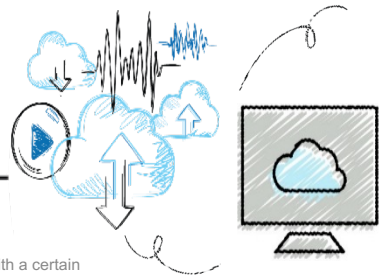
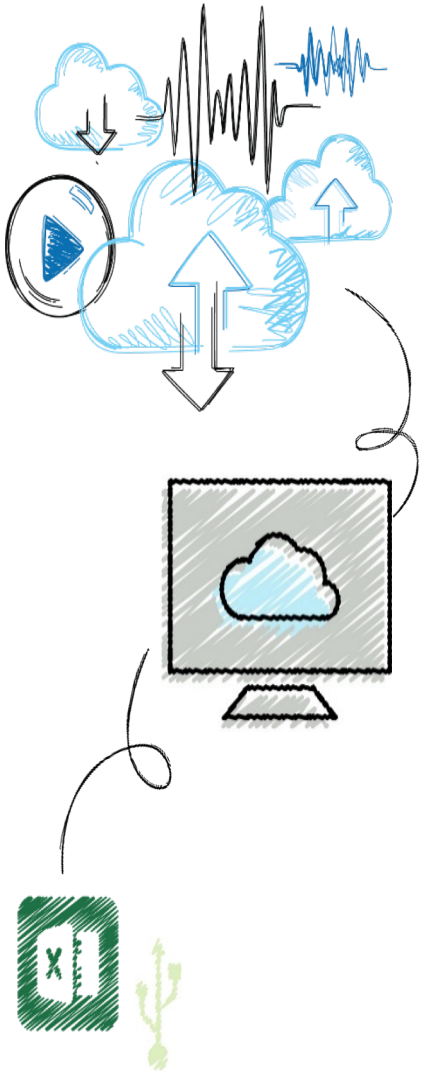
Principles of Information Systems, Thirteenth Edition

Chapter 13

Cybercrime and Information System Security





Objectives

After completing this chapter, you will be able to:

Explain why computer incidents are so prevalent

Identify and briefly describe the types of computer exploits and their impact

Identify specific measures used to prevent computer crime

Outline actions that must be taken in the event of a successful security intrusion

The Threat Landscape

- Number of cybercrimes are increasing
- Organizations are putting in place a range of countermeasures to combat cybercrime

Why Computer Incidents Are So Prevalent

- Increasing Complexity Increases Vulnerability
  - Cloud computing, networks, computers, mobile devices, virtualization, OS applications, Web sites, switches, routers, and gateways are interconnected and driven by millions of lines of code
- Expanding and Changing Systems Introduce New Risks
  - It is difficult for IT organizations to keep up with the pace of technological change, successfully perform an ongoing assessment of new security risks, and implement approaches for dealing with them
- Increased Prevalence of Bring Your Own Device Policies
  - Bring your own device (BYOD): a business policy that permits (encourages) employees to use their own mobile devices to access company computing resources and applications
  - BYOD makes it difficult for IT organizations to adequately safeguard additional portable devices with various OSs and applications

Why Computer Incidents Are So Prevalent

- Increasing Sophistication of Those Who Would Do Harm
  - Today's computer menace is organized and may be part of an organized group that has an agenda and targets specific organizations and Web sites

TABLE 13.2 Classifying perpetrators of computer crime

Type of Perpetrator	Description
Black hat hacker	Someone who violates computer or Internet security maliciously or for illegal personal gain (in contrast to a white hat hacker who is someone who has been hired by an organization to test the security of its information systems)
Cracker	An individual who causes problems, steals data, and corrupts systems
Malicious insider	An employee or contractor who attempts to gain financially and/or disrupt a company's information systems and business operations
Industrial spy	An individual who captures trade secrets and attempts to gain an unfair competitive advantage
Cybercriminal	Someone who attacks a computer system or network for financial gain
Hacktivist	An individual who hacks computers or Web sites in an attempt to promote a political ideology
Cyberterrorist	Someone who attempts to destroy the infrastructure components of governments, financial institutions, and other corporations, utilities, and emergency response units

Types of Exploits

- Common attacks include:
  - Ransomware
  - Viruses
  - Worms
  - Trojan horses
  - Spam
  - Distributed denial-of-service attacks
  - Rootkits
  - Phishing
  - Identity theft
  - Cyberespionage and cyberterrorism

Types of Exploits

- **Ransomware**
  - Malware that stops you from using your computer or accessing your data until you meet certain demands such as paying a ransom to the attacker
    - Example: NotPetya
- **Viruses**
  - A piece of programming code (usually disguised as something else) that causes a computer to behave in an unexpected and undesirable manner
  - Spread to other machines when a computer user shares an infected file (e.g., sends an email with a virus-infected MS Word file)
  - Macro viruses have become a common and easily created form of virus
- **Worms**
  - A harmful program that duplicates itself without human intervention
- Malware (malicious software) can fit into multiple categories. For example, NotPetya is a worm and a ransomware

Types of Exploits

- **Trojan Horses**
  - A seemingly harmless program in which malicious code is hidden
  - A victim on the receiving end is usually tricked into opening it because it appears to be useful software from a legitimate source
  - Might be designed to enable the attacker to destroy hard drives, corrupt files, control the computer remotely, launch attacks against other computers, steal passwords or spy on users
  - Often creates a "backdoor" on a computer that enables an attacker to gain future access
  - Logic bomb
    - A type of Trojan horse that executes when it is triggered by a specific event.
    - For example, overwriting a computer's master boot record at a predetermined time and day
  - Android Trojan Horse
    - https://www.cse.wustl.edu/~jain/cse571-11/ftp/trojan/index.html
    - Capable of SMS scanning, password theft, GPS tracking, etc

Types of Exploits

- **Spam**
  - The use of email systems to send unsolicited email to large numbers of people
  - Also an inexpensive method of marketing used by many legitimate organizations
  - CAN-SPAM Act (قانون امريكي) states that it is legal to spam, provided the messages meet a few basic requirements
    - Spammers cannot disguise their identity by using a false return address
    - The email must include a label specifying that it is an ad or a solicitation
    - The email must include a way for recipients to opt out of future mass mailings

Types of Exploits

- Spam (cont'd)
  - CAPTCHA is software generates and grades tests that humans can pass and all but the most sophisticated computer programs cannot

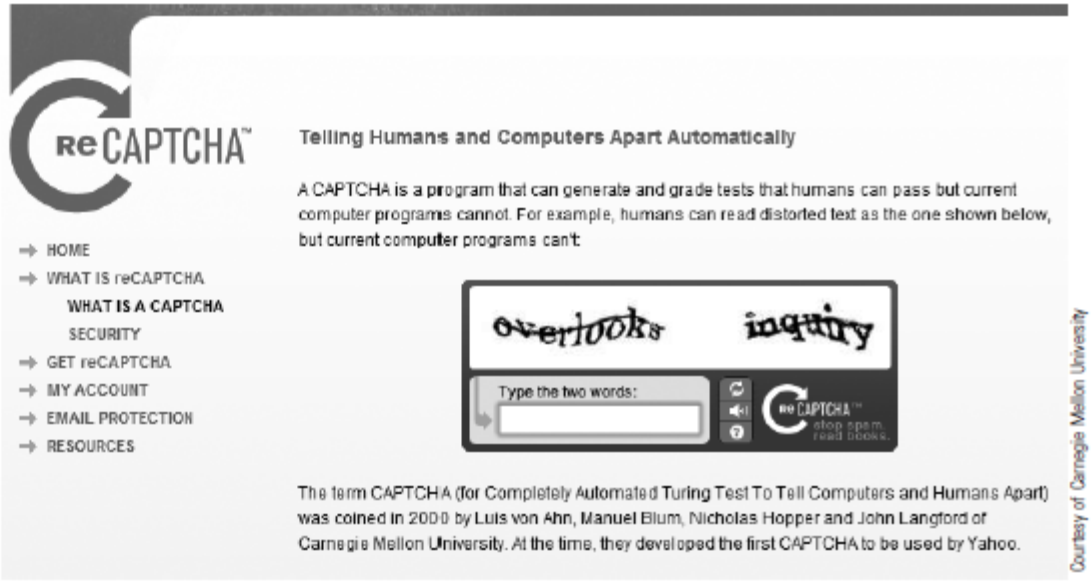
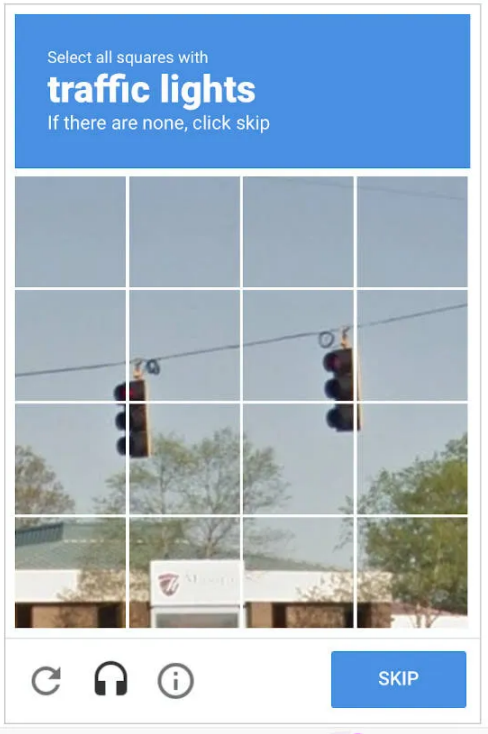
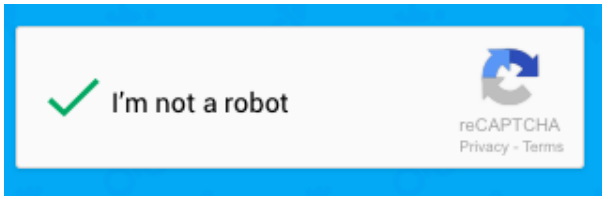


FIGURE 13.1
Example of CAPTCHA
CAPTCHA is used to distinguish humans from automated bots.

Types of Exploits

- An overview of CAPTCHAs (optional): https://www.youtube.com/watch?v=lUTvB1O8eEg&t=409s
- New types of CAPTCHAs:





Types of Exploits

- **Distributed Denial-of-Service Attacks**
  - An attack in which a malicious hacker takes over computers via the Internet and causes them to flood a target site with demands for data and other small tasks
  - Keeps target so busy responding to requests that legitimate users cannot get in
  - Botnet
    - A large group of computers, controlled from one or more remote locations by hackers, without the consent of their owners
    - Sometimes called zombies
    - Frequently used to distribute spam and malicious code

Types of Exploits

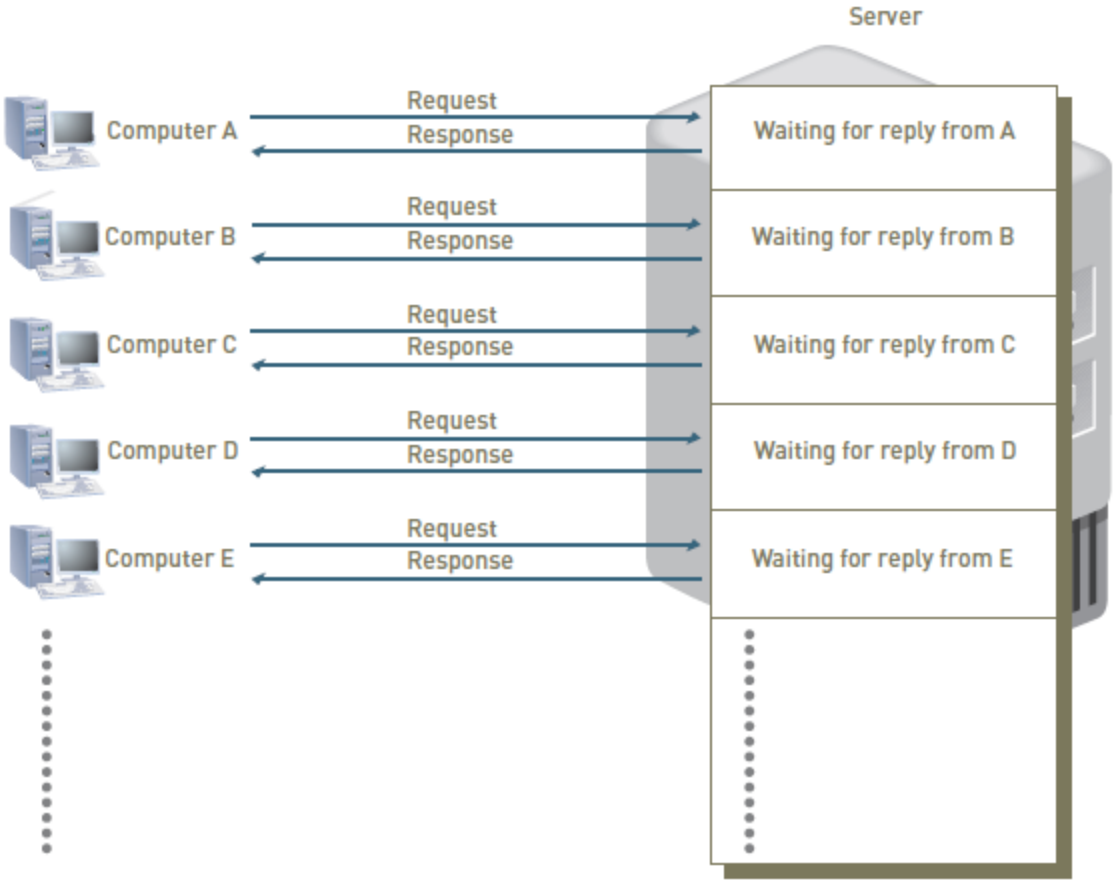


FIGURE 13.2

Distributed denial-of-service attack

A DDoS attack floods a target site with demands for data and other small tasks.

Types of Exploits

- **Rootkit**
  - A set of programs that enables its user to gain administrator-level access to a computer without the end user's consent or knowledge
  - Example: Stuxnet, which targeted the control systems of Iran's nuclear facilities in 2010

Types of Exploits

- **Phishing**
  - The act of fraudulently using email to try to get the recipient to reveal personal data
  - One form of it:
    - Sending legitimate-looking emails urging recipients to take action to avoid a negative consequence or to receive a reward
  - Spear-phishing is a variation of phishing where fraudulent emails are sent to a certain organization's employees
    - Much more precise and narrow
    - Designed to look like they came from high-level executives within organization

Types of Exploits

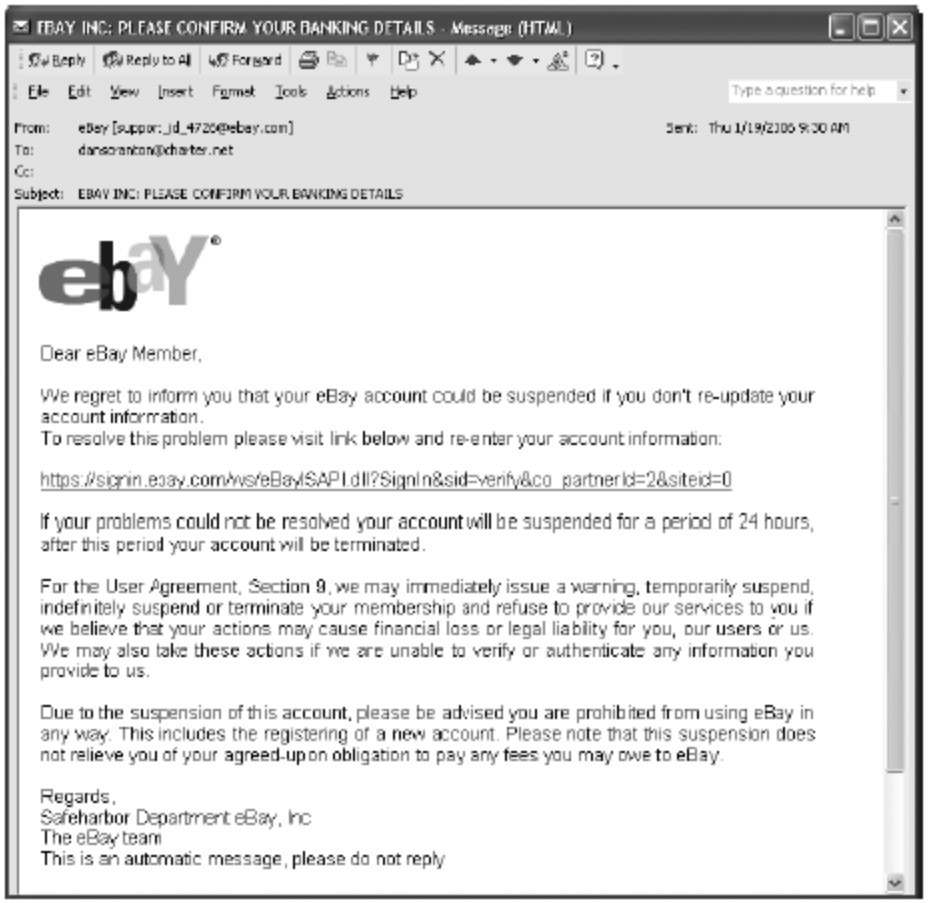


FIGURE 13.3
Example of phishing email
Phishing attacks attempt to get the recipient to reveal personal data.

Types of Exploits

- **Identity Theft**
  - The theft of personal information and then used without their permission
- **Data breach**
  - the unintended release of sensitive data or the access of sensitive data by unauthorized individuals
    - Often results in identity theft
  - Most e-commerce Web sites use some form of encryption technology to protect information as it comes from the consumer. They employ various security measures, including:
    - Secure communication protocol (HTTPS)
    - Encryption of customer data
    - etc

Types of Exploits

- **Cyberespionage**
  - Involves the development of malware that secretly steals data in the computer systems of organizations
  - Often carried out by governments or state-sponsored entities
  - Target entities: government agencies, military contractors, political organizations, and manufacturing firms
  - Mostly targeted toward high-value data such as the following:
    - Sales, marketing, and new product development plans, schedules, and budgets
    - Details about product designs and innovative processes
    - Employee personal information
    - Customer and client data
    - Sensitive information about partners and partner agreements

Types of Exploits

- **Cyberterrorism**
  - The intimidation of government or civilian population by using information technology to disable critical national infrastructure
  - Purpose: achieving political, religious, or ideological goals
  - Department of Homeland Security (DHS) provides a link that enables users to report cyber incidents
  - Cyberterrorists try daily to gain unauthorized access to a number of important and sensitive sites

Federal Laws for Prosecuting Computer Attacks

TABLE 13.4 Federal laws that address computer crime

Federal Law	Subject Area
Computer Fraud and Abuse Act (U.S. Code Title 18, Section 1030)	Addresses fraud and related activities in association with computers, including the following: • 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
Fraud and Related Activity in Connection with Access Devices Statute (U.S. Code Title 18, Section 1029)	Covers false claims regarding unauthorized use of credit cards
Identity Theft and Assumption Deterrence Act (U.S. Code Title 18, Section 1028)	Makes identity theft a federal crime, with penalties of up to 15 years' of imprisonment and a maximum fine of $250,000
Stored Wire and Electronic Communications and Transactional Records Access Statutes (U.S. Code Title 18, Chapter 121)	Focuses on unlawful access to stored communications to obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage
USA Patriot Act	Defines cyberterrorism and associated penalties

Prevention

- Organizations should implement a layered security solution to make computer break-ins so difficult that an attacker gives up
  - If an attacker breaks through one layer, another layer must then be overcome
- درهم وقاية خير من قنطار علاج
- Next slides discuss the following layers of protective measures:
  - Educating Employees and Contract Workers
  - Implementing a Corporate Firewall
  - Utilizing a Security Dashboard
  - Installing Antivirus Software on Personal Computers
  - Implementing Safeguards against Attacks by Malicious Insiders
  - Addressing the Most Critical Internet Security Threats
  - Conducting Periodic IT Security Audits

Educating Employees and Contract Workers

- Users can protect an organization's information systems by:
  - Guarding their passwords to protect against unauthorized access to their accounts
  - Prohibiting others from using their passwords
  - Applying strict access controls (file and directory permissions) to protect data from disclosure or destruction
  - Reporting all unusual activity to the organization's IT security group
  - Protecting portable computers and data storage (hundreds of thousands of laptops are lost or stolen per year)

Implementing a Corporate Firewall

- Firewall
  - A system of software, hardware, or a combination of both that stands guard between an organization's internal network and the Internet
  - Also, it can be used to limit network access based on the organization's access policy

Utilizing a Security Dashboard

- Security dashboard software provides a comprehensive display of all vital data related to an organization's security defenses

	Operation-level Scorecard: KPI				
No	Control/KPI	Target	Actual	Status	Remarks
1	Number of violations of segregation of duties	0	3		
2	Number of users who do not comply with password standards	Max. 2	7		
3	Percentage of suspected and actual violations	Max. 5	7		
4	Pecentage of critical assets covered by internal/external penetration tests	Min. 95	98		
5	Number of computers with patches behind agreed-upon SLA	Max. 2	1		
6	Number of outdated policies, procedures, standards and guidelines	Max. 4	5		
7	Number of internal audits scheduled	Min. 2	2		
8	Number of penetration tests not performed as required for the quarter	Max. 1	0		
9	Percentage of agents/employees trained on information security policies and procedures as part of induction	100	90		
10	Number of corrective/preventive actions taken based on analysis of logs	Min. 5	10		
11	Percentage of changes carried out as per change control procedure	100	90		

Note: Target and actual amounts are hypothetical figures for the purpose of this example. Categorization into green, amber and red is done on a predefined basis.

FIGURE 13.4

Security dashboard

A security dashboard provides a comprehensive display of all vital data related to an organization's security defenses.

Source: ISACA

Installing Antivirus Software on Personal Computers

- Antivirus software
  - Scans for specific sequence of bytes, known as a virus signature, that indicates the presence of a specific virus
- If virus is found
  - Antivirus software informs the user and may clean, delete, or quarantine any files, directories, or disks affected by the malicious code
- It is crucial that antivirus software be continually updated with the latest virus signatures

Implementing Safeguards against Attacks by Malicious Insiders

- User accounts that remain active after employees leave a company are a potential security risk
  - IS staff must promptly delete (or inactivate) computer accounts of departing employees
- Another safeguard
  - Create roles and user accounts so that users have the authority to perform their responsibilities and nothing more

Addressing the Most Critical Internet Security Threats

- Computer attackers
  - Know that many organizations are slow to fix problems
  - Scan the Internet for vulnerable systems
- US-CERT regularly updates a summary of the most frequent, high-impact vulnerabilities being reported
  - Find it at https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Actions required to address these issues include installing a known patch to the software
  - And keeping applications and OSs up-to-date

Conducting Periodic IT Security Audits

- Security audit
  - Evaluates whether an organization has well-considered security policy in place and if it is being followed
- Some organizations also perform a penetration test
  - Individuals try to break through the measures and identify vulnerabilities

Detection

- Intrusion detection system (IDS)
  - Software and/or hardware that monitors a network for suspicious activity or policy violations
  - Notifies network security personnel when it detects network traffic that attempts to circumvent the security measures of a networked computer environment

Detection

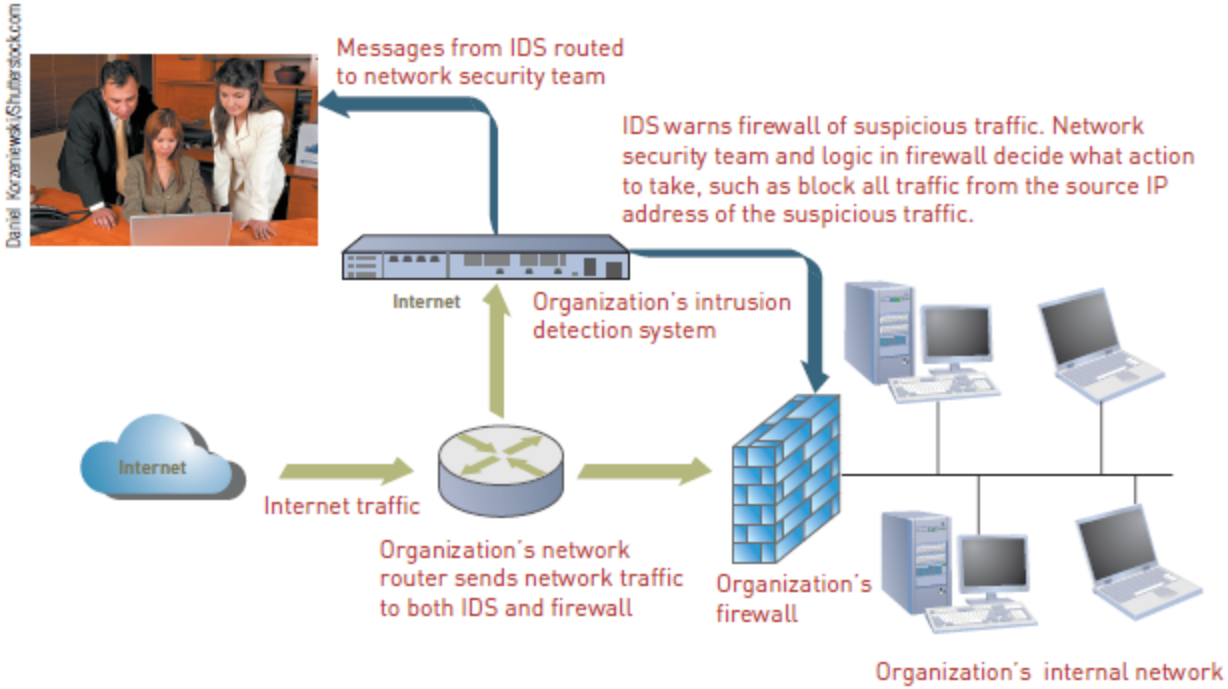


FIGURE 13.5

Intrusion detection system

An IDS notifies network security personnel when it detects network traffic that attempts to circumvent the security measures of a networked computer environment.

Response

- A response plan should be developed well in advance of any incident
  - Should be approved by the organization's legal department and senior management
- A well-developed response plan helps keep an incident under technical and emotional control
- In a security incident, the primary goal must be to:
  - Regain control and limit damage, not to attempt to monitor or catch an intruder
- The plan addresses the following if intrusion occurs:
  - Notification
  - Evidence protection and Activity log maintenance
  - Containment
  - Eradication
  - Recovery

Incident Notification

- Key element of a response plan is to
  - Define who to notify and who not to notify in the event of a security incident
- Questions to cover:
  - Within the company, who needs to be notified, and what information does each person need to have?
  - Under what conditions should the company contact major customers and suppliers?
  - How does the company inform them of a disruption in business without unnecessarily alarming them?
  - When should local authorities or the FBI be contacted?
- A critical ethical question:
  - What to tell customers and others whose personal data may have been compromised?

Protection of Evidence and Activity Logs

- Organizations should document all details of a security incident as it works to resolve the incident
- Documentation captures valuable evidence for a future prosecution

Incident Containment

- The incident response plan should clearly define the process for deciding if an attack is dangerous enough to warrant shutting down or disconnecting critical systems from the network

Eradication

- Eradication is the process of eliminating the root cause of the security incident with a high degree of confidence
- Before eradication, the IT security group must:
  - Verify that all necessary backups are current, complete, and free of any malware
  - Create a forensic disk image of each compromised system
  - After eradication, a new backup must be created

Incident Follow-Up

- Follow-up should include:
  - Determining how the organization's security was compromised
  - A review to determine exactly what happened and to evaluate how the organization responded
  - An estimate of the monetary damage
  - A decision on how much effort should be put into capturing the perpetrator
  - A decision on whether it has an ethical or a legal duty to inform customers or clients of a cyber attack

Using a Managed Security Service Provider (MSSP)

- Managed Security Service Provider (MSSP)
  - A company that monitors, manages, and maintains computer and network security for other organizations
  - Includes companies such as AT&T, Computer Sciences Corporation, Dell SecureWorks, IBM, Symantec, and Verizon

Computer Forensics

- Computer Forensics
  - A discipline that combines elements of law and computer science to identify, collect, examine, and preserve data from computer systems, networks, and storage devices in a manner that preserves the integrity of the data gathered
- Computer forensics investigators work as a team to investigate an incident and conduct the forensic analysis
- Proper handling of computer forensics investigation is the key to fighting computer crime successfully in a court of law
- Numerous certifications exist:
  - CCE (Certified Computer Examiner), CISSP (Certified Information Systems Security Professional), CSFA (CyberSecurity Forensic Analyst), and GCFA (Global Information Assurance Certification Certified Forensic Analyst)

Summary

- Computer crime is a serious and rapidly growing area of concern requiring management attention
- Organizations must take strong measures to ensure secure, private, and reliable computing experiences for their employees, customers, and business partners