THOMSON
COURSE TECHNOLOGY

Ethics in Information Technology, Second Edition

Chapter 3
Computer and Internet Crime

Objectives

- 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 (continued)

- What are some characteristics of common computer criminals, including their objectives, available resources, willingness to accept risk, and frequency of attack?
- 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 Worsening Problem

- Security of information technology is of utmost importance
  - Protect confidential data
    - Safeguard private customer and employee data
  - Protect against malicious acts of theft or disruption
  - Must be balanced against other business needs and issues
- Number of IT-related security incidents is increasing around the world

IT Security Incidents: A Worsening Problem (continued)

- Computer Emergency Response Team Coordination Center (CERT/CC)
  - Established in 1988 at the Software Engineering Institute (SEI)
  - Charged with
    - Coordinating communication among experts during computer security emergencies
    - Helping to prevent future incidents

Increasing Complexity Increases Vulnerability

- Computing environment is enormously complex
  - Continues to increase in complexity
  - Number of possible entry points to a network expands continuously

Higher Computer User Expectations

- Computer help desks
  - Under intense pressure to provide fast responses to users' questions
  - Sometimes forget to
    - Verify users' identities
    - Check whether users are authorized to perform the requested action
- Computer users share login IDs and passwords

Expanding and Changing Systems Introduce 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 keep up with the pace of technological change

Increased Reliance on Commercial Software with Known Vulnerabilities

- Exploit
  - Attack on information system
  - Takes advantage of a particular system vulnerability
  - Due to poor system design or implementation
- Patch
  - "Fix" to eliminate the problem
  - Users are responsible for obtaining and installing patches
  - Delays in installing patches expose users to security breaches

Increased Reliance on Commercial Software with Known Vulnerabilities (continued)

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

Number of Vulnerabilities Reported to CERT/CC

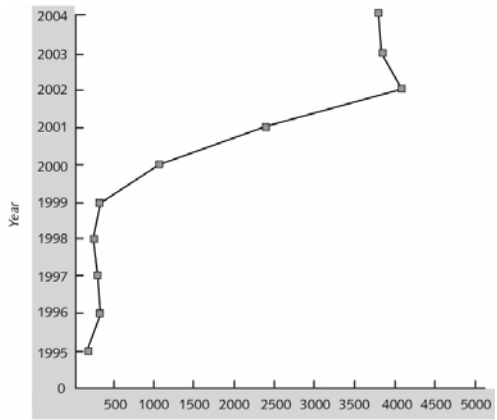

FIGURE 3-1 Number of vulnerabilities reported to CERT/CC

Types of Attacks

- Most frequent attack is on a networked computer from an outside source
- Types of attacks
  - Virus
  - Worm
  - Trojan horse
  - Denial of service

Viruses

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

Viruses (continued)

- Does not spread itself from computer to computer
  - Must be passed on to other users through
    - Infected e-mail document attachments
    - Programs on diskettes
    - Shared files
- 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 virus or worm attack
  - Lost data and programs
  - Lost productivity
  - Effort for IT workers

Cost Impact of Worms

TABLE 3-1 Cost impact of worms

Name	Year released	Worldwide economic impact
ILOVEYOU	2000	$8.75 billion
Code Red	2001	$2.62 billion
SirCam	2001	$1.15 billion
Melissa	1999	$1.10 billion

Trojan Horses

- Program that a hacker secretly installs
- Users are tricked into installing it
- Logic bomb
  - Executes under specific conditions

Denial-of-Service (DoS) 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
- Spoofing generates a false return address on packets

Denial-of-Service (DoS) Attacks (continued)

- Ingress filtering - When Internet service providers (ISPs) prevent incoming packets with false IP addresses from being passed on
- Egress filtering - Ensuring spoofed packets don't leave a network

Perpetrators

- Motives are the same as other criminals
- Different objectives and access to varying resources
- Different levels of risk to accomplish an objective

Classifying Perpetrators of Computer Crime

TABLE 3-2 Classifying perpetrators of computer crime

Type of perpetrator	Objectives	Resources available to perpetrator	Level of risk acceptable to perpetrator	Frequency of attack
Hacker	Test limits of system and gain publicity	Limited	Minimal	High
Cracker	Cause problems, steal data, and corrupt systems	Limited	Moderate	Medium
Insider	Make money and disrupt company's information systems	Knowledge of systems and passwords	Moderate	Low

TABLE 3-2 Classifying perpetrators of computer crime (continued)

Type of perpetrator	Objectives	Resources available to perpetrator	Level of risk acceptable to perpetrator	Frequency of attack
Industrial spy	Capture trade secrets and gain competitive advantage	Well funded and well trained	Minimal	Low
Cyber-criminal	Make money	Well funded and well trained	Moderate	Low
Cyber-terrorist	Destroy key infrastructure components	Not necessarily well funded or well trained	Very high	Low

Hackers and Crackers

- Hackers
  - Test limitations of systems out of intellectual curiosity
- Crackers
  - Cracking is a form of hacking
  - Clearly criminal activity

Malicious Insiders

- Top security concern for companies
- Estimated 85 percent of all fraud is committed by employees
- Usually due to weaknesses in internal control procedures
- Collusion is 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

- Illegally 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 the potential for online credit card fraud sites:
  - Use encryption technology
  - Verify the address submitted online against the issuing bank
  - Request a card verification value (CVV)
  - Use transaction-risk scoring software

Cybercriminals (continued)

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

Legal Overview: The Check Clearing for the 21st Century Act

- Requires that banks accept paper documents
  - In lieu of original paper checks
  - Speeds clearing of checks
- New opportunities for check fraud
  - Bankers don't fully realize the extent of possible increased fraud

Cyberterrorists

- Intimidate or coerce governments to advance political or social objectives
- Launch computer-based attacks
- Seek to cause harm
  - Rather than gather information
- Many experts believe terrorist groups pose only a limited threat to information systems

Reducing Vulnerabilities

- Security
  - Combination of technology, policy, and people
  - Requires a wide range of activities to be effective
- Assess threats to an organization's computers and network
- Identify actions that address the most serious vulnerabilities
- Educate users
- Monitor to detect a possible intrusion
- Create a clear reaction plan

Risk Assessment

- Organization's review of:
  - Potential threats to computers and network
  - Probability of threats occurring
- Identify investments that can best protect an organization from the most likely and serious threats
- Reasonable assurance
- Improve security in areas with:
  - Highest estimated cost
  - Poorest level of protection

Risk Assessment for a Hypothetical Company

TABLE 3-3 Risk assessment for a hypothetical company

Risk	Estimated probability of such an event occurring	Estimated cost of a successful attack	Probability × cost = expected cost impact	Assessment of current level of protection	Relative priority to be fixed
Denial-of-service attack	80%	$500,000	$400,000	Poor	1
E-mail attachment with harmful worm	70%	$200,000	$140,000	Poor	2
Harmful virus	90%	$50,000	$45,000	Good	3
Invoice and payment fraud	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 (continued)

- 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 security policy
- Discuss recent security incidents that affected 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
- Firewall
  - Limits network access
- Antivirus software
  - Scans for a specific sequence of bytes
    - Known as the virus signature
  - Norton Antivirus
  - Dr. Solomon's Antivirus from McAfee

Firewall Protection

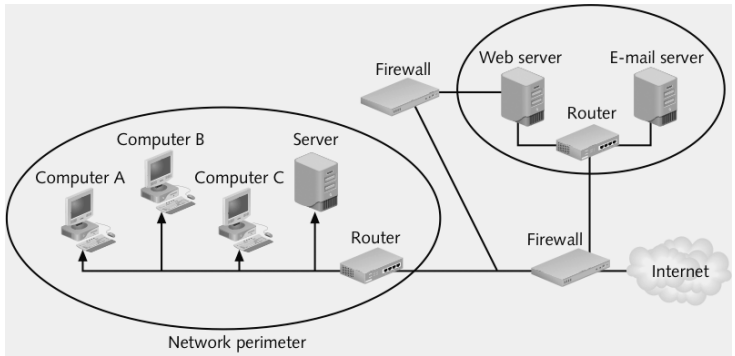

FIGURE 3-3 Firewall protection

Popular Firewall Software for Personal Computers

TABLE 3-4 Popular firewall software for personal computers

Software	Vendor
Norton Personal Firewall	Symantec
Tiny Personal Firewall	Tiny Software
BlackICE Defender	Network Ice Corporation
ZoneAlarm Pro	Zone Labs
Personal Firewall	McAfee

Prevention (continued)

- Antivirus software
  - Continually updated with the latest virus detection information
    - Called definitions
- Departing employees
  - Promptly delete computer accounts, login IDs, and passwords
- Carefully define employee roles
- Create roles and user accounts

Prevention (continued)

- Keep track of well-known vulnerabilities
  - SANS (System Administration, Networking, and Security) Institute
  - CERT/CC
- Back up critical applications and data regularly
- Perform a security audit

Detection

- Detection systems
  - Catch intruders in the act
- Intrusion detection system
  - Monitors system and 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

Detection (continued)

- Intrusion prevention systems (IPSs)
  - Prevent attacks by blocking
    - Viruses
    - Malformed packets
    - Other threats
  - Sits directly behind the firewall

Detection (continued)

- Honeypot
  - Provides would-be hackers with fake information about the network
  - Decoy server
  - Well-isolated from the rest of the network
  - Can extensively log activities of intruders

Response

- Response plan
  - Develop well in advance of any incident
  - Approved by
    - Legal department
    - Senior management
- Primary goals
  - Regain control
  - Limit damage

Response (continued)

- 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 (continued)

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

Response (continued)

- 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 regarding IT security include determining which information systems and data most need protection
- 65-fold increase in the number of reported IT security incidents from 1997 to 2003
- Most incidents involve a:
  - Virus
  - Worm
  - Trojan horse
  - Denial-of-service

Summary (continued)

- Perpetrators include:
  - Hackers
  - Crackers
  - Industrial spies
  - Cybercriminals
  - Cyberterrorists

Summary (continued)

- Key elements of a multilayer process for managing security vulnerabilities include:
  - Assessment
  - User education
  - Response plan