Cyber Law and Policy

Lesson 4

Computer Crimes

Objectives

- As you read this chapter, consider the following questions:
  - What key trade-offs and ethical issues are associated with the safeguarding of data and information systems?
  - Why has there been a dramatic increase in the number of computer-related security incidents in recent years?
  - What are the most common types of computer security attacks?

Objectives (cont'd.)

- Who are the primary perpetrators of computer crime, and what are their objectives?
- What are the key elements of a multilayer process for managing security vulnerabilities based on the concept of reasonable assurance?
- What actions must be taken in response to a security incident?
- What is computer forensics, and what role does it play in responding to a computer incident?

IT Security Incidents: A Major Concern

- Security of information technology is of utmost importance
  - Safeguard:
    - Confidential business data
    - Private customer and employee data
  - Protect against malicious acts of theft or disruption
  - Balance against other business needs and issues
- Number of IT-related security incidents is increasing around the world

Why Computer Incidents Are So Prevalent

- Increasing complexity increases vulnerability
  - Computing environment is enormously complex
    - Continues to increase in complexity
    - Number of entry points expands continuously
    - Cloud computing and virtualization software
- Higher computer user expectations
  - Computer help desks under intense pressure
    - Forget to verify users' IDs or check authorizations
- Computer users share login IDs and passwords

Why Computer Incidents Are So Prevalent (cont'd.)

- Expanding/changing systems equal new risks
  - Network era
    - Personal computers connect to networks with millions of other computers
    - All capable of sharing information
  - Information technology
    - Global
    - Necessary tool for organizations to achieve goals
    - Increasingly difficult to match pace of technological change

Why Computer Incidents Are So Prevalent (cont'd.)

- Increased reliance on commercial software with known vulnerabilities
  - Exploit
    - Attack on information system
    - Takes advantage of system vulnerability
    - Due to poor system design or implementation
  - Patch
    - "Fix" to eliminate the problem
    - Users are responsible for obtaining and installing
    - Delays expose users to security breaches

Why Computer Incidents Are So Prevalent (cont'd.)

- Zero-day attack
  - Before a vulnerability is discovered or fixed
- U.S. companies rely on commercial software with known vulnerabilities

Types of Computer Crime

- Business attacks
- Financial attacks
- Terrorist attacks
- Objection attacks
- Fun attacks

Most Common Computer Crimes

- Fraud by computer manipulation
- Computer forgery
- Damage to or modifications of computer data or programs

Most Common Computer Crimes

- Unauthorized access to computer systems and service
- Unauthorized reproduction of legally protected computer programs

Computer Crimes Are Hard to Prosecute

- Lack of understanding
- Lack of physical evidence
- Lack of recognition of assets
- Lack of political impact
- Complexity of case
- Juveniles

Types of Exploits

- Computers as well as smartphones can be target
- Types of attacks
  - Virus
  - Worm
  - Trojan horse
  - Distributed denial of service
  - Rootkit
  - Spam
  - Phishing (spear-phishing, smishing, and vishing)

Viruses

- Pieces of programming code
- Usually disguised as something else
- Cause unexpected and undesirable behavior
- Often attached to files
- Deliver a “payload”
- Spread by actions of the “infected” computer user
  - Infected e-mail document attachments
  - Downloads of infected programs
  - Visits to infected Web sites

Worms

- Harmful programs
  - Reside in active memory of a computer
  - Duplicate themselves
- Can propagate without human intervention
- Negative impact of worm attack
  - Lost data and programs
  - Lost productivity
  - Additional effort for IT workers

Trojan Horses

- Malicious code hidden inside seemingly harmless programs
- Users are tricked into installing them
- Delivered via email attachment, downloaded from a Web site, or contracted via a removable media device
- Logic bomb
  - Executes when triggered by certain event

Distributed Denial-of-Service (DDoS) Attacks

- Malicious hacker takes over computers on the Internet and causes them to flood a target site with demands for data and other small tasks
  - The computers that are taken over are called zombies
  - Botnet is a very large group of such computers
- Does not involve a break-in at the target computer
  - Target machine is busy responding to a stream of automated requests
  - Legitimate users cannot access target machine

Rootkits

- Set of programs that enables its user to gain administrator-level access to a computer without the end user's consent or knowledge
- Attacker can gain full control of the system and even obscure the presence of the rootkit
- Fundamental problem in detecting a rootkit is that the operating system currently running cannot be trusted to provide valid test results

Spam

- Abuse of email systems to send unsolicited email to large numbers of people
  - Low-cost commercial advertising for questionable products
  - Method of marketing also used by many legitimate organizations
- Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act
  - Legal to spam if basic requirements are met

Spam (cont'd.)

- Completely Automated Public Turing Test to Tell Computers and Humans Apart (CAPTCHA)
  - Software generates tests that humans can pass but computer programs cannot

Phishing

- Act of using email fraudulently to try to get the recipient to reveal personal data
- Legitimate-looking emails lead users to counterfeit Web sites
- Spear-phishing
  - Fraudulent emails to an organization’s employees
- Smishing
  - Phishing via text messages
- Vishing
  - Phishing via voice mail messages

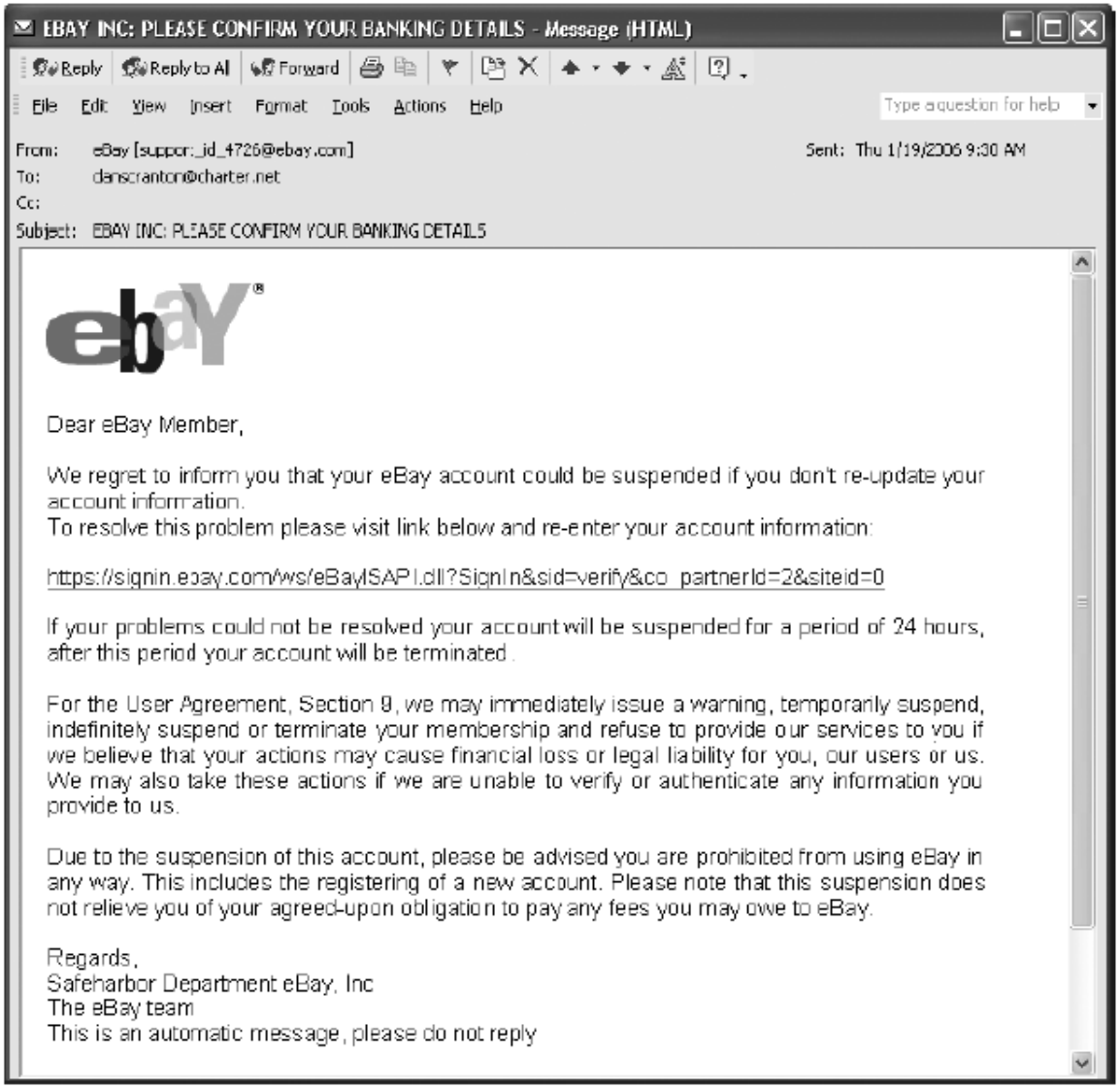

FIGURE 3-3 Example of phishing

Source Line: Course Technology/Cengage Learning.

Types of Perpetrators

- Perpetrators include:
  - Thrill seekers wanting a challenge
  - Common criminals looking for financial gain
  - Industrial spies trying to gain an advantage
  - Terrorists seeking to cause destruction
- Different objectives and access to varying resources
- Willing to take different levels of risk to accomplish an objective

Types of Perpetrators (cont'd.)

TABLE 3-4 Classifying perpetrators of computer crime

Type of perpetrator	Typical motives
Hacker	Test limits of system and/or gain publicity
Cracker	Cause problems, steal data, and corrupt systems
Malicious insider	Gain financially and/or disrupt company's information systems and business operations
Industrial spy	Capture trade secrets and gain competitive advantage
Cybercriminal	Gain financially
Hacktivist	Promote political ideology
Cyberterrorist	Destroy infrastructure components of financial institutions, utilities, and emergency response units

Source Line: Course Technology/Cengage Learning.

Hackers and Crackers

- Hackers
  - Test limitations of systems out of intellectual curiosity
    - Some smart and talented
    - Others inept; termed “lamers” or “script kiddies”
- Crackers
  - Cracking is a form of hacking
  - Clearly criminal activity

Malicious Insiders

- Major security concern for companies
- Fraud within an organization is usually due to weaknesses in internal control procedures
- Collusion
  - Cooperation between an employee and an outsider
- Insiders are not necessarily employees
  - Can also be consultants and contractors
- Extremely difficult to detect or stop
  - Authorized to access the very systems they abuse
- Negligent insiders have potential to cause damage

Industrial Spies

- Use illegal means to obtain trade secrets from competitors
- Trade secrets are protected by the Economic Espionage Act of 1996
- Competitive intelligence
  - Uses legal techniques
  - Gathers information available to the public
- Industrial espionage
  - Uses illegal means
  - Obtains information not available to the public

Cybercriminals

- Hack into corporate computers to steal
- Engage in all forms of computer fraud
- Chargebacks are disputed transactions
- Loss of customer trust has more impact than fraud
- To reduce potential for online credit card fraud:
  - Use encryption technology
  - Verify the address submitted online against the issuing bank
  - Request a card verification value (CVV)
  - Use transaction-risk scoring software

Cybercriminals (cont'd.)

- Smart cards
  - Contain a memory chip
  - Updated with encrypted data each time card is used
  - Used widely in Europe
  - Not widely used in the U.S.

Hacktivists and Cyberterrorists

- Hacktivism
  - Hacking to achieve a political or social goal
- Cyberterrorist
  - Attacks computers or networks in an attempt to intimidate or coerce a government in order to advance certain political or social objectives
  - Seeks to cause harm rather than gather information
  - Uses techniques that destroy or disrupt services

Federal Laws for Prosecuting Computer Attacks

TABLE 3-5 Federal laws that address computer crime

Federal law	Subject area
USA Patriot Act	Defines cyberterrorism and penalties
Identity Theft and Assumption Deterrence Act (U.S. Code Title 18, Section 1028)	Makes identity theft a Federal crime with penalties up to 15 years imprisonment and a maximum fine of $250,000
Fraud and Related Activity in Connection with Access Devices Statute (U.S. Code Title 18, Section 1029)	False claims regarding unauthorized use of credit cards
Computer Fraud and Abuse Act (U.S. Code Title 18, Section 1030)	Fraud and related activities in association with computers: • Accessing a computer without authorization or exceeding authorized access • Transmitting a program, code, or command that causes harm to a computer • Trafficking of computer passwords • Threatening to cause damage to a protected computer
Stored Wire and Electronic Communications and Transactional Records Access Statutes (U.S. Code Title 18, Chapter 121)	Unlawful access to stored communications to obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage

Source Line: Course Technology/Cengage Learning.

Implementing Trustworthy Computing

- Trustworthy computing
  - Delivers secure, private, and reliable computing
  - Based on sound business practices

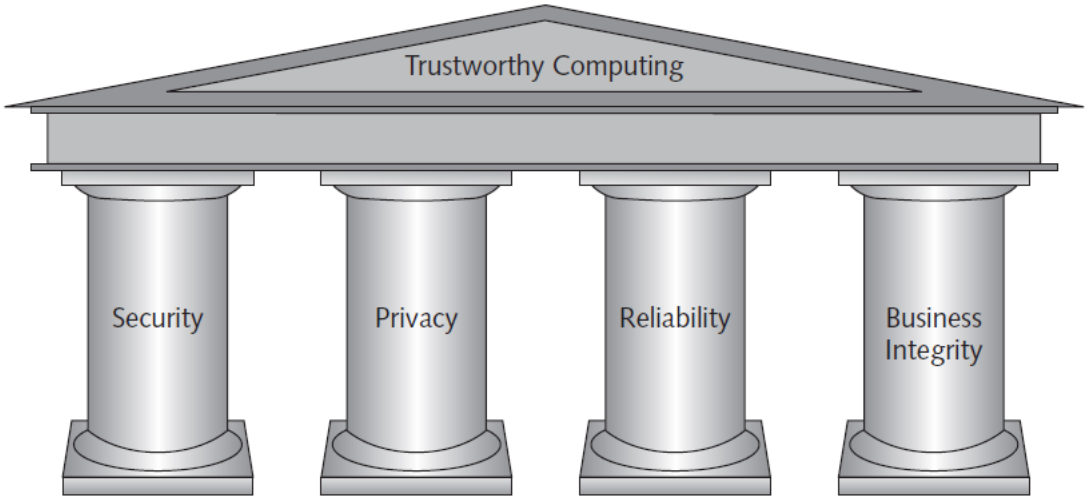

FIGURE 3-4 Microsoft's four pillars of trustworthy computing
Source Line: Course Technology/Cengage Learning.

Implementing Trustworthy Computing (cont'd.)

- Security of any system or network
  - Combination of technology, policy, and people
  - Requires a wide range of activities to be effective
- Systems must be monitored to detect possible intrusion
- Clear reaction plan addresses:
  - Notification, evidence protection, activity log maintenance, containment, eradication, and recovery

Summary

- Ethical decisions in determining which information systems and data most need protection
- Most common computer exploits
  - Viruses
  - Worms
  - Trojan horses
  - Distributed denial-of-service attacks
  - Rootkits
  - Spam
  - Phishing, spear-fishing, smishing, vishing

Summary (cont'd.)

- Perpetrators include:
  - Hackers
  - Crackers
  - Malicious insider
  - Industrial spies
  - Cybercriminals
  - Hacktivist
  - Cyberterrorists

Summary (cont'd.)

- Must implement multilayer process for managing security vulnerabilities, including:
  - Assessment of threats
  - Identifying actions to address vulnerabilities
  - User education
- IT must lead the effort to implement:
  - Security policies and procedures
  - Hardware and software to prevent security breaches
- Computer forensics is key to fighting computer crime in a court of law