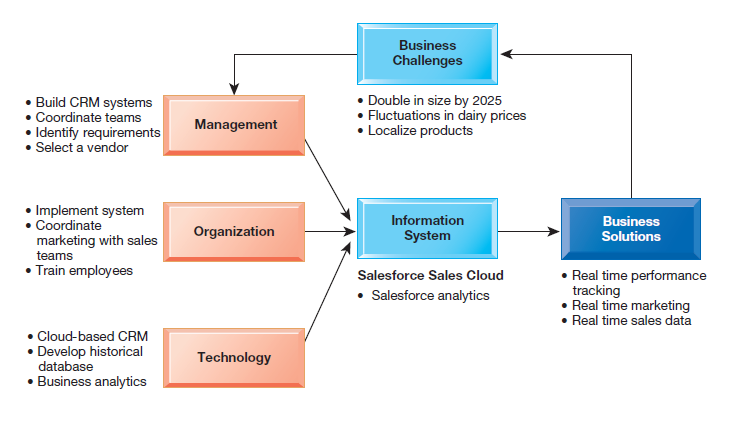
**CH8 Securing Information Systems**

學習目標:

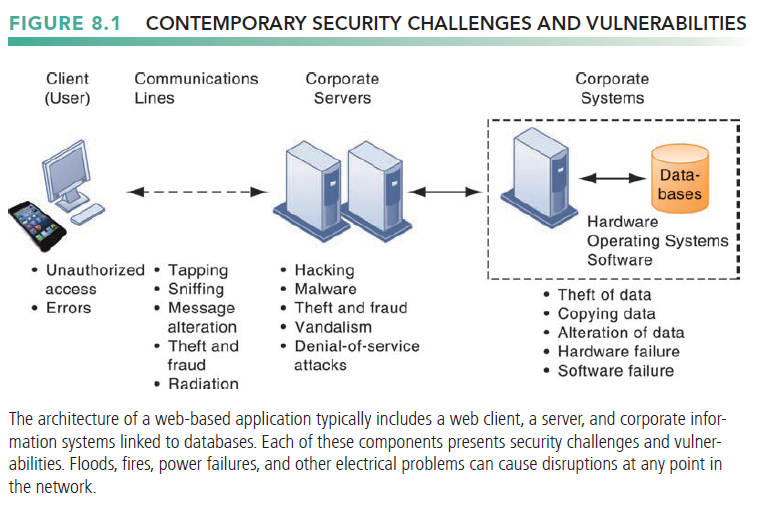
* 1. 為什麼資訊系統容易受到破壞，錯誤和濫用？
  2. 安全(security)和控制(control)的商業價值是什麼？
  3. 安全和控制的組織框架是什麼組成的？
  4. 保護資訊資源最重要的工具和技術是什麼？
* Hackers Attack Singapore’s Telecom Infrastructure



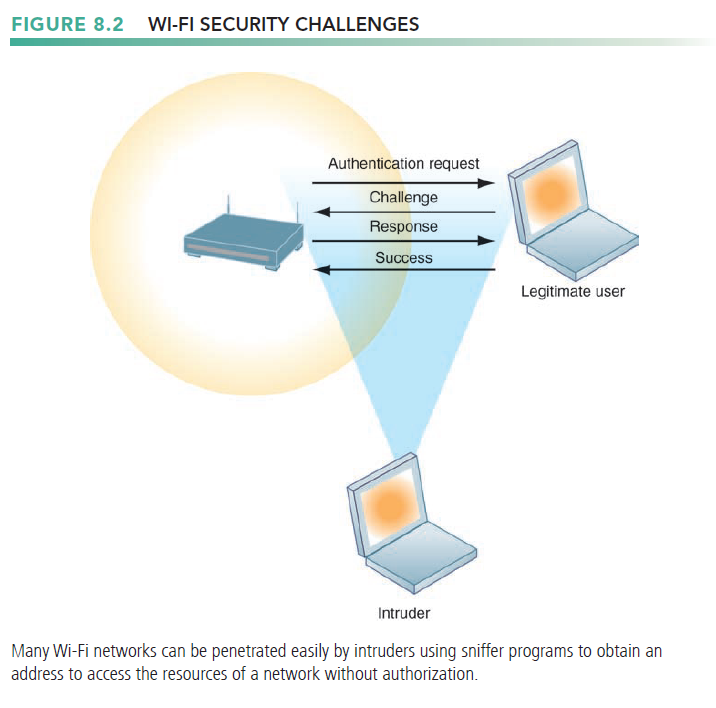
* Here are some questions to think about: What security vulnerabilities were exploited by the hackers? What management, organizational, and technological factors contributed to these security weaknesses? What was the business impact of these problems?

1. Why are information systems vulnerable to destruction, error, and abuse?
   * Preface

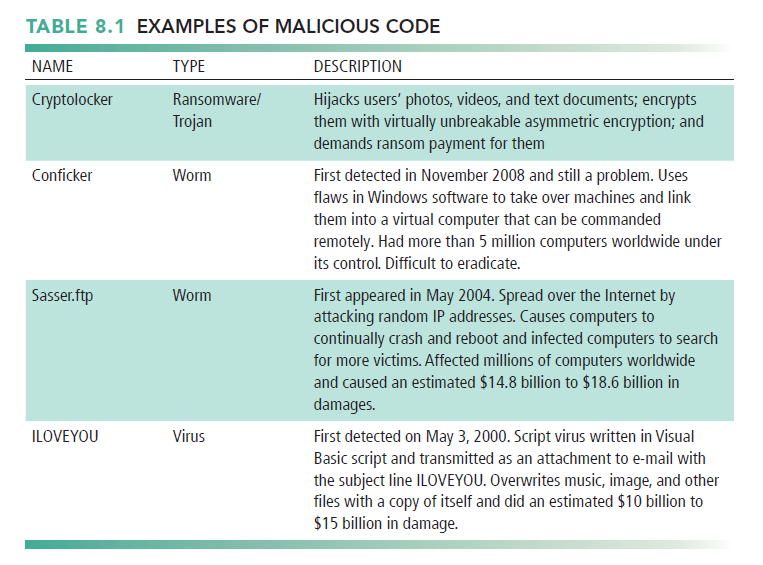
* Security
* the policies, procedures, and technical measures used to prevent unauthorized access, alteration, theft, or physical damage to information systems.
* Control
* methods, policies, and organizational procedures that ensure the safety of the organization’s assets, the accuracy and reliability of its records, and operational adherence to management standards.
  + Why Systems are Vulnerable
* Preface
* Accessibility of networks
* Hardware problems (breakdowns, configuration errors, damage from improper use or crime)
* Software problems (programming errors, installation errors, unauthorized changes)
* Disasters
* Use of networks/computers outside of firm’s control
* Loss and theft of portable devices



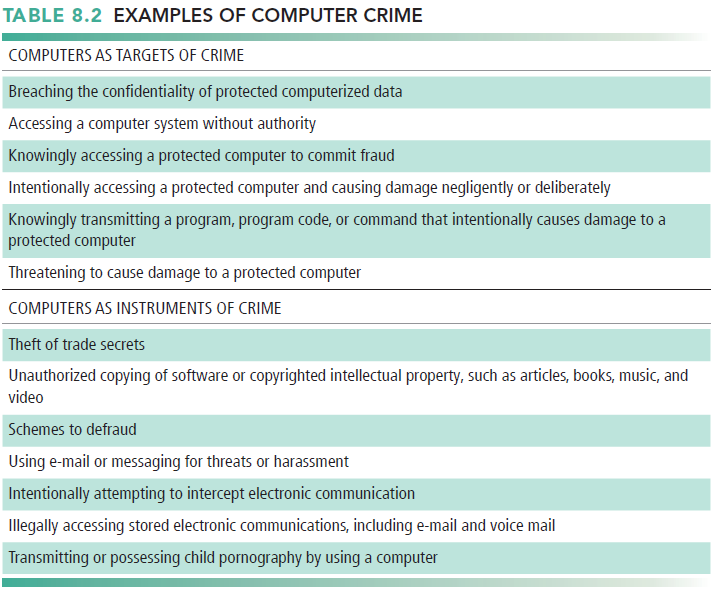
* Internet Vulnerabilities
* Large public networks are more vulnerable than internal networks
  + Network open to anyone
* Size of Internet means abuses can have wide impact
* When the Internet becomes part of the corporate network, the organization’s information systems are even more vulnerable to actions from outsiders
* Use of fixed Internet addresses with cable / DSL modems creates fixed targets for hackers
* Unencrypted VOIP
* E-mail, P2P, IM
  + Interception
  + Attachments with malicious software
  + Transmitting trade secrets
* Wireless Security Challenges
* Radio frequency bands easy to scan
* SSIDs (service set identifiers)
  + Identify access points
  + Broadcast multiple times
  + Can be identified by sniffer programs
  + War driving - eavesdroppers drive by buildings or park outside and try to intercept wireless network traffic.
  + Once access point is breached, intruder can use OS to access networked drives and files
* set up rogue access points on a different radio channel in physical locations close to users to force a user’s radio network interface controller (NIC) to associate with the rogue access point.



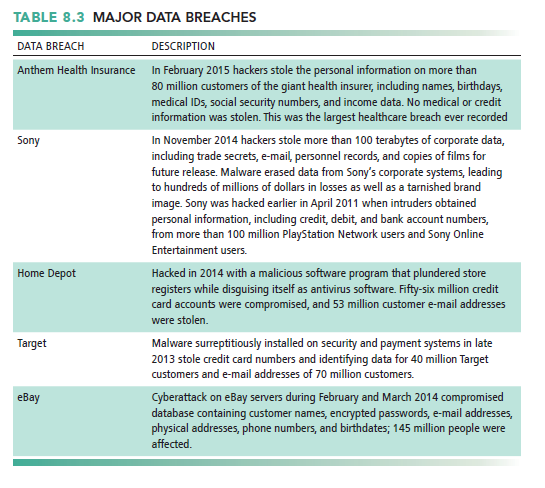
* + Malicious Software: Viruses, Worms, Trojan Horses, and Spyware



* Virus
* a rogue software program that attaches itself to other software programs or data files to be executed, usually without user knowledge or permission.
* Most computer viruses deliver a payload
* Viruses typically spread from computer to computer when humans take an action
* Worms
* independent computer programs that copy themselves from one computer to other computers over a network.
* worms can operate on their own
* destroy data and programs as well as disrupt or even halt the operation of computer networks.
* Worms and viruses spread by
* Downloads (drive-by downloads)
* E-mail, IM attachments
* Downloads on Web sites and social networks
* Smartphones as vulnerable as computers
* Hackers can do to a smartphone just about anything they can do to any Internet device
* more than 6 million samples of mobile malware
* Blogs, wikis, and social networking
* have emerged as new conduits for malware
* Members are more likely to trust messages they receive from friends, even if this communication is not legitimate.
* Internet of Things (IoT)
* required to protect IoT devices and platforms from both information attacks and physical tampering, to encrypt their communications
* simple processors and operating systems that may not support sophisticated security approaches.
* Trojan horses
* a software program that appears to be benign but then does something other than expected.
* a way for viruses or other malicious code to be introduced into a computer system
* An example of a modern-day Trojan horse is the Zeus Trojan
  + used to steal login credentials for banking by surreptitiously capturing people’s keystrokes as they use their computers.
* SQL injection attacks
* take advantage of vulnerabilities in poorly coded web application software to introduce malicious program code into a company’s systems and networks.
* An attacker uses this input validation error to send a rogue SQL query to the underlying database to access the database, plant malicious code, or access other systems on the network.
* Ransomware
* proliferating on both desktop and mobile devices
* tries to extort money from users by taking control of their computers or displaying annoying pop-up messages
* from downloading an infected attachment, clicking a link inside an e-mail, or visiting the wrong website
* example
  + WannaCry, CryptoLocker
* 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
  + Hackers and Computer Crime
* Preface
* Hacker
  + an individual who intends to gain unauthorized access to a computer system.
* Cracker
  + typically used to denote a hacker with criminal intent, although in the public press
* Activities include
  + System intrusion
  + System damage
  + Cybervandalism - Intentional disruption, defacement, destruction of Web site or corporate information system
* Spoofing and Sniffing
* 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
* Sniffing
  + a type of eavesdropping program that monitors information traveling over a network.
  + enable hackers to steal proprietary information from anywhere on a network
* Denial-of-Service Attacks
* denial-of-service (DoS)
  + Flooding server with thousands of false requests to crash the network
  + The network receives so many queries that it cannot keep up with them and is thus unavailable to service legitimate requests
* distributed denial-of-service (DDoS)
  + uses numerous computers to inundate and overwhelm the network from numerous launch points.
* Botnet
  + Networks of “zombie” PCs infiltrated by bot malware
  + Deliver 90 percent of world spam, 80 percent of world malware
  + Grum botnet: controlled 560K to 840K computers
* 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:



* Identity Theft
* Identity theft
  + an imposter obtains key pieces of personal information, such as social security numbers, driver’s license numbers, or credit card numbers, to impersonate someone else.
  + Identity theft has flourished on the Internet, with credit card files a major target of website hackers.
* Phishing
  + setting up fake websites or sending e-mail messages that look like those of legitimate businesses to ask users for confidential personal data.
* spear phishing
  + messages appear to come from a trusted source, such as an individual within the recipient’s own company or a friend.
* evil twins
  + wireless networks that pretend to offer trustworthy Wi-Fi connections to the Internet
* Pharming
  + redirects users to a bogus web page, even when the individual types the correct web page address into his or her browser.



* Click Fraud
* occurs when an individual or computer program fraudulently clicks an online ad without any intention of learning more about the advertiser or making a purchase.
* Global Threats: Cyberterrorism and Cyberwarfare
* Preface
  + The most popular sources of malware attacks include the United States, India, Germany, South Korea, China, Netherlands, United Kingdom, and Russia.
* Cyberwarfare
  + a state-sponsored activity designed to cripple and defeat another state or nation by penetrating its computers or networks to cause damage and disruption.
  + includes defending against these types of attacks.
  + Internal Threats: Employees
* Security threats often originate inside an organization
* Sloppy security procedures
* user lack of knowledge is the single greatest cause of network security breaches.
* Social engineering
* Tricking employees into revealing their passwords by pretending to be legitimate members of the company in need of information
* End users introduce errors by entering faulty data or by not following the proper instructions for processing data and using computer equipment.
* Information systems specialists may create software errors as they design and develop new software or maintain existing programs.
  + Software Vulnerability
* Commercial software contains flaws that create security vulnerabilities
* Commercial software contains flaws that create security vulnerabilities
* The main source of bugs is the complexity of decision-making code.
* Flaws can open networks to intruders
* zero-day vulnerabilities
* holes in the software unknown to its creator
* Hackers then exploit this security hole before the vendor becomes aware of the problem and hurries to fix it.
* Patches
* To correct software flaws once they are identified
* small pieces of software
* repair the flaws without disturbing the proper operation of the software
* patch management
  + users of the software to track these vulnerabilities, test, and apply all patches.

1. What is the business value of security and control?
   * Preface

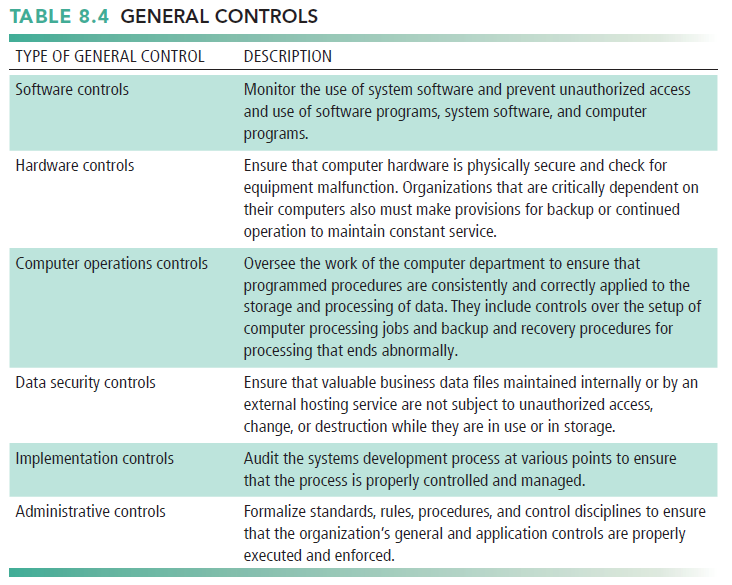
* Failed computer systems can lead to significant or total loss of business function.
* Firms now are more vulnerable than ever.
* Confidential personal and financial data
* Trade secrets, new products, strategies
* A security breach may cut into a firm’s market value almost immediately.
* Inadequate security and controls also bring forth issues of liability.
  + Legal and Regulatory Requirements for Electronic Records Management
* 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
  + Electronic Evidence and Computer Forensics
* 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
* may reside on computer storage media in the form of computer files and as ambient data , which are not visible to the average user.
* The cost of responding to a discovery request can be enormous if the company has trouble assembling the required data or the data

have been corrupted or destroyed

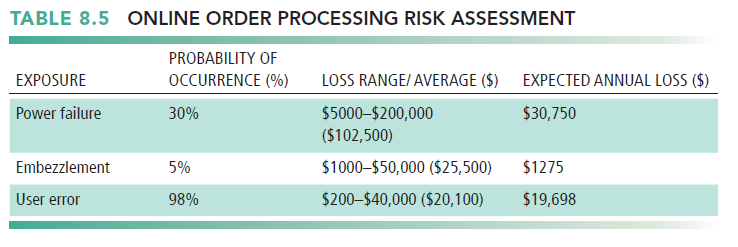
* + Courts now impose severe financial and even criminal penalties for improper destruction of electronic documents.
* Computer forensics
* Scientific collection, examination, authentication, preservation, and analysis of data from computer storage media for use as evidence in court of law
* Includes recovery of ambient and hidden data
* It deals with the following problems.
  + Recovering data from computers while preserving evidential integrity
  + Securely storing and handling recovered electronic data
  + Finding significant information in a large volume of electronic data
  + Presenting the information to a court of law

1. What are the components of an organizational framework for security and control?
   * Information Systems Controls

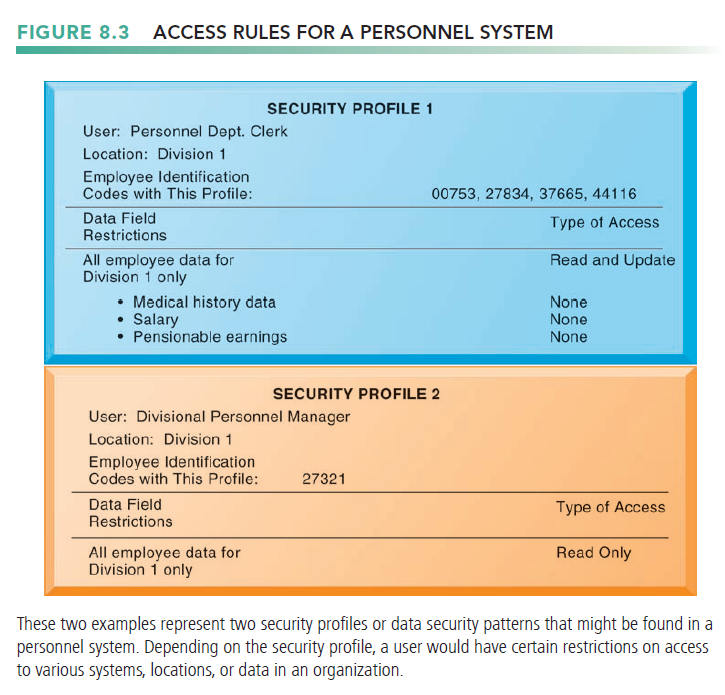
* Manual and automated controls
* General controls
* govern the design, security, and use of computer programs and the security of data files in general throughout the organization’s information technology infrastructure.
* general controls apply to all computerized applications
* combination of hardware, software, and manual procedures that create an overall control environment.
* include software controls, physical hardware controls, computer operations controls, data security controls, controls over the systems development process, and administrative controls



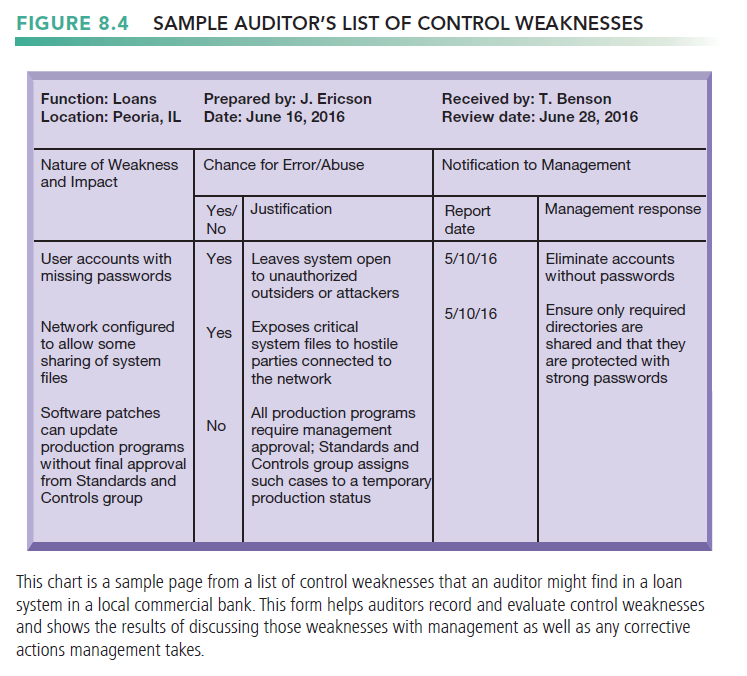
* application controls
* specific controls unique to each computerized application, such as payroll or order processing
* Include both automated and manual procedures
  + ensure that only authorized data are completely and accurately processed by that application.
* Application controls can be classified as
  + 1. Input controls
  + check data for accuracy and completeness when they enter the system
  + input controls for input authorization, data conversion, data editing, and error handling
    1. Processing controls
  + data are complete and accurate during updating.
    1. Output controls
  + ensure that the results of computer processing are accurate, complete, and properly distributed.
  + Risk Assessment
* determines the level of risk to the firm if a specific activity or process is not properly controlled
* Types of threat
* Probability of occurrence during year
* Potential losses, value of threat
* Expected annual loss



* + Security Policy
* consists of statements ranking information risks, identifying acceptable security goals, and identifying the mechanisms for achieving these goals.
* Drives other policies
* acceptable use policy (AUP)
  + defines acceptable uses of the firm’s information resources and computing equipment
  + A good AUP defines unacceptable and acceptable actions for every user and specifies consequences for noncompliance.
* Authorization policies
  + Determine differing levels of user access to information assets
* identity management.
* consists of business processes and software tools for identifying the valid users of a system and controlling their access to system resources.
  + Identifies and authorizes different categories of users
  + Specifies which portion of system users can access
  + Authenticating users and protects identities
* identity management system
  + capture the access rules for different levels of users

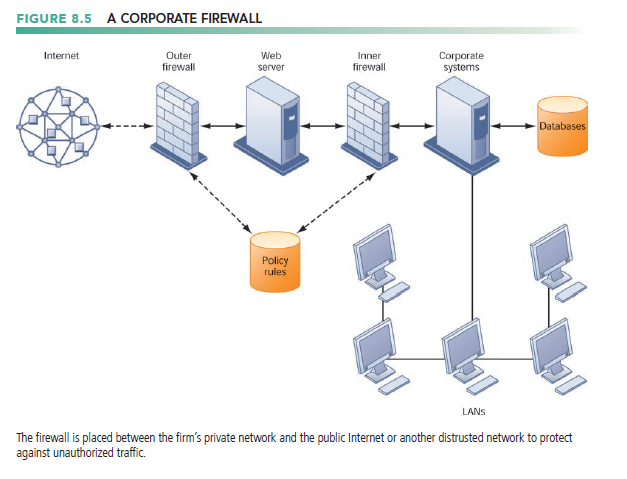


* + Disaster Recovery Planning and Business Continuity Planning
* Disaster recovery planning
* planning devises plans for the restoration of disrupted computing and communications services.
* Focus primarily on the technical issues involved in keeping systems up and running
* Business continuity planning
* focuses on how the company can restore business operations after a disaster strikes.
* identifies critical business processes and determines action plans for handling mission-critical functions if systems go down
* Business managers and information technology specialists
* 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
* Examines firm’s overall security environment as well as controls governing individual information systems
* Examines firm’s overall security environment as well as controls governing individual information systems
* may also examine data quality.
* review technologies, procedures, documentation, training, and personnel.
* Lists and ranks all control weaknesses and estimates probability of their occurrence
* assesses the financial and organizational impact of each threat

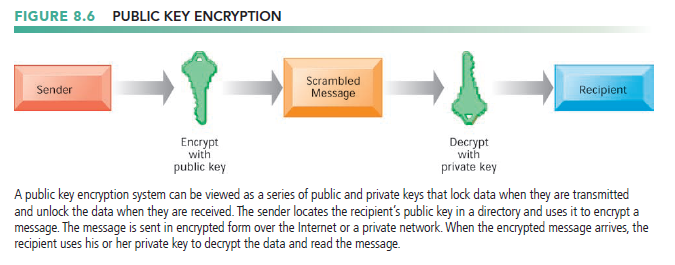


1. What are the most important tools and technologies for safeguarding information resources?
   * Identity Management and Authentication

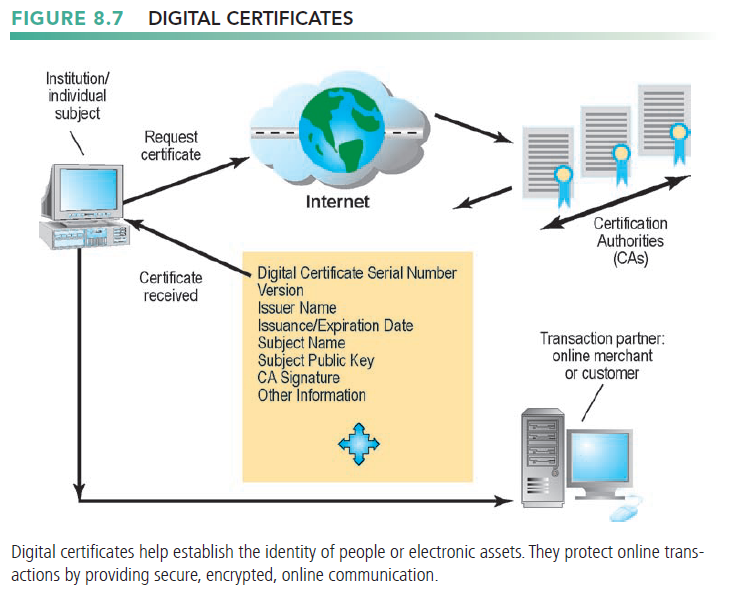
* Identity management software
* Automates the process of keeping track of all these users and their system privileges
* assigning each user a unique digital identity for accessing each
* includes tools for authenticating users, protecting user identities, and controlling access to system resources.
* Authentication
* the ability to know that a person is who he or she claims to be.
* Password systems
* Tokens
* Smart cards
* Biometric authentication
* Two-factor authentication
  + Firewalls, Intrusion Detection Systems, and Antivirus Software
* Firewalls
* prevent unauthorized users from accessing private networks
* a combination of hardware and software that controls the flow of incoming and outgoing network traffic
* the firewall often resides on a specially designated computer separate from the rest of the network
* identifies names, IP addresses, applications, and other characteristics of incoming traffic.
* Technologies include:
  + 1. Static packet filtering
  + examines selected fields in the headers of data packets flowing back and forth between the trusted network and the Internet, examining individual packets in isolation.
    1. Stateful inspection
  + provides additional security by determining whether packets are part of an ongoing dialogue between a sender and a receiver.
    1. Network address translation (NAT)
  + Conceals the IP addresses of the organization’s internal host computer(s) to prevent sniffer programs outside the firewall from ascertaining them and using that information to penetrate internal systems.
    1. Application proxy filtering
  + Application proxy filtering examines the application content of packets.
  + A proxy server stops data packets originating outside the organization, inspects them, and passes a proxy to the other side of the firewall.



* Intrusion Detection Systems
* full-time monitoring tools placed at the most vulnerable points or hot spots of corporate networks to detect and deter intruders continually.
* 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 Systems (UTM)
* combined into a single appliance various security tools, including firewalls, virtual private networks, intrusion detection systems, and web content filtering and anti-spam software.
  + Securing Wireless Networks
* WEP(Wired Equivalent Privacy)
* encryption keys are relatively easy to crack.
* Assigning unique name to network’s SSID and not broadcasting SSID
* Using it with VPN technology
* Wi-Fi Alliance finalized WPA2 specification, replacing WEP with stronger standards
* Continually changing keys
* Encrypted authentication system with central server
  + Encryption and Public Key Infrastructure
* Encryption
* the process of transforming plain text or data into cipher text that cannot be read by anyone other than the sender and the intended receiver
* Secure Sockets Layer (SSL) and successor Transport Layer Security (TLS)
* enable client and server computers to manage encryption and decryption activities as they communicate with each other during a secure web session.
* designed to establish a secure connection between two computers.
* Secure Hypertext Transfer Protocol (S-HTTP)
* encrypting data flowing over the Internet, but it is limited to individual messages
* 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



* 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
  + Symantec, GoDaddy, and Comodo.
* 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
  + Ensuring System Availability
* Preface
* Online transaction processing requires 100% availability, no downtime
  + Downtime refers to periods of time in which a system is not operational.
* Fault-tolerant computer systems
  + contain redundant hardware, software, and power supply components that create an environment that provides continuous, uninterrupted service.
  + use special software routines or self-checking logic built into their circuitry to detect hardware failures and automatically switch to a backup device
  + can be removed and repaired without disruption to the computer or downtime.
* Controlling Network Traffic: Deep Packet Inspection(DP)
* examines data files and sorts out low-priority online material while assigning higher priority to business-critical files.
* it decides whether a specific data packet can continue to its destination or should be blocked or delayed while more important traffic proceeds.
* Security Outsourcing
* Managed security service providers (MSSPs)
  + monitor network activity and perform vulnerability testing and intrusion detection
* SecureWorks, AT&T, Verizon, IBM, Perimeter eSecurity, and Symantec are leading providers of MSSP services.
  + Security Issues for Cloud Computing and the Mobile Digital Platform
* 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
  + These kinds of controls can be written into the service level agreement (SLA) before signing with a cloud provider.
* Cloud Security Alliance (CSA)
  + created industrywide standards for cloud security, specifying best practices to secure cloud computing.
* 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
  + 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
* Early and regular testing
* Walkthrough
* Review of specification or design document by small group of qualified people
* Debugging
* Process by which errors are eliminated