

*Introduction to Computer and  
Internet Crime*

# 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?

# 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
- 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
    - Ubiquitous
    - 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 Exploits

- Most frequent attack is on a networked computer from an outside source
  - Can also attack smartphones
- Types of attacks
  - Virus
  - Worm
  - Trojan horse
  - Botnet
  - Distributed denial of service

# Types of Exploits (cont'd.)

- Types of attacks (cont'd.)
  - Rootkit
  - Spam
  - Phishing

# Viruses

- Pieces of programming code
- Usually disguised as something else
- Cause unexpected and undesirable behavior
- Often attached to files
- Deliver a “payload”

# Viruses (cont'd.)

- Do not spread from computer to computer
  - Must be passed on to other users through:
    - Infected e-mail document attachments
    - Downloads of infected programs
    - Visits to infected Web sites
- Macro viruses
  - Most common and easily created viruses
  - Created in an application macro language
  - Infect documents and templates

# 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
  - Effort for IT workers

# Trojan Horses

- Malicious code hidden inside seemingly harmless programs
- Users are tricked into installing them
- Logic bomb
  - Executes when triggered by certain event

# Botnets

- Large group of computers
  - Controlled from remote locations by hackers
  - Without the knowledge or consent of their owners
- Collective processing capacity exceeds that of the world's most powerful supercomputers
- Estimated that about one in four personal computers in the United States is part of a botnet
- Dealing with “bot” computers within an organization's network can be expensive

# 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
- Does not involve a break-in at the target computer
  - Target machine is busy responding to a stream of automated requests
  - Legitimate users cannot get in



# 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

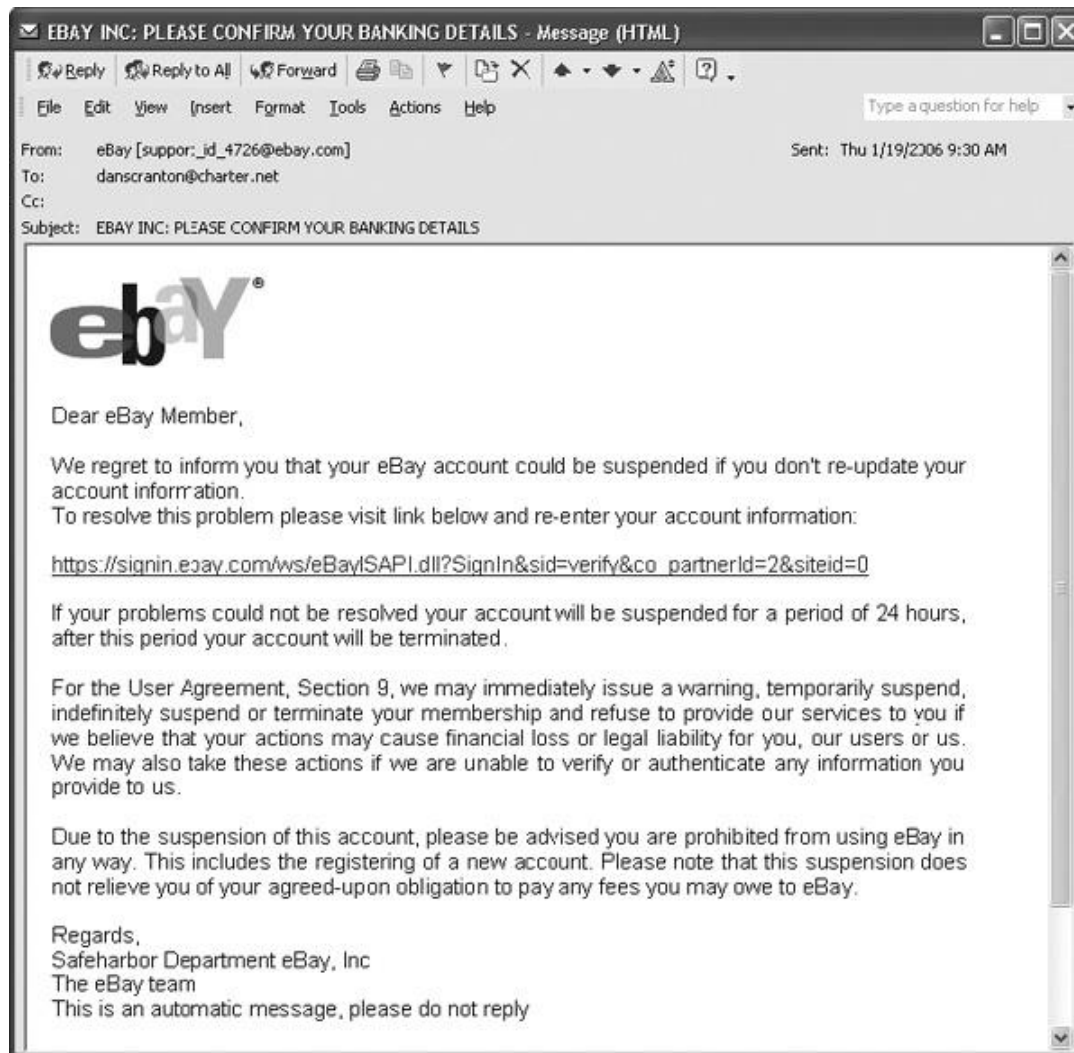
- Abuse of e-mail systems to send unsolicited e-mail to large numbers of people
  - Low-cost commercial advertising for questionable products
  - Method of marketing also used by many legitimate organizations
- Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act
  - Legal 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 e-mail fraudulently to try to get the recipient to reveal personal data
- Legitimate-looking e-mails lead users to counterfeit Web sites
- Spear-phishing
  - Fraudulent e-mails to an organization's employees



**FIGURE 3-2** Example of phishing

# 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
- Different levels of risk to accomplish an objective

# Types of Perpetrators (cont'd.)

**TABLE 3-3** 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

# 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 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

# 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 and 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.

# Hacktivism 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

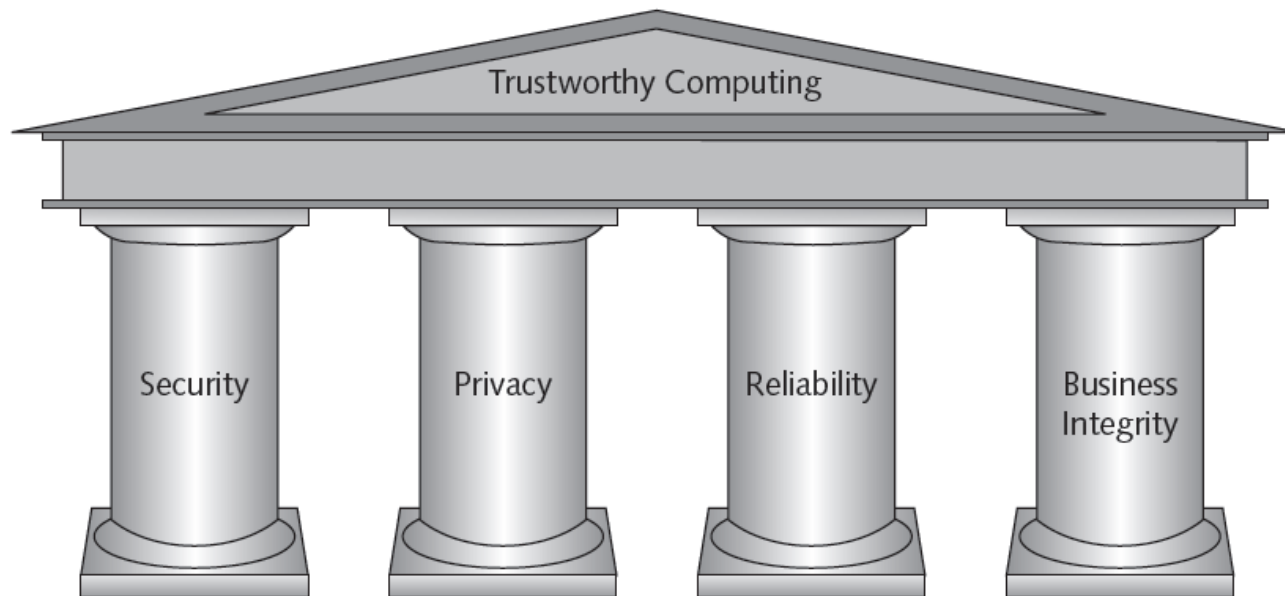
# Federal Laws for Prosecuting Computer Attacks

**TABLE 3-4** Federal laws that apply to computer attacks

Federal law	Subject area
USA Patriot Act	Defines cyberterrorism and penalties
Computer Fraud and Abuse Act	Malicious code and unauthorized access to computers
Identity Theft and Assumption Deterrence Act	Identity theft
U.S. Code Title 18, Part I, Chapter 47, Section 1030	Fraud and related activities in association with computers: <ul style="list-style-type: none"> <li>• Accessing a computer without authorization or exceeding authorized access</li> <li>• Transmission of a program, code, or command that causes harm to a computer</li> <li>• Trafficking of computer passwords</li> <li>• Threats to cause damage to a protected computer</li> </ul>
U.S. Code Title 18, Part I, Chapter 121, Section 2701	Unlawful access to stored communications to obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage

# Implementing Trustworthy Computing

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



**FIGURE 3-3** Microsoft's Four Pillars of Trustworthy Computing

# 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



# Risk Assessment

- Process of assessing security-related risks:
  - To an organization's computers and networks
  - From both internal and external threats
- Identifies investments that best protect from most likely and serious threats
- Identifies most dangerous threats
- Focuses security efforts on areas of highest payoff

# Risk Assessment (cont'd.)

**TABLE 3-6** Risk assessment for hypothetical company

Risk	Business objective threatened	Estimated probability of such an event occurring	Estimated cost of a successful attack	Probability × cost = expected cost	Assessment of current level of protection	Relative priority to be fixed
Distributed denial-of-service attack	24/7 operation of B2C Web site	40%	\$500,000	\$200,000	Poor	1
E-mail attachment with harmful worm	Rapid and reliable communications among employees and suppliers	70%	\$200,000	\$140,000	Poor	2
Harmful virus	Employees' use of personal productivity software	90%	\$50,000	\$45,000	Good	3
Invoice and payment fraud	Reliable cash flow	10%	\$200,000	\$20,000	Excellent	4

# Establishing a Security Policy

- A security policy defines:
  - Organization's security requirements
  - Controls and sanctions needed to meet the requirements
- Delineates responsibilities and expected behavior
- Outlines what needs to be done
  - Not how to do it
- Automated system policies should mirror written policies

# Establishing a Security Policy (cont'd.)

- Trade-off between:
  - Ease of use
  - Increased security
- Areas of concern
  - E-mail attachments
  - Wireless devices
- VPN uses the Internet to relay communications but maintains privacy through security features
- Additional security includes encrypting originating and receiving network addresses

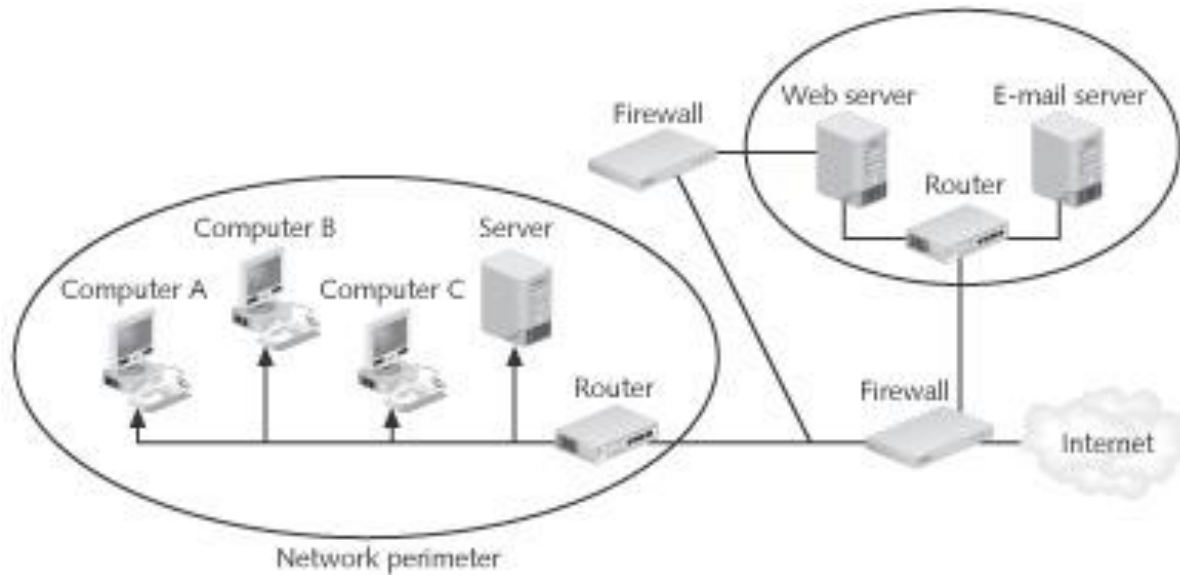
# Educating Employees, Contractors, and Part-Time Workers

- Educate users about the importance of security
  - Motivate them to understand and follow policy
- Discuss recent security incidents that affect the organization
- Help protect information systems by:
  - Guarding passwords
  - Not allowing others to use passwords
  - Applying strict access controls to protect data
  - Reporting all unusual activity

# Prevention

- Implement a layered security solution
  - Make computer break-ins harder
- Installing a corporate firewall
  - Limits network access
- Intrusion prevention systems
  - Block viruses, malformed packets, and other threats
- Antivirus software
  - Scans for sequence of bytes or virus signature
- United States Computer Emergency Readiness Team (US-CERT) serves as clearinghouse

# Prevention (cont'd.)



**FIGURE 3-5** Firewall

# Prevention (cont'd.)

**TABLE 3-7** Popular firewall software for personal computers

Software	Vendor
Norton Personal Firewall	Symantec
Comodo	Comodo Security Solutions, Inc.
Online Armor	Tall Emu Pty Ltd
ZoneAlarm Pro	Check Point Software Technologies
Personal Firewall	McAfee



# Prevention (cont'd.)

- Safeguards against attacks by malicious insiders
- Departing employees and contractors
  - Promptly delete computer accounts, login IDs, and passwords
- Carefully define employee roles and separate key responsibilities
- Create roles and user accounts to limit authority

# Prevention (cont'd.)

- Address most critical Internet security threats
  - Keep track of well-known vulnerabilities
    - SANS (System Administration, Networking, and Security) Institute
    - US-CERT
- Conduct periodic IT security audits
  - Evaluate policies and whether they are followed
  - Review access and levels of authority
  - Test system safeguards

# Detection

- Detection systems
  - Catch intruders in the act
- Intrusion detection system
  - Monitors system/network resources and activities
  - Notifies the proper authority when it identifies:
    - Possible intrusions from outside the organization
    - Misuse from within the organization
  - Knowledge-based approach
  - Behavior-based approach

# Response

- Response plan
  - Develop well in advance of any incident
  - Approved by:
    - Legal department
    - Senior management
- Primary goals
  - Regain control and limit damage
  - Not to monitor or catch an intruder

# Response (cont'd.)

- Incident notification defines:
  - Who to notify
  - Who not to notify
- Security experts recommend against releasing specific information about a security compromise in public forums
- Document all details of a security incident
  - All system events
  - Specific actions taken
  - All external conversations

# Response (cont'd.)

- Act quickly to contain an attack
- Eradication effort
  - Collect and log all possible criminal evidence
  - Verify necessary backups are current and complete
  - Create new backups
- Follow-up
  - Determine how security was compromised
    - Prevent it from happening again

# Response (cont'd.)

- Review
  - Determine exactly what happened
  - Evaluate how the organization responded
- Capture the perpetrator
- Consider the potential for negative publicity
- Legal precedent
  - Hold organizations accountable for their own IT security weaknesses

# 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



# Summary (cont'd.)

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

# Summary (cont'd.)

- Key elements of a multilayer process for managing security vulnerabilities include:
  - 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