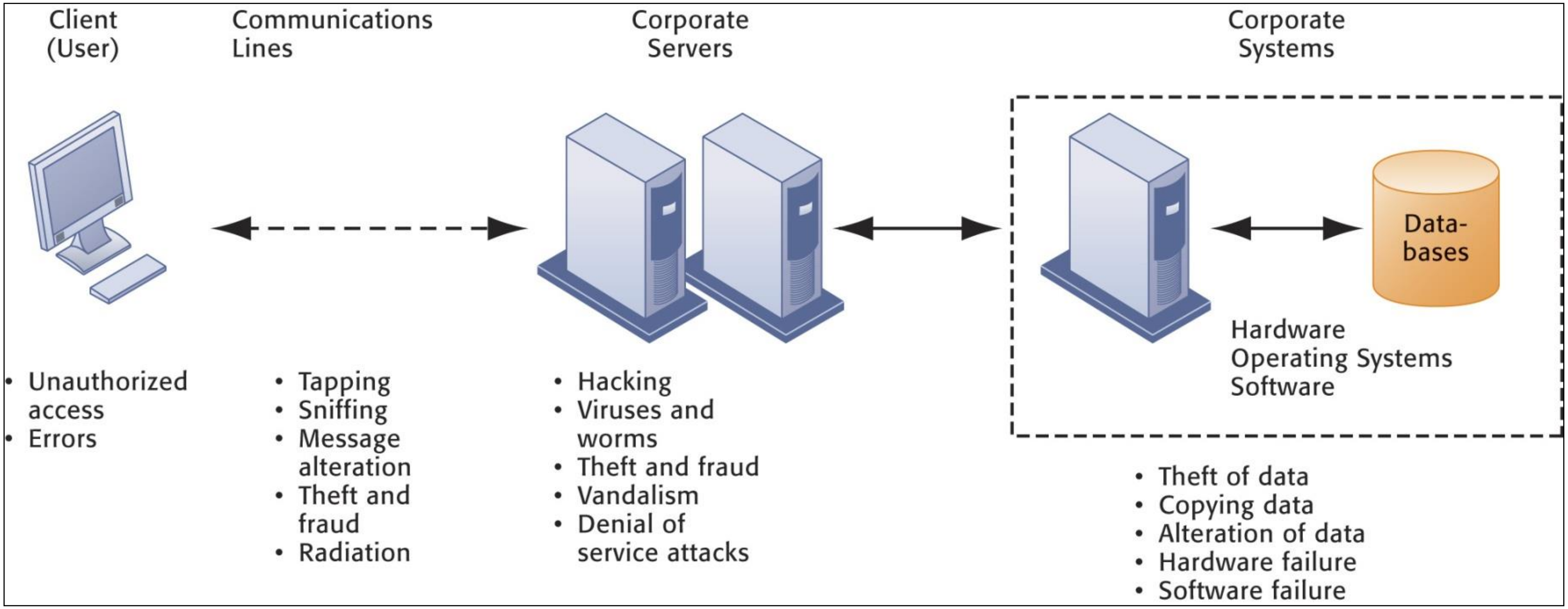
System Vulnerability and Abuse

- **Security:**
  - Policies, procedures and technical measures used to prevent unauthorized access, alteration, theft, or physical damage to information systems
- **Controls:**
  - Methods, policies, and organizational procedures that ensure safety of organization’s assets; accuracy and reliability of its accounting records; and operational adherence to management standards

System Vulnerability and Abuse

- **Why systems are vulnerable**
  - **Hardware problems**
    - Breakdowns, configuration errors, damage from improper use or crime
  - **Software problems**
    - Programming errors, installation errors, unauthorized changes)
  - **Disasters**
    - Power failures, flood, fires, etc.
  - **Use of networks and computers outside of firm’s control -** . When data are available over a network, there are even more vulnerabilities
    - E.g., with domestic or offshore outsourcing vendors

Contemporary Security Challenges and Vulnerabilities



The architecture of a Web-based application typically includes a Web client, a server, and corporate information systems linked to databases. Each of these components presents security challenges and vulnerabilities. Floods, fires, power failures, and other electrical problems can cause disruptions at any point in the network.

System Vulnerability and Abuse

- **Internet vulnerabilities -** Internet is so huge that when abuses do occur, they can have an enormously widespread impact. And when the Internet becomes part of the corporate network, the organization’s information systems are even more vulnerable to actions from outsiders
  - **Network open to anyone**
  - **Size of Internet means abuses can have wide impact**
  - **Use of fixed Internet addresses with permanent connections to Internet eases identification by hackers**
  - **E-mail attachments**
  - **E-mail used for transmitting trade secrets**
  - **IM messages lack security, can be easily intercepted**

Compromising Web Sites

- **SQL injection technique** exploits sloppy programming practices that do not validate user input
  - Hackers submit data to Web forms that exploits site' s unprotected software and sends rogue SQL query to database
  - IBM identifies SQL injection as the fastest growing security threat, with over half a million attack attempts recorded each day.
  - Firms have to check the integrity of their Web sites for vulnerabilities
- Related programming exploits:
  - **DNS cache poisoning exploits**
    - can redirect Internet address to IP address mapping and the consequences are huge.
  - Cross-site scripting attacks
    - may be used by attackers to bypass access controls accounted for roughly 80.5% of all security vulnerabilities documented by Symantec as of 2007

Securing Wireless Networks - Challenges

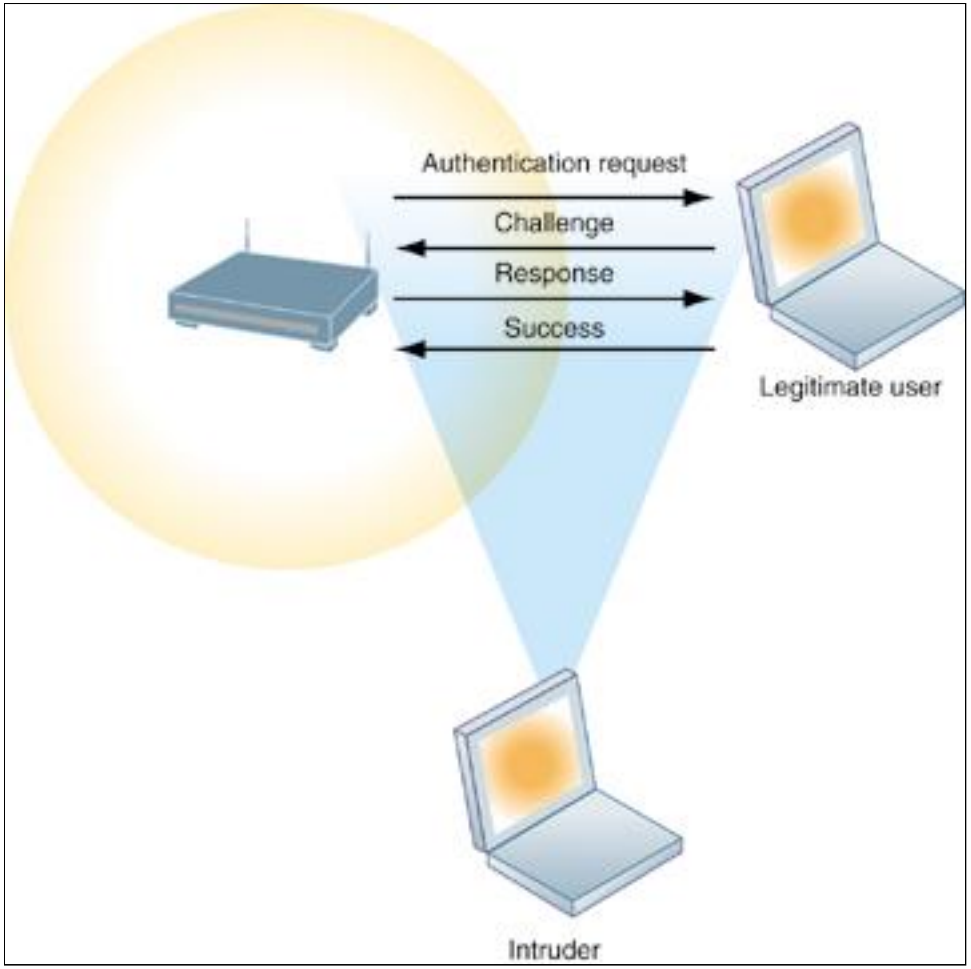
- Radio frequency bands easy to scan
- SSIDs (service set identifiers)
  - Identify access points.
  - Broadcast multiple times.
- War driving
  - Eavesdroppers drive by buildings and try to intercept network traffic
  - When hacker gains access to SSID, has access to network's resources
- WEP (Wired Equivalent Privacy)
  - Security standard for 802.11
  - The WEP specification calls for an access point and its users to share the same 40-bit encrypted password.
  - Basic specification uses shared password for both users and access point
  - Users often fail to use security features
  - Assigning unique name to network's SSID
  - *TJX fiasco - they should have used WPA (Now WPA2)*
- Wi-Fi Alliance finalized WAP2 specification, replacing WEP with stronger standards
  - Continually changing keys
  - Encrypted authentication system with central server

System Vulnerability and Abuse

The service set identifiers (SSIDs) identifying the access points in a Wi-Fi network are broadcast multiple times (as illustrated by the orange sphere) and can be picked up fairly easily by intruders’ sniffer programs

Many Wi-Fi networks can be penetrated easily by intruders using sniffer programs to obtain an address to access the resources of a network without authorization.

Wi-Fi Security Challenges



The TJX Breach

- Business establishments are increasingly under risk of information security threats
    - Network in TJX retail store was infiltrated via an insecure Wi-Fi base station
    - 45.7 million credit and debit card numbers were stolen
    - Driver’s licenses and other private information pilfered from 450,000 customers
    - TJX suffered under settlement costs and court-imposed punitive action to the tune of $150 million
    - **Even without lawsuit liabilities, Forrester Research estimates that the cost to TJX for the data breach could surpass $1 billion over five years.**

The TJX Breach

- Factors that amplified severity of TJX security breach are:
  - Personnel betrayal: An alleged FBI informant used insider information to mastermind the attacks
  - **Management** gaffe**:** Executives made conscious **decisions not to upgrade legacy systems that were vulnerable to security compromises**
  - **Technology** lapse: TJX *used WEP, a insecure wireless security technology*
    - failed to follow the **most basic security measures** like installing **antivirus software, upgrading wireless security, encrypting data, and creating and using access controls, and establishing information system controls** (general and application).
  - **Procedural** gaffes: TJX had received an *extension on the rollout of mechanisms that might have discovered and plugged the hole* before the hackers got in
    - **Also willfully violated the Payment Card Industry (PCI) Data Security Standard by holding onto data for years**

System Vulnerability and Abuse

- **Malware (malicious software)**
    - **Viruses**
        - Rogue software program that attaches itself to other software programs or data files in order to be executed
    - **Worms**
        - Independent programs that copy themselves from one computer to other computers over a network.
    - **Worms and viruses spread by**
        - Downloads (drive-by downloads)
        - E-mail, IM attachments
        - Downloads on Web sites and social networks

System Vulnerability and Abuse

- **Malware (cont.)**
  - **Smartphones as vulnerable as computers**
    - Study finds 13,000 types of smartphone malware
  - **Trojan horses**
    - Software that appears benign but does something other than expected
      - In 2004, users were enticed by a sales message from a *supposed* anti-virus vendor.
      - On the vendor’s site, a small program called Mitglieder was downloaded to the user’s machine. The program
  - **SQL injection attacks (already discussed)**
    - Hackers submit data to Web forms that exploits site’s unprotected software and sends rogue SQL query to database

System Vulnerability and Abuse

- **Malware (cont.)**
  - **Spyware**
    - Small programs install themselves surreptitiously on computers to monitor user Web surfing activity and serve up advertising
    - Key loggers
      - Record every keystroke on computer to steal serial numbers, passwords, launch Internet attacks
    - Other types:
      - Reset browser home page
      - Redirect search requests
      - Slow computer performance by taking up memory

Cookies

- ***Cookie*** – a small file that contains information about you and your Web activities, which a Web site places on your computer
- Handle cookies by using
  - Web browser cookie management option
  - Buy a program that manages cookies
- Not executable, cannot deliver a virus or other malicious code
- Only web server that delivered it can read it
- Your computer can store cookies from many web sites
- May be a security risk if it is implemented poorly on site that you have shared personal information with and rely on cookies to access it
  - Anyone who can access the cookie on your hard drive can now access that personal information
  - Most reputable sites to not rely on cookies for authentication alone.

Hackers and Computer Crime

- **Computer crime**
  - Defined as "any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution"
  - **Computer may be target of crime:**
  - **Computer may be instrument of crime:**

System Vulnerability and Abuse

- **Hackers and computer crime**
  - **Hackers vs. crackers**
  - **Activities include:**
    - System intrusion
    - System damage
    - Cybervandalism
      - Intentional disruption, defacement, destruction of Web site or corporate information system
  - **White hat hacker – hackers hired by companies to reveal security weaknesses within the firm’s systems**

System Vulnerability and Abuse

- **Spoofing**
  - **Misrepresenting oneself by using fake e-mail addresses or masquerading as someone else**
  - **Redirecting Web link to address different from intended one, with site masquerading as intended destination**
- **Sniffer**
  - **Eavesdropping program that monitors information traveling over network**
  - **Enables hackers to steal proprietary information such as e-mail, company files, and so on**
    - use your debit card information to purchase items illegally.
    - steal your logon and passwords for various accounts.
    - assume your identity.

System Vulnerability and Abuse

- **Denial-of-service attacks (DoS)**
  - **Flooding server with thousands of false requests to crash the network**
- **Distributed denial-of-service attacks (DDoS)**
  - **Use of numerous computers to launch a DoS**
  - **Botnets**
    - Networks of “zombie” PCs infiltrated by bot malware
    - Deliver 90% of world spam, 80% of world malware
    - Grum botnet: controlled 560K to 840K computers

System Vulnerability and Abuse

- **Computer crime**
  - **Defined as “any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution”**
  - **Computer may be target of crime, for example:**
    - Breaching confidentiality of protected computerized data
    - Accessing a computer system without authority
  - **Computer may be instrument of crime, for example:**
    - Theft of trade secrets
    - Using e-mail for threats or harassment

System Vulnerability and Abuse

- **Identity theft**
  - **Theft of personal Information (social security ID, driver' s license, or credit card numbers) to impersonate someone else**
- **Phishing**
  - **Setting up fake Web sites or sending e-mail messages that look like legitimate businesses to ask users for confidential personal data.**
- **Evil twins**
  - **Wireless networks that pretend to offer trustworthy Wi-Fi connections to the Internet**

System Vulnerability and Abuse

- Pharming
  - Redirects users to a bogus Web page, even when individual types correct Web page address into his or her browser
- Click fraud
  - Occurs when individual or computer program fraudulently clicks on online ad without any intention of learning more about the advertiser or making a purchase
- Cyberterrorism and Cyberwarfare

Stuxnet and the Changing Face of Cyberwarfare

- Is cyberwarfare a serious problem? Why or why not?
- Assess the management, organization, and technology factors that have created this problem.
- What makes Stuxnet different from other cyberwarfare attacks? How serious a threat is this technology?
- What solutions have been proposed for this problem? Do you think they will be effective? Why or why not?

System Vulnerability and Abuse

- **Internal threats: Employees**
  - **Security threats often originate inside an organization**
  - **Inside knowledge**
  - **Sloppy security procedures**
    - User lack of knowledge
  - **Social engineering:**
    - Tricking employees into revealing their passwords by pretending to be legitimate members of the company in need of information

System Vulnerability and Abuse

- **Software vulnerability**
  - **Commercial software contains flaws that create security vulnerabilities**
    - Hidden bugs (program code defects)
      - Zero defects cannot be achieved because complete testing is not possible with large programs
    - Flaws can open networks to intruders
  - **Patches**
    - Small pieces of software to repair flaws
    - Exploits often created faster than patches can be released and implemented

Business Value of Security and Control

- Failed computer systems can lead to significant or total loss of business function.
- Firms now are more vulnerable than ever.
  - Confidential personal and financial data
  - Trade secrets, new products, strategies
- A security breach may cut into a firm’s market value almost immediately.
- Inadequate security and controls also bring forth issues of liability.

Business Value of Security and Control

- **Legal and regulatory requirements for electronic records management and privacy protection**
- **Firms face new legal obligations for the retention and storage of electronic records as well as for privacy protection**
  - **HIPAA:** Medical security and privacy rules and procedures
  - **Gramm-Leach-Bliley Act:** Requires financial institutions to ensure the security and confidentiality of customer data
  - **Sarbanes-Oxley Act:** Imposes responsibility on companies and their management to safeguard the accuracy and integrity of financial information that is used internally and released externally

Business Value of Security and Control

- **Electronic evidence**
  - **Evidence for white collar crimes often in digital form**
    - Data on computers, e-mail, instant messages, e-commerce transactions
  - **Proper control of data can save time and money when responding to legal discovery request**
- **Computer forensics:**
  - **Scientific collection, examination, authentication, preservation, and analysis of data from computer storage media for use as evidence in court of law**
  - **Includes recovery of ambient and hidden data**

Establishing a Framework for Security and Control

- **Information systems controls**
  - Manual and automated controls
  - General and application controls
- **General controls**
  - **Govern design, security, and use of computer programs and security of data files in general throughout organization’s information technology infrastructure**
  - **Apply to all computerized applications**
  - **Combination of hardware, software, and manual procedures to create overall control environment**

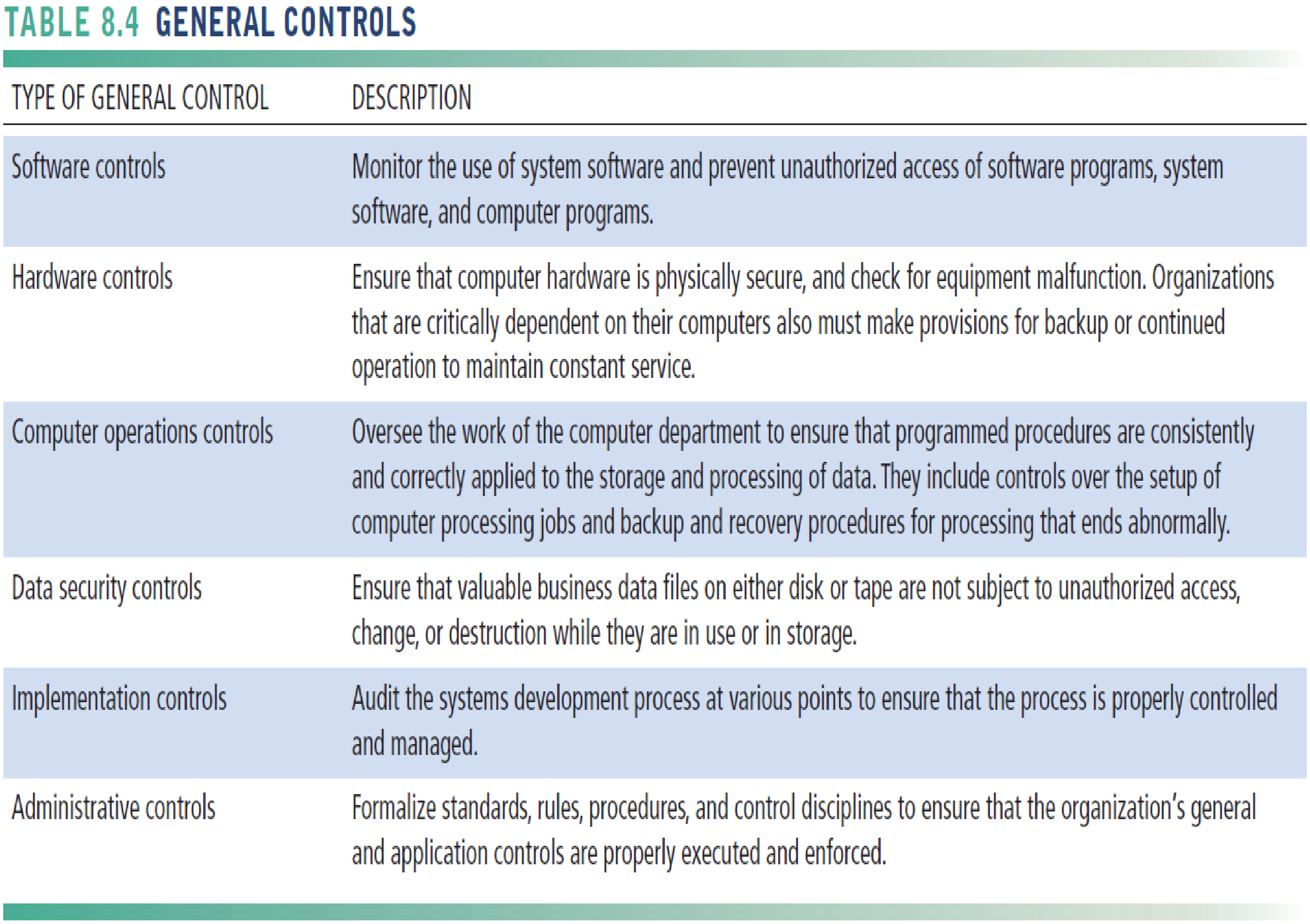


TABLE 8.4 GENERAL CONTROLS

TYPE OF GENERAL CONTROL	DESCRIPTION
Software controls	Monitor the use of system software and prevent unauthorized access of software programs, system software, and computer programs.
Hardware controls	Ensure that computer hardware is physically secure, and check for equipment malfunction. Organizations that are critically dependent on their computers also must make provisions for backup or continued operation to maintain constant service.
Computer operations controls	Oversee the work of the computer department to ensure that programmed procedures are consistently and correctly applied to the storage and processing of data. They include controls over the setup of computer processing jobs and backup and recovery procedures for processing that ends abnormally.
Data security controls	Ensure that valuable business data files on either disk or tape are not subject to unauthorized access, change, or destruction while they are in use or in storage.
Implementation controls	Audit the systems development process at various points to ensure that the process is properly controlled and managed.
Administrative controls	Formalize standards, rules, procedures, and control disciplines to ensure that the organization's general and application controls are properly executed and enforced.

Establishing a Framework for Security and Control

- **Application controls**
  - Specific controls unique to each computerized application, such as payroll or order processing
  - Include both automated and manual procedures
  - Ensure that only authorized data are completely and accurately processed by that application
  - Types of application controls:
    - **Input controls -** input authorization, data conversion, data editing, and error handling
    - **Processing controls -** establish that data are complete and accurate during updating
    - **Output controls -** ensure that the results of computer processing are accurate, complete, and properly distributed

Establishing a Framework for Security and Control

- **Risk assessment:** Determines level of risk to firm if specific activity or process is not properly controlled
  - Types of threat
  - Probability of occurrence during year
  - Potential losses, value of threat
  - Expected annual loss

- Risk cost = probability X impact

EXPOSURE	PROBABILITY	LOSS RANGE (AVG)	EXPECTED ANNUAL LOSS
Power failure	30%	$5K–$200K ($102,500)	$30,750
Embezzlement	5%	$1K–$50K ($25,500)	$1,275
User error	98%	$200–$40K ($20,100)	$19,698

Establishing a Framework for Security and Control

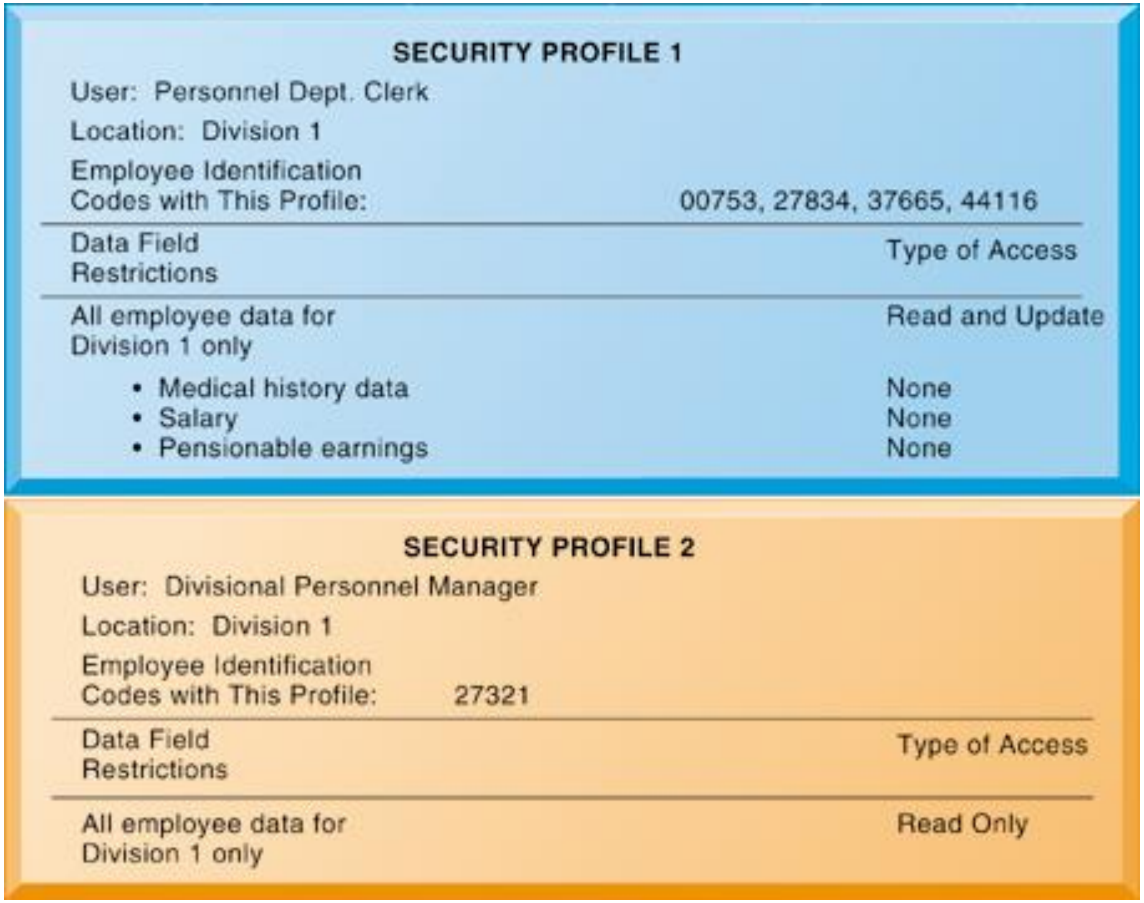
- **Security policy**
  - **Ranks information risks, identifies acceptable security goals, and identifies mechanisms for achieving these goals**
  - **Drives other policies**
    - Acceptable use policy (AUP)
      - Defines acceptable uses of firm’s information resources and computing equipment
      - Privacy, user responsibility, and personal use of company equipment and networks, unacceptable and acceptable actions for every user, and consequences for noncompliance
        - Example: every employee with a laptop or mobile handheld to use an approved device and employ a password or other method of identification when logging onto the corporate network.
        - No flash drives in USB ports or CD or DVDs
    - **Identity management system:** Manages access to each part of the information system.
    - Example: table which controls which employees can access various systems

Establishing a Framework for Security and Control

- **Identity management**
  - **Business processes and tools to identify valid users of system and control access**
    - Identifies and authorizes different categories of users
    - Specifies which portion of system users can access
    - Authenticating users and protects identities
  - **Identity management systems**
    - Captures access rules for different levels of users

Security Profiles for a Personnel System

These two examples represent two security profiles or data security patterns that might be found in a personnel system. Depending on the security profile, a user would have certain restrictions on access to various systems, locations, or data in an organization.



SECURITY PROFILE 1

User: Personnel Dept. Clerk

Location: Division 1

Employee Identification Codes with This Profile: 00753, 27834, 37665, 44116

Data Field Restrictions	Type of Access
All employee data for Division 1 only	Read and Update
• Medical history data	None
• Salary	None
• Pensionable earnings	None

SECURITY PROFILE 2

User: Divisional Personnel Manager

Location: Division 1

Employee Identification Codes with This Profile: 27321

Data Field Restrictions	Type of Access
All employee data for Division 1 only	Read Only

Establishing a Framework for Security and Control

- **Disaster recovery planning:** Devises plans for restoration of disrupted services
  - MasterCard, maintains a duplicate computer center in Kansas City, Missouri, to serve as an emergency backup to its primary computer center in St. Louis.
- **Business continuity planning:** Focuses on restoring business operations after disaster
  - **Both types of plans needed to identify firm’ s most critical systems**
  - **Business impact analysis to determine impact of an outage**
  - **Management must determine which systems restored first**

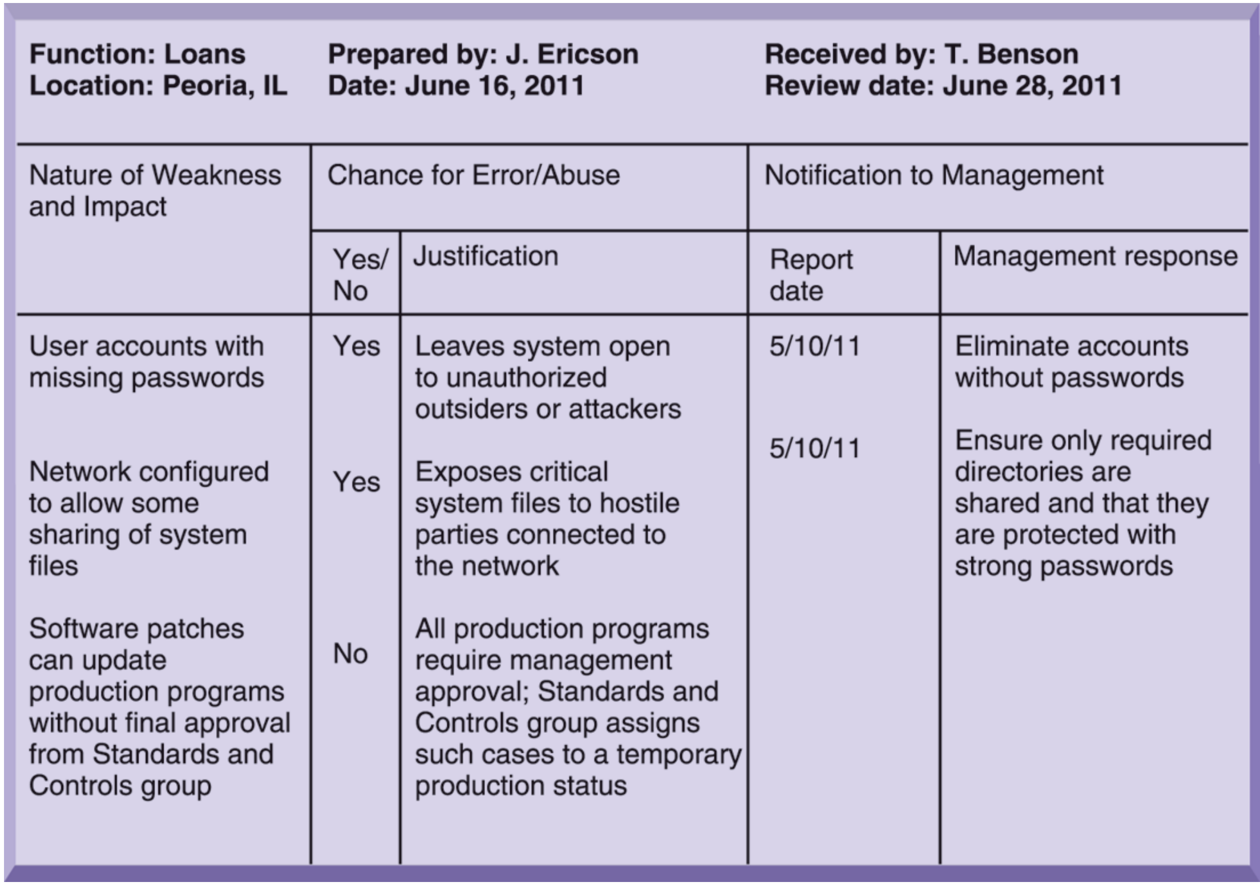
The Role of Auditing

- **MIS audit -** determines if existing security measures and controls are effective
  - Examines firm's overall security environment as well as controls governing individual information systems
  - Reviews technologies, procedures, documentation, training, and personnel
  - May even simulate disaster to test response of technology, IS staff, other employees
  - Lists and ranks all control weaknesses and estimates probability of their occurrence
  - Assesses financial and organizational impact of each threat

SAMPLE AUDITOR'S LIST OF CONTROL WEAKNESSES

This chart is a sample page from a list of control weaknesses that an auditor might find in a loan system in a local commercial bank. This form helps auditors record and evaluate control weaknesses and shows the results of discussing those weaknesses with management, as well as any corrective actions taken by management.

FIGURE 8-4



Function: Loans **Location: Peoria, IL**	**Prepared by: J. Ericson** **Date: June 16, 2011**	**Received by: T. Benson** **Review date: June 28, 2011**	

Nature of Weakness and Impact	Chance for Error/Abuse		Notification to Management	
	Yes/ No	Justification	Report date	Management response
User accounts with missing passwords	Yes	Leaves system open to unauthorized outsiders or attackers	5/10/11	Eliminate accounts without passwords
Network configured to allow some sharing of system files	Yes	Exposes critical system files to hostile parties connected to the network	5/10/11	Ensure only required directories are shared and that they are protected with strong passwords
Software patches can update production programs without final approval from Standards and Controls group	No	All production programs require management approval; Standards and Controls group assigns such cases to a temporary production status		

Technologies and Tools for Protecting Information Resources

- Identity management software
  - Automates keeping track of all users and privileges
  - Authenticates users, protecting identities, controlling access
- Authentication
  - Password systems
  - Tokens - – may be physical device or software that authorized user is given to make authentication easier/ quicker
  - Smart cards
  - Biometric authentication

Technologies and Tools for Protecting Information Resources

- **Firewall:**
  - **Combination of hardware and software that prevents unauthorized users from accessing private networks**
  - **Firewalls can deter, but not completely prevent, network penetration by outsiders and should be viewed as one element in an overall security plan**

A CORPORATE FIREWALL

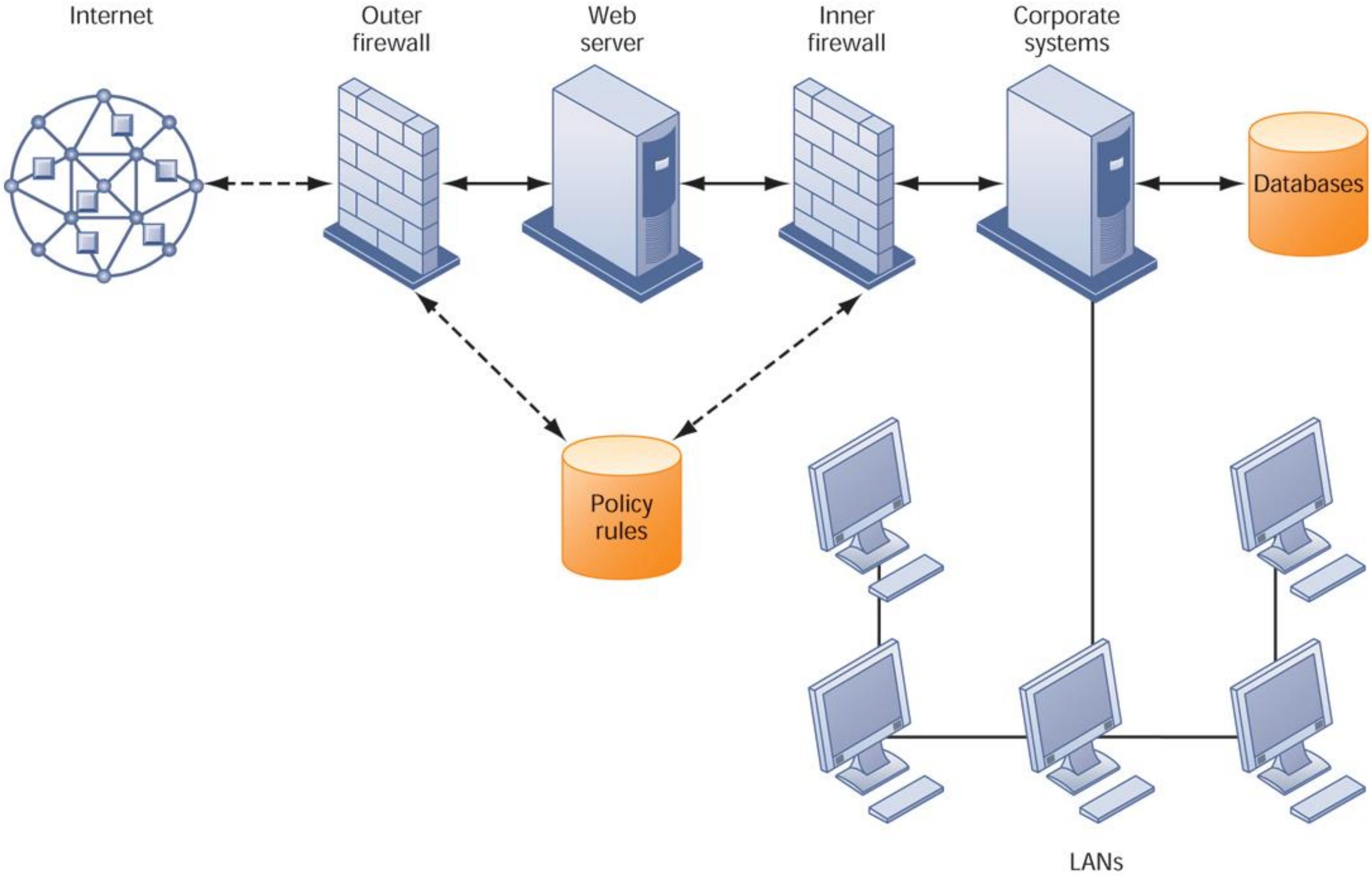


FIGURE 8-5

T
fi
p
d
a

tı

Technologies and Tools for Protecting Information Resources

- **Intrusion detection systems:**
  - **Monitors hot spots on corporate networks to detect and deter intruders**
  - **Examines events as they are happening to discover attacks in progress**
- **Antivirus and antispyware software:**
  - **Checks computers for presence of malware and can often eliminate it as well**
  - **Requires continual updating**

- **Unified threat management (UTM) System**
  - Comprehensive security management products
  - Tools include
    - Firewalls
    - Intrusion detection
    - Web content filtering –
      - What bothers management is not knowing what employees are doing on the web:
      - How much time do employees spend on social networks or gaming sites?
      - Is anyone downloading malware or pornography?
      - Why is the Internet running slowly today?
    - Antispam software – why?

Technologies and Tools for Protecting Information Resources

- **Securing wireless networks**
  - **WEP security can provide some security by:**
    - Assigning unique name to network’s SSID and not broadcasting SSID
    - Using it with VPN technology
  - **Wi-Fi Alliance finalized WAP2 specification, replacing WEP with stronger standards**
    - Continually changing keys
    - Encrypted authentication system with central server

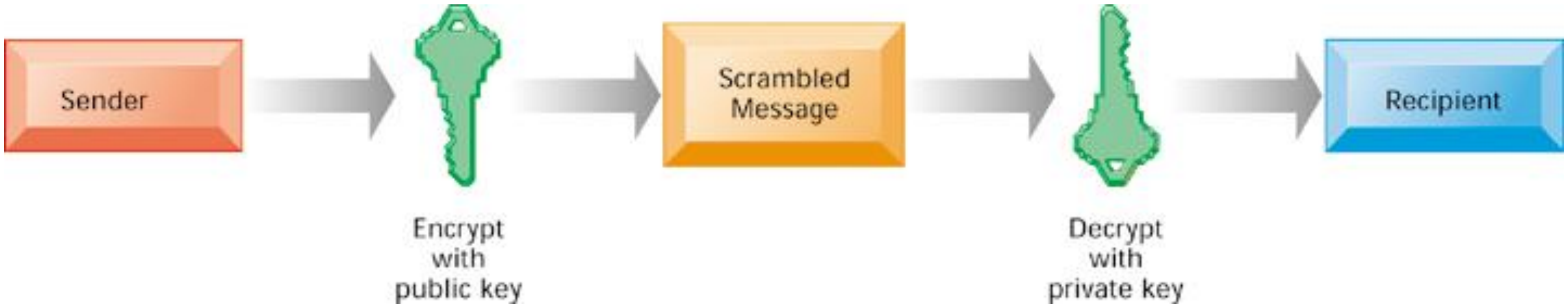
Technologies and Tools for Protecting Information Resources

- **Encryption:**
  - **Transforming text or data into cipher text that cannot be read by unintended recipients**
  - **Two methods for encryption on networks**
    - Secure Sockets Layer (SSL) and successor Transport Layer Security (TLS)
    - Secure Hypertext Transfer Protocol (S-HTTP)

Technologies and Tools for Protecting Information Resources

- **Two methods of encryption**
    - **Symmetric key encryption**
        - Sender and receiver use single, shared key
    - **Public key encryption**
        - Uses two, mathematically related keys: Public key and private key
        - Sender encrypts message with recipient’ s public key
        - Recipient decrypts with private key
        - The strength of an encryption key is measured by its bit length.
            - Today, a typical key will be 128 bits long (a string of 128 binary digits).

Public Key Encryption



A public key encryption system can be viewed as a series of public and private keys that lock data when they are transmitted and unlock the data when they are received. The sender locates the recipient's public key in a directory and uses it to encrypt a message. The message is sent in encrypted form over the Internet or a private network. When the encrypted message arrives, the recipient uses his or her private key to decrypt the data and read the message.

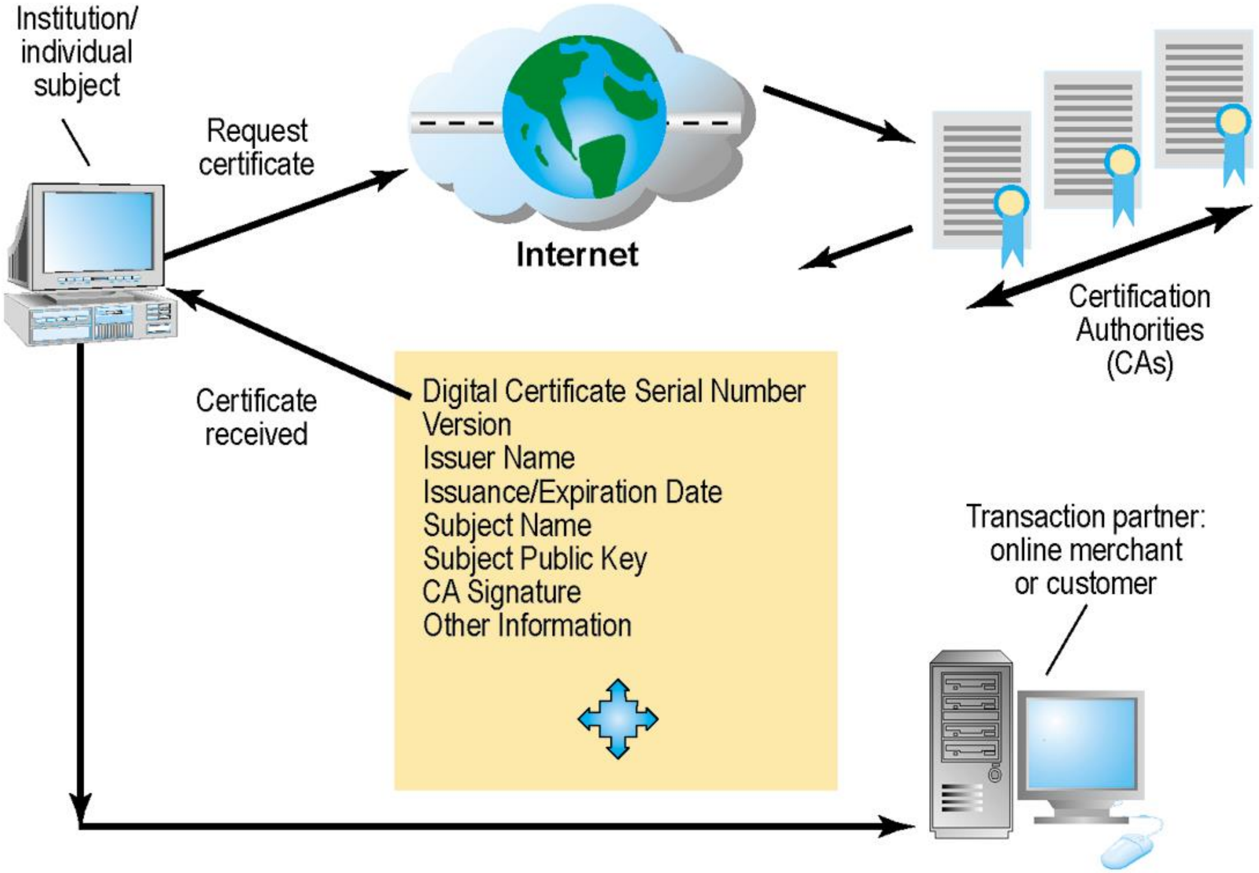
Technologies and Tools for Protecting Information Resources

- **Digital certificate:**
  - Data file used to establish the identity of users and electronic assets for protection of online transactions
  - Uses a trusted third party, certification authority (CA), to validate a user’ s identity
  - CA verifies user’ s identity, stores information in CA server, which generates encrypted digital certificate containing owner ID information and copy of owner’ s public key
- **Public key infrastructure (PKI)**
  - Use of public key cryptography working with certificate authority
  - Widely used in e-commerce

DIGITAL CERTIFICATES

Digital certificates help establish the identity of people or electronic assets. They protect online transactions by providing secure, encrypted, online communication.

The institution or individual requests a certificate over the Internet from a CA; the certificate received from the CA can then be used to validate a transaction with an online merchant or customer.



Technologies and Tools for Protecting Information Resources

- **Ensuring system availability**
  - **Online transaction processing requires 100% availability, no downtime**
  - **There is a huge $$ loss in downtime**
- **Fault-tolerant computer systems**
  - **For continuous availability, for example, stock markets**
  - **Contain redundant hardware, software, and power supply components that create an environment that provides continuous, uninterrupted service**
- **High-availability computing**
  - **Helps recover quickly from crash**
  - **Minimizes, does not eliminate, downtime**
- Firms with heavy e-commerce processing or for firms that depend on digital networks for their internal operations require high-availability computing, using tools such as backup servers, distribution of processing across multiple servers, high-capacity storage, and good disaster recovery and business continuity plans

Hot Site

- A hot site is a commercial disaster recovery service that allows a business to continue computer and network operations in the event of a computer or equipment disaster.
- If an firm’s data center becomes inoperable it can move all data processing operations to a hot site.
- A hot site is a duplicate of the original site of the organization, with full computer systems as well as near-complete backups of user data.
  - The site has all the equipment needed for the enterprise to continue operation, including office space and furniture, telephone jacks and computer equipment.
- Real time synchronization between the two sites may be used to completely mirror the data environment of the original site.
- Following a disruption to the original site, the hot site exists so that the organization can relocate with minimal losses to normal operations.
- Ideally, a hot site will be up and running within a matter of hours or even less.
- Example – Hurricane Katrina - oil company hot sites

Technologies and Tools for Security

- **Recovery-oriented computing**
  - Designing systems that recover quickly with capabilities to help operators pinpoint and correct of faults in multi-component systems
- **Controlling network traffic**- enables a network to sort low-priority data packets from high-priority ones in order to improve performance for business critical communication
  - Deep packet inspection (DPI) - enables a network to sort low-priority data packets from high-priority ones in order to improve performance for business critical communication.
- **Security outsourcing**
  - Managed security service providers (MSSPs)

Technologies and Tools for Protecting Information Resources

- **Security in the cloud**
  - **Responsibility for security resides with company owning the data**
  - **Firms must ensure providers provides adequate protection:**
    - Where data are stored
    - Meeting corporate requirements, legal privacy laws
    - Segregation of data from other clients
    - Audits and security certifications
  - **Service level agreements (SLAs)**

Technologies and Tools for Protecting Information Resources

- **Securing mobile platforms**
  - **Security policies should include and cover any special requirements for mobile devices**
    - Guidelines for use of platforms and applications
  - **Mobile device management tools**
    - Authorization
    - Inventory records
    - Control updates
    - Lock down/erase lost devices
    - Encryption
  - **Software for segregating corporate data on devices**

How Secure Is Your Smartphone?

- It has been said that a smartphone is a microcomputer in your hand. Discuss the security implications of this statement.
- What management, organizational, and technology issues must be addressed by smartphone security?
- What problems do smartphone security weaknesses cause for businesses?
- What steps can individuals and businesses take to make their smartphones more secure?

Technologies and Tools for Protecting Information Resources

- **Ensuring software quality**
  - **Software metrics: Objective assessments of system in form of quantified measurements**
    - Number of transactions
    - Online response time
    - Payroll checks printed per hour
    - Known bugs per hundred lines of code
  - **Testing: Early and regular testing – Testing is complex and requires various types of tests**
    - **Walk through:** Review of specification or design document by small group of qualified people
    - **Debugging:** Process by which errors are eliminated
    - Majority of testing done by IS – error free, performance: response time, throughput, accuracy
    - Some testing done by end users – does the system meet the functional requirements as originally described in the Requirements document