Ethical, Social and Security Issues in Information Systems

Acknowledgement: Most of the slides Management Information Systems: Managing the Digital Firm, by Laudon, J. and Laudon, K., Published by: Prentice Hall; 11th edition (2010)

Some Ethical & Social cases

- **What ethical, social, and political issues are raised by information systems?**
- **What are impacts of having and obeying Ethical & Privacy cases?**

Some Ethical & Social Issues

- **In Australia**
  - It is illegal to marry before the age of 18
  - It unethical but not illegal to bear a child at the age of 15
  - To live together (male & female) is neither illegal nor unethical
- Do all countries have the same ethical and social code
- Name a few international ethical and social codes?

- **In Australia**
  - One doctor can not provide patient data without written permission from the patient
  - Medical labs can not provide report to any one other than the patient
  - Personal data held in one organization can not be used by another organization (this includes police, defense, Foreign Affairs and taxation)
  - Australian public doesn't want national ID card for the fear of privacy concerns
  - Flight info of one can not be given to other
  - One can not make inquiry on behalf of others
  - Video evidence in courts is not acceptable

A Case

- Someone was bugging me …. I learned that he had .. and I also knew that …..
- I was anxious to verify my info from the systems that I had access to and then perhaps initiate an action against him. But I didn't didn’t access info from the systems, because…..
- Why?

A Case

- One person made a mess in the toilet at work while making ablution (wadhu)
- Someone objected to it
- Person said, my English was poor, could you write
- He did
- The person went to court, who ordered a compensation $$$$

A Case

- A friend of mine working in a government department, one day, gave me a CD containing many records of airplane accidents in Australia
- When I informed of this to my supervisor, he said the CD was a problem bomb and I should destroy it immediately, which I did
- Why did my supervisor warned me?

Ethics

Principles of right and wrong that individuals, acting as free moral agents, use to make choices to guide their behaviors

- **Information systems and ethics**
  - **Information systems raise new ethical questions because they create opportunities for:**
    - **Intense social change, threatening existing distributions of power, money, rights, and obligations**
    - **New kinds of crime**

A Case

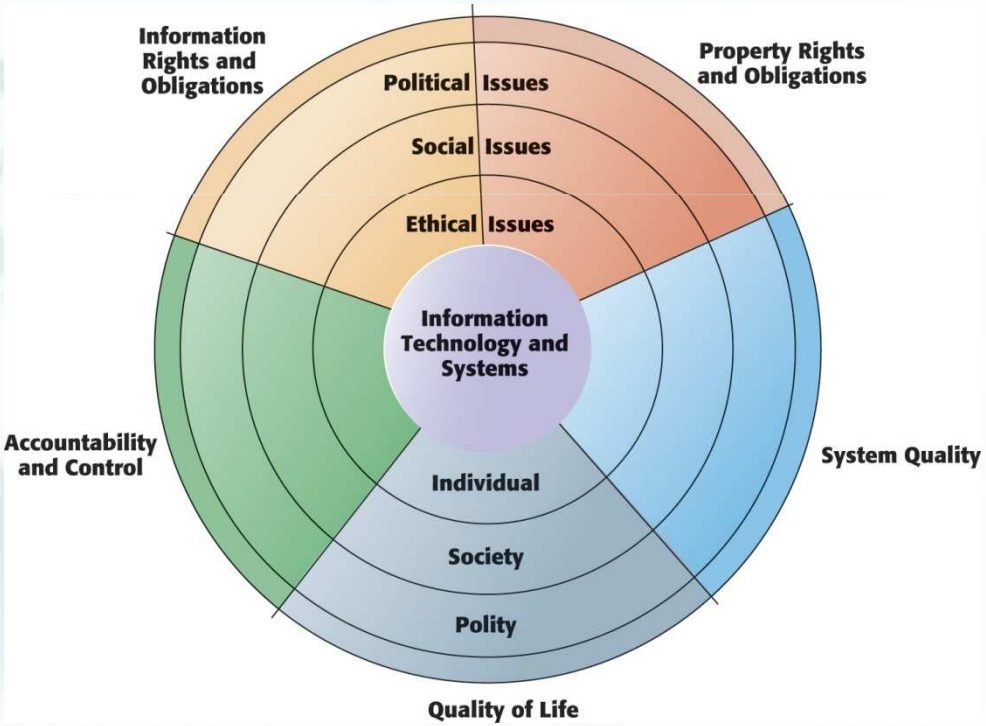
- While working at an information sensitive government department, I was approached by a friend to find out.....
- What were the privacy issues?
- What you think could be penalty the penaly had I provided info

A Model for Thinking About Ethical, Social, and Political Issues

- Society as a calm pond
- IT as rock dropped in pond, creating ripples of new situations not covered by old rules
- Social and political institutions cannot respond overnight to these ripples—it may take years to develop etiquette, expectations, laws
    - Requires understanding of ethics to make choices in legally gray areas

Understanding Ethical and Social Issues Related to Systems

The Relationship Among Ethical, Social, Political Issues in an Information Society



The introduction of new information technology has a ripple effect, raising new ethical, social, and political issues that must be dealt with on the individual, social, and political levels. These issues have five moral dimensions: information rights and obligations, property rights and obligations, system quality, quality of life, and accountability and control.

Figure 12-1

Five Moral Dimensions of the Information Age

1. Information rights and obligations
2. Property rights and obligations
3. Accountability and control
4. System quality
5. Quality of life

Key Technology Trends That Raise Ethical Issues

- Doubling of computer power
  - More organizations depend on computer systems for critical operations
- Rapidly declining data storage costs
  - Organizations can easily maintain detailed databases on individuals
- Networking advances and the Internet
  - Copying data from one location to another and accessing personal data from remote locations are much easier

Key Technology Trends That Raise Ethical Issues

- Advances in data analysis techniques
  - Companies can analyze vast quantities of data gathered on individuals for:
    - Profiling
      - Combining data from multiple sources to create dossiers of detailed information on individuals
    - Nonobvious relationship awareness (NORA)
      - Combining data from multiple sources to find obscure hidden connections that might help identify criminals or terrorists

Airport Abbreviation

- One fine day I received two ASIO officers who came to see me at work at the UC
- At that time I then was the General Secretary of the Islamic Society of my state
- The officers talked about general issues for over half an hour
- At the end they discussed a specific issue with me

Credit card purchases can make personal information available to market researchers, telemarketers, and direct-mail companies. Advances in information technology facilitate the invasion of privacy.

Understanding Ethical and Social Issues Related to Systems

Nonobvious Relationship Awareness (NORA)

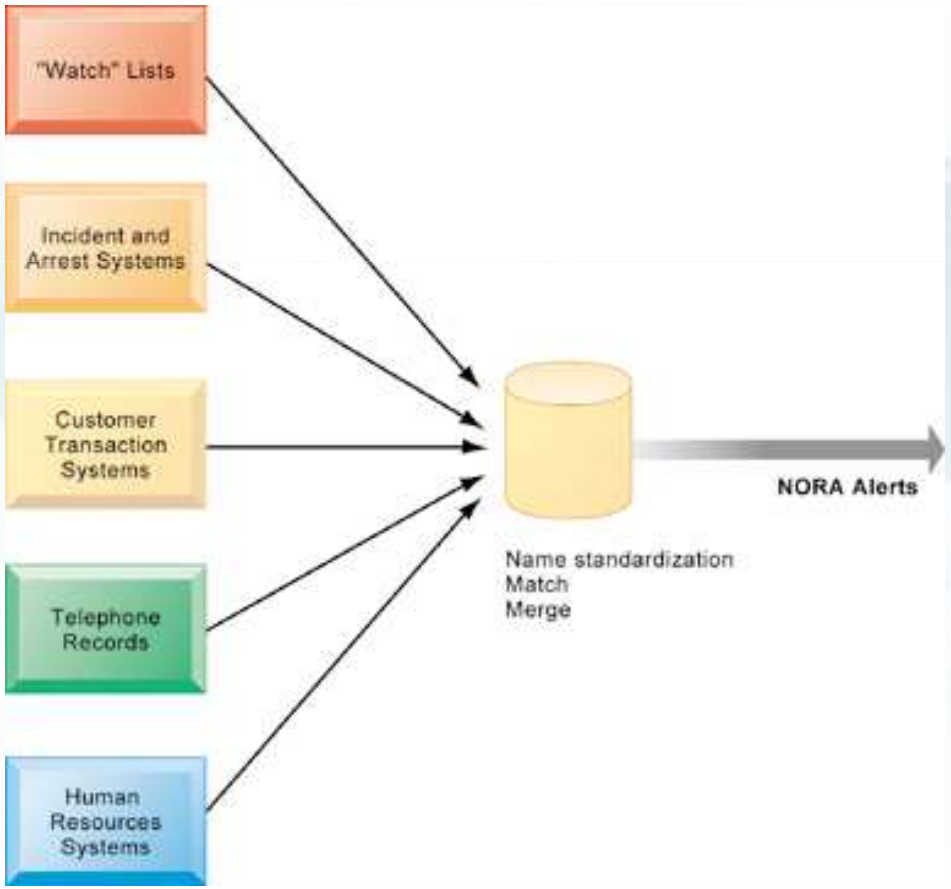


Figure 12-2

NORA technology can take information about people from disparate sources and find obscure, nonobvious relationships. It might discover, for example, that an applicant for a job at a casino shares a telephone number with a known criminal and issue an alert to the hiring manager.

Ethics in an Information Society

- **Basic concepts for ethical analysis**
  - **Responsibility:**
    - Accepting the potential costs, duties, and obligations for decisions
  - **Accountability:**
    - Mechanisms for identifying responsible parties
  - **Liability:**
    - Permits individuals (and firms) to recover damages done to them
  - **Due process:**
    - Laws are well known and understood, with an ability to appeal to higher authorities

- **Ethical analysis: A five-step process**

1. **Identify and clearly describe the facts**
2. **Define the conflict or dilemma and identify the higher-order values involved**
3. **Identify the stakeholders**
4. **Identify the options that you can reasonably take**
5. **Identify the potential consequences of your options**

- **Candidate Ethical Principles**
  - **Golden Rule**
    - Do unto others as you would have them do unto you
  - **Immanuel Kant's Categorical Imperative**
    - If an action is not right for everyone to take, it is not right for anyone
  - **Descartes' rule of change**
    - If an action cannot be taken repeatedly, it is not right to take at all

- **Candidate Ethical Principles (cont.)**
  - **Utilitarian Principle**
    - Take the action that achieves the higher or greater value
  - **Risk Aversion Principle**
    - Take the action that produces the least harm or least potential cost
  - **Ethical "no free lunch" rule**
    - Assume that virtually all tangible and intangible objects are owned by someone unless there is a specific declaration otherwise

Ethics in an Information Society

- **Professional codes of conduct**
  - Promulgated by associations of professionals
    - E.g. AMA, ABA, AITP, ACM
  - Promises by professions to regulate themselves in the general interest of society
- **Real-world ethical dilemmas**
  - One set of interests pitted against another
  - E.g. Right of company to maximize productivity of workers vs. workers right to use Internet for short personal tasks

Information Rights: Privacy and Freedom in the Internet Age

- **Privacy:**
  - **Claim of individuals to be left alone, free from surveillance or interference from other individuals, organizations, or state. Claim to be able to control information about yourself**
- **In U.S., privacy protected by:**
  - **First Amendment (freedom of speech)**
  - **Fourth Amendment (unreasonable search and seizure)**
  - **Additional federal statues (e.g. Privacy Act of 1974)**

- **Fair information practices:**
  - Set of principles governing the collection and use of information
  - Basis of most U.S. and European privacy laws
  - Based on mutuality of interest between record holder and individual
  - Restated and extended by FTC in 1998 to provide guidelines for protecting online privacy

- **FTC FIP principles:**
  - **Notice/awareness (core principle):**
    - **Web sites must disclose practices before collecting data**
  - **Choice/consent (core principle):**
    - **Consumers must be able to choose how information is used for secondary purposes**
  - **Access/participation:**
    - **Consumers must be able to review, contest accuracy of personal data**

- FTC FIP principles (cont.)
  - Security:
    - Data collectors must take steps to ensure accuracy, security of personal data
  - Enforcement:
    - Must be mechanism to enforce FIP principles

- European Directive on Data Protection:
  - Requires companies to inform people when they collect information about them and disclose how it will be stored and used.
  - Requires informed consent of customer
  - EU member nations cannot transfer personal data to countries without similar privacy protection (e.g. U.S.)
  - U.S. businesses use safe harbor framework
    - Self-regulating policy and enforcement that meets objectives of government legislation but does not involve government regulation or enforcement.

- **Internet Challenges to Privacy:**
  - **Cookies**
    - Tiny files downloaded by Web site to visitor's hard drive
    - Identify visitor's browser and track visits to site
    - Allow Web sites to develop profiles on visitors
  - **Web bugs**
    - Tiny graphics embedded in e-mail messages and Web pages
    - Designed to monitor who is reading message and transmit information to another computer
  - **Spyware**
    - Surreptitiously installed on user's computer
    - May transmit user's keystrokes or display unwanted ads

The Moral Dimensions of Information Systems

- U.S. allows businesses to gather transaction information and use this for other marketing purposes (Data selling in India)
- Online industry promotes self-regulation over privacy legislation, however, extent of responsibility taken varies
- Most Web sites do not have any privacy policies

- **Technical solutions**
  - **The Platform for Privacy Preferences (P3P)**
    - **Allows Web sites to communicate privacy policies to visitor's Web browser – user**
    - **User specifies privacy levels desired in browser settings**
    - **E.g. "medium" level accepts cookies from first-party host sites that have opt-in or opt-out policies but rejects third-party cookies that use personally identifiable information without an opt-in policy**

The Moral Dimensions of Information Systems

How Cookies Identify Web Visitors

1. The Web server reads the user's Web browser and determines the operating system, browser name, version number, Internet address, and other information.
2. The server transmits a tiny text file with user identification information called a cookie, which the user's browser receives and stores on the user's computer hard drive.
3. When the user returns to the Web site, the server requests the contents of any cookie it deposited previously in the user's computer.
4. The Web server reads the cookie, identifies the visitor, and calls up data on the user.

Cookies are written by a Web site on a visitor's hard drive. When the visitor returns to that Web site, the Web server requests the ID number from the cookie and uses it to access the data stored by that server on that visitor. The Web site can then use these data to display personalized information.

Figure 12-3

The Moral Dimensions of Information Systems

Web sites are posting their privacy policies for visitors to review. The TRUSTe seal designates Web sites that have agreed to adhere to TRUSTe's established privacy principles of disclosure, choice, access, and security.

Property Rights: Intellectual Property

- Intellectual property: Intangible property of any kind created by individuals or corporations
- Three main ways that intellectual property is protected
  - Trade secret: Intellectual work or product belonging to business, not in the public domain
  - Copyright: Statutory grant protecting intellectual property from being copied for the life of the author, plus 70 years
  - Patents: Grants creator of invention an exclusive monopoly on ideas behind invention for 20 years

- **Challenges to Intellectual Property Rights**
  - Digital media different from physical media (e.g. books)
    - Ease of replication
    - Ease of transmission (networks, Internet)
    - Difficulty in classifying software
    - Compactness
    - Difficulties in establishing uniqueness
- **Digital Millennium Copyright Act (DMCA)**
  - Makes it illegal to circumvent technology-based protections of copyrighted materials

- **Accountability, Liability, Control**
  - **Computer-related liability problems**
    - **If software fails, who is responsible?**
      - **If seen as part of machine that injures or harms, software producer and operator may be liable**
      - **If seen as similar to book, difficult to hold author/publisher responsible**
      - **What should liability be if software seen as service? Would this be similar to telephone systems not being liable for transmitted messages?**

Quality of Life: Equity, Access, and Boundaries

- **Negative social consequences of systems**
  - **Balancing power: Although computing power decentralizing, key decision-making remains centralized**
  - **Rapidity of change: Businesses may not have enough time to respond to global competition**
  - **Maintaining boundaries: Computing, Internet use lengthens work-day, infringes on family, personal time**
  - **Dependence and vulnerability: Public and private organizations ever more dependent on computer systems**

The Moral Dimensions of Information Systems

- **Computer crime and abuse**
  - **Computer crime: Commission of illegal acts through use of compute or against a computer system – computer may be object or instrument of crime**
  - **Computer abuse: Unethical acts, not illegal**
    - **Spam: High costs for businesses in dealing with spam**
- **Employment: Reengineering work resulting in lost jobs**
- **Equity and access – the digital divide:**
  - **Certain ethnic and income groups in the United States less likely to have computers or Internet access**
  - **What about poor nations?**

- **Health risks:**
  - **Repetitive stress injury (RSI)**
    - **Largest source is computer keyboards**
    - **Carpal Tunnel Syndrome (CTS)**
  - **Computer vision syndrome (CVS)**
  - **Technostress**
  - **Role of radiation, screen emissions, low-level electromagnetic fields**

The Moral Dimensions of Information Systems

Repetitive stress injury (RSI) is the leading occupational disease today. The single largest cause of RSI is computer keyboard work

Punching bag

Interactive Session: People
Flexible Scheduling at Wal-Mart: Good or Bad for Employees?

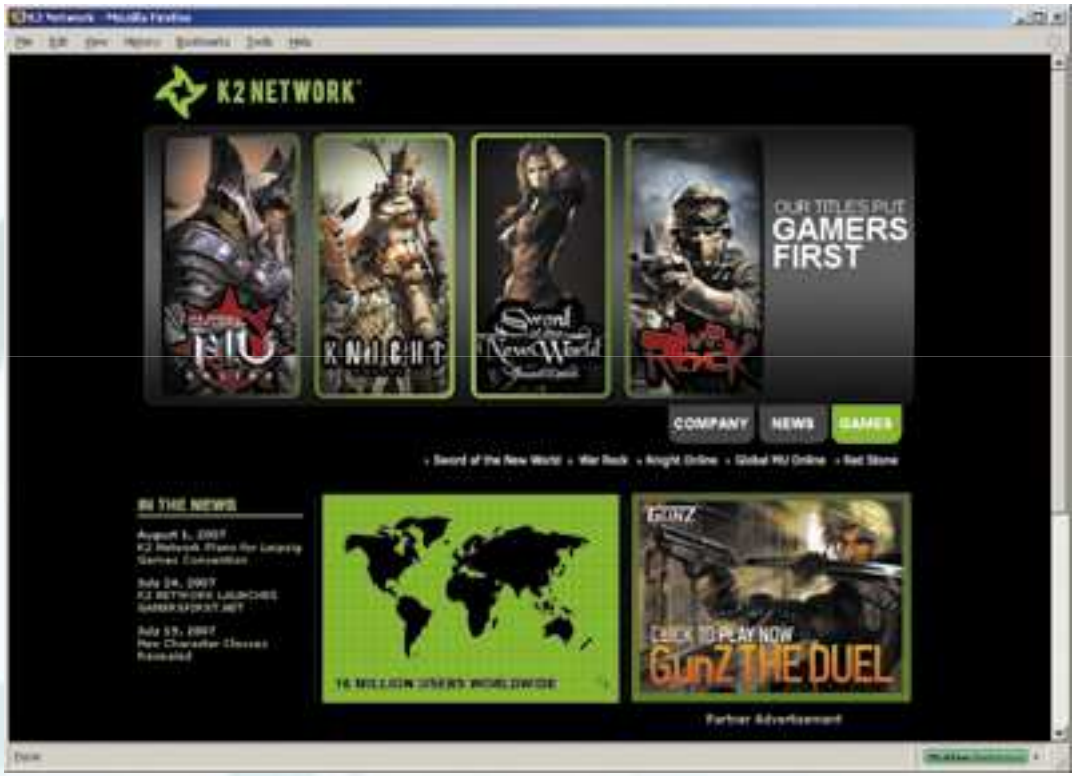
- Read the Interactive Session and then discuss the following questions:
  - What is the ethical dilemma facing Wal-Mart in this case? Do Wal-Mart's associates also face an ethical dilemma? If so, what is it?
  - What ethical principles apply to this case? How do they apply?
  - What are the potential effects of computerized scheduling on employee morale? What are the consequences of these effects for Wal-Mart?

STUDENT LEARNING OBJECTIVES

- Why are information systems vulnerable to destruction, error, and abuse?
- What is the business value of security and control?
- What are the components of an organizational framework for security and control?
- Evaluate the most important tools and technologies for safeguarding information resources.

Online Games Need Security, Too

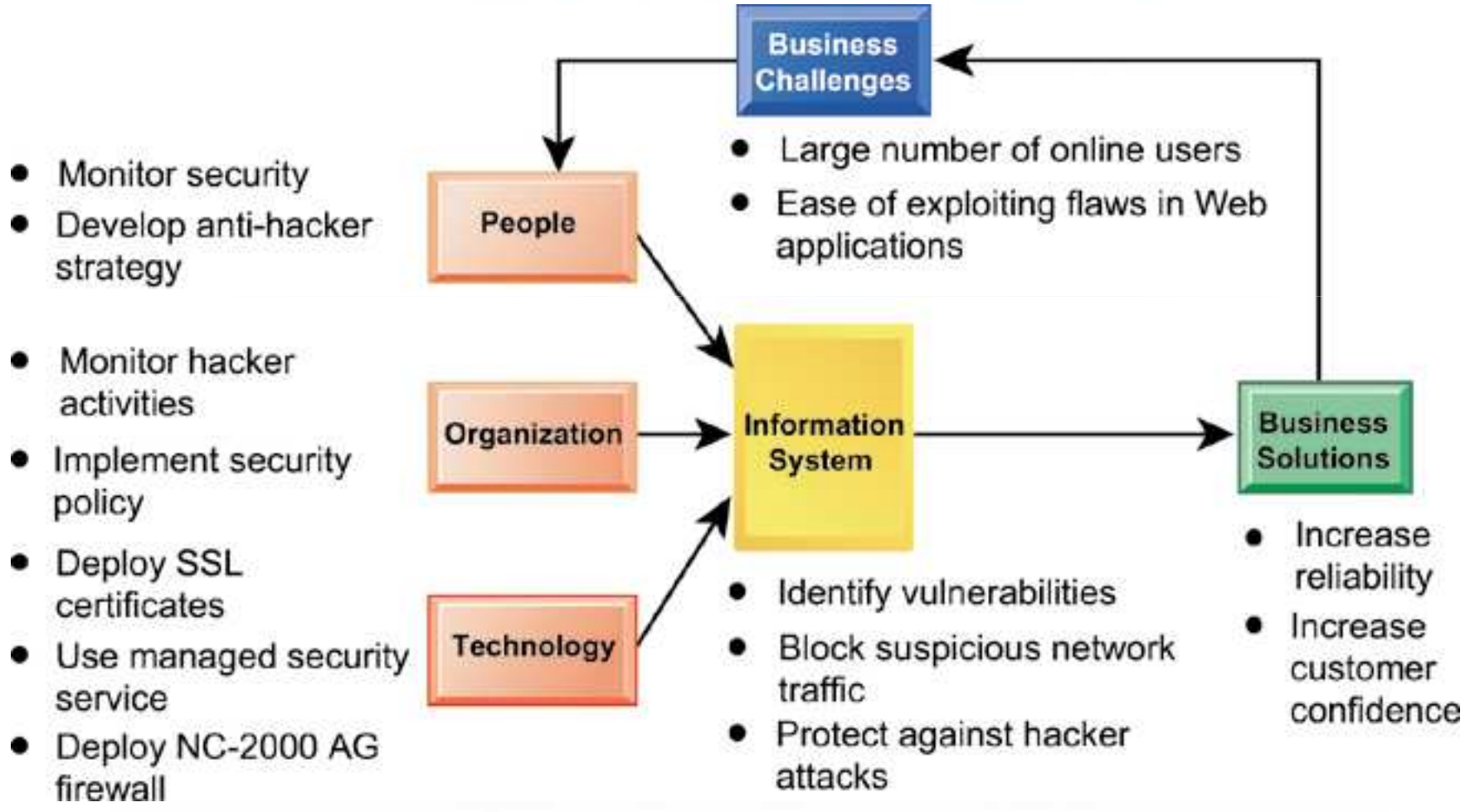
- **Problem:** Threat of attacks from hackers hoping to steal information or gaming assets.
- **Solutions: Deploy an advanced security system** to identify threats and reduce hacking attempts.



Online Games Need Security, Too

- **NetContinuum's NC-2000 AG firewall and Cenzic's ClickToSecure service work in tandem to minimize the chance of a security breach.**
- **Demonstrates IT's role in combating cyber crime.**
- **Illustrates digital technology's role in achieving security on the Web.**

Online Games Need Security, Too



System Vulnerability and Abuse

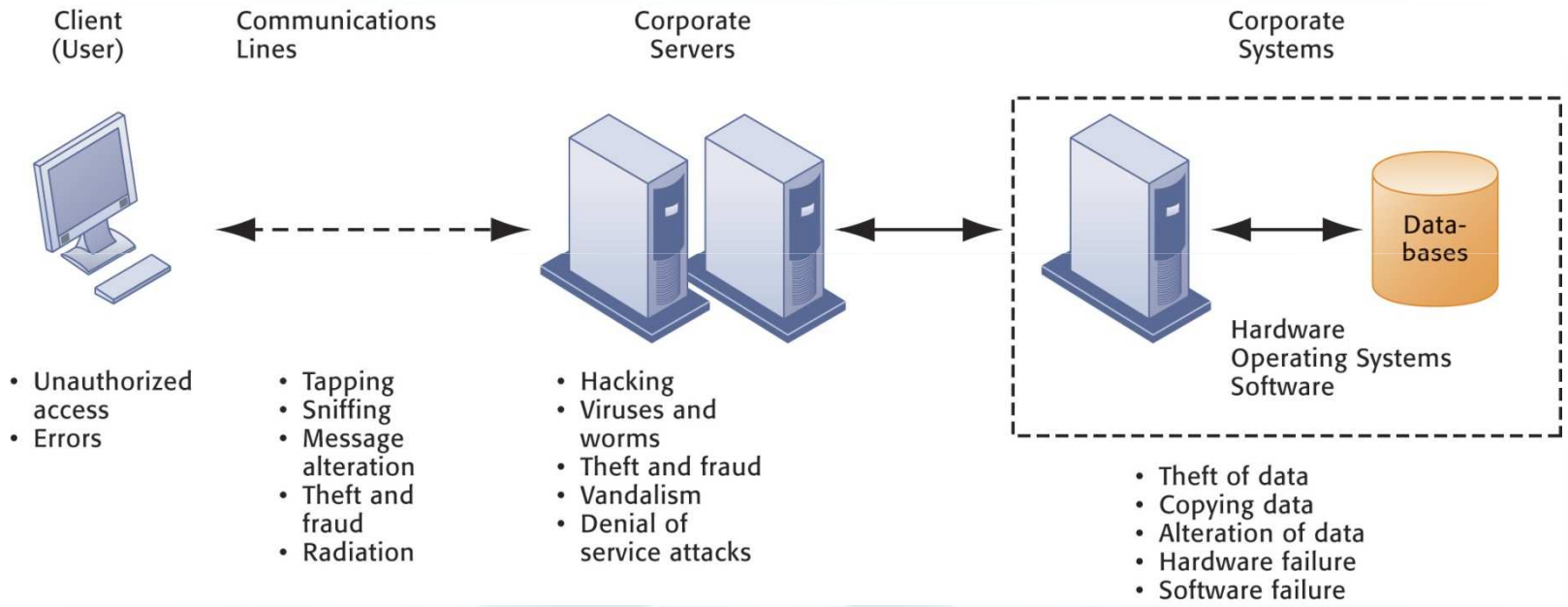
- **An unprotected computer connected to Internet may be disabled within seconds**
- **Security:**
  - Policies, procedures and technical measures used to prevent unauthorized access, alteration, theft, or physical damage to information systems
- **Controls:**
  - Methods, policies, and organizational procedures that ensure safety of organization's assets; accuracy and reliability of its accounting records; and operational adherence to management standards

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**
  - E.g. with domestic or offshore outsourcing vendors

System Vulnerability and Abuse

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.

Figure 7-1

- **Internet vulnerabilities**
  - 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

- **Wireless security 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
    - Basic specification uses shared password for both users and access point
    - Users often fail to use security features

Wi-Fi Security Challenges

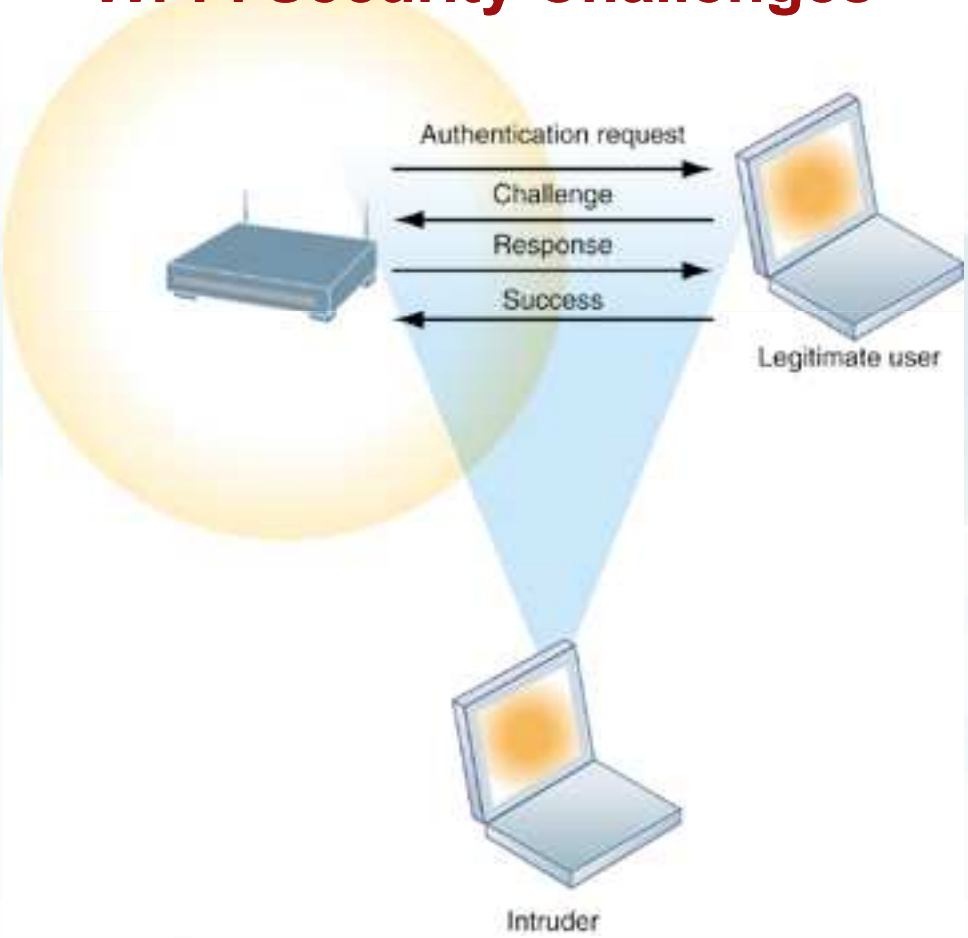


Figure 7-2

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.

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

- **Malware**
  - **Viruses**
    - Rogue software program that attaches itself to other software programs or data files in order to be executed
  - **Worms**
    - Independent computer programs that copy themselves from one computer to other computers over a network.
  - **Trojan horses**
    - Software program that appears to be benign but then does something other than expected.

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

- **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

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

Hackers and Computer Crime

- **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, etc.

Hackers and Computer Crime

- **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

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, e.g.:**
    - Breaching confidentiality of protected computerized data
    - Accessing a computer system without authority
  - **Computer may be instrument of crime, e.g.:**
    - Theft of trade secrets
    - Using e-mail for threats or harassment

Hackers and Computer Crime

- **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

Hackers and Computer Crime

- **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

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

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**
  - Vendors release small pieces of software to repair flaws
  - However, amount of software in use can mean exploits created faster than patches 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 more vulnerable than ever
- A security breach may cut into firm's market value almost immediately
- Inadequate security and controls also bring forth issues of liability

Legal and Regulatory Requirements for Electronic Records Management

- 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

Electronic Evidence and Computer Forensics

- **Evidence for white collar crimes often found in digital form**
  - Data stored on computer devices, e-mail, instant messages, e-commerce transactions
- **Proper control of data can save time, 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

- **Information systems 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

- **Types of general controls**
  - **Software controls**
  - **Hardware controls**
  - **Computer operations controls**
  - **Data security controls**
  - **Implementation controls**
  - **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
  - Include:
    - **Input controls**
    - **Processing controls**
    - **Output controls**

- **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**

EXPOSURE	PROBABILITY	LOSS RANGE	EXPECTED ANNUAL LOSS
Power failure	30%	$5K - $200K	$30,750
Embezzlement	5%	$1K - $50K	$1,275
User error	98%	$200 - $40K	$19,698

- **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
    - **Authorization policies**
      - Determine differing levels of user access to information assets

- **Authorization management systems**
  - Establish where and when a user is permitted to access certain parts of a Web site or corporate database.
  - Allow each user access only to those portions of system that person is permitted to enter, based on information established by set of access rules, profile

Disaster Recovery Planning and Business Continuity Planning

- **Disaster recovery planning:** Devises plans for restoration of disrupted services
- **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**
  - 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

Function: Loans **Prepared by: J. Ericson** **Received by: T. Benson**
Location: Peoria, IL **Date: June 16, 2008** **Review date: June 28, 2008**

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	5/10/08	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	5/10/08	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		

Figure 7-4

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.

Access Control

- Policies and procedures to prevent improper access to systems by unauthorized insiders and outsiders
  - Authorization
  - Authentication
    - Password systems
    - Tokens
    - Smart cards
    - Biometric authentication

Technologies and Tools for Security

This NEC PC has a biometric fingerprint reader for fast yet secure access to files and networks. New models of PCs are starting to use biometric identification to authenticate users.

Firewalls, Intrusion Detection Systems, and Antivirus Software

- Firewall:
  - Combination of hardware and software that prevents unauthorized users from accessing private networks
  - Technologies include:
    - Static packet filtering
    - Network address translation (NAT)
    - Application proxy filtering

Firewalls, Intrusion Detection Systems, and Antivirus Software

- **Intrusion detection systems:**
  - Monitor 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
  - Require continual updating

Securing Wireless Networks

- **WEP security can be improved:**
  - Activating it
  - Assigning unique name to network's 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

Digital Certificates

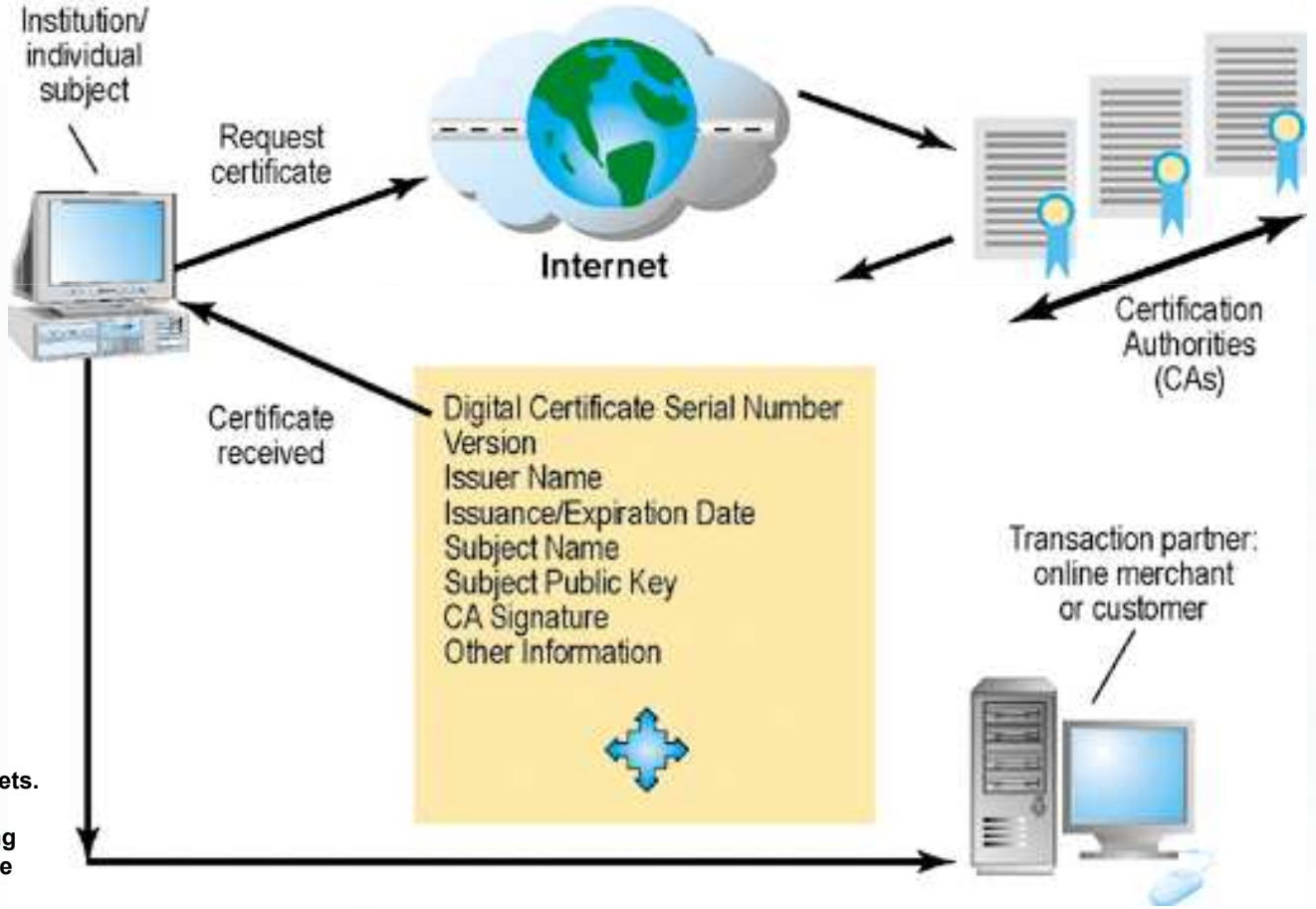


Figure 7-7

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

Ensuring System Availability

- **Online transaction processing requires 100% availability, no downtime**
- **Fault-tolerant computer systems**
  - For continuous availability, e.g. 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

Ensuring System Availability

- **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**
  - Deep packet inspection (DPI) (video and music blocking)
- **Security outsourcing**
  - Managed security service providers (MSSPs)

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

Interactive Session: Organizations
Can Salesforce.com On-Demand Remain in Demand?

- **Read the Interactive Session and then discuss the following questions:**
  - **How did the problems experienced by Salesforce.com impact its business?**
  - **How did the problems impact its customers?**
  - **What steps did Salesforce.com take to solve the problems? Were these steps sufficient?**
  - **List and describe other vulnerabilities discussed in this chapter that might create outages at Salesforce.com and measures to safeguard against them.**