5e

Ethics in Information Technology

Chapter 3
Computer and Internet Crime

George W. Reynolds

Learning 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?
- Who are the primary perpetrators of computer crime, and what are their objectives?

Learning 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?

Motivating information

- Qatar experienced a combined 4,268,553 e-mail, URL, and malware cyber-threats detected during the first half of 2020.
- In total, Trend Micro blocked 27.8bn cyber threats in the first half of 2020, 93% of which were e-mail-borne.
- Business Email Compromise (BEC) detections increased by 18% from the second half of 2019
- There is a 36% increase in new ransomware families.

Source: Gulf-times.com, Trend Micro Wednesday ‹23 September 2020 07:45 PM

Ethical Decisions Regarding IT Security

- To deal with computer crime, the firm should:
  - Pursue prosecution of the criminals at all costs
  - Maintain a low profile to avoid the negative publicity
  - Inform affected customers or take some other action
- Following decisions should be taken by the firm
  - How much resources should be spent to safeguard against computer crime
  - What actions should be taken when a software is found susceptible to hacking
  - What should be done if recommended computer security safeguards increase operating costs

9 key cybersecurity statistics at-a-glance

(reference www.csoonline.com)

- 94% of malware is delivered via email
- Phishing attacks account for more than 80% of reported security incidents
- $17,700 is lost every minute due to phishing attacks
- 60% of breaches involved vulnerabilities for which a patch was available but not applied
- 63% of companies said their data was potentially compromised within the last twelve months due to a hardware- or silicon-level security breach
- Attacks on IoT devices tripled in the first half of 2019.
- fileless attacks grew by 256 percent over the first half of 2019
- Data breaches cost enterprises an average of $3.92 million
- 40% of IT leaders say cybersecurity jobs are the most difficult to fill

Why Computer Incidents are So Prevalent

Top Countries

1	Islamic Republic of Afghanistan	33.77%
2	Republic of Tajikistan	28.07%
3	Burkina Faso	27.89%
4	Republic of Benin	27.64%
5	Republic of Chad	27.14%
6	Republic of Guinea-Bissau	26.78%
7	South Sudan	26.51%
8	Republic of the Union of Myanmar	26.46%
9	Republic of Guinea	26.31%
10	Republic of Uzbekistan	26.22%

Top Infections

1	DangerousObject.Multi.Generic	12,36%
2	HackTool.Win32.KMSAuto.gen	7,94%
3	HackTool.MSIL.HackKMS.a	4,04%
4	HackTool.Win32.KMSAuto.ew	3,17%
5	HackTool.MSIL.KMSAuto.dh	3,08%
6	HackTool.MSIL.KMSAuto.di	2,44%
7	Trojan.WinLNK.Agent.gen	2,20%
8	HackTool.Win64.HackKMS.b	2,15%
9	HackTool.Win32.KMSAuto.om	1,81%
10	HackTool.MSIL.HackKMS.d	1,77%

Source: https://statistics.securelist.com/en/on-access-scan/month

Why Computer Incidents are So Prevalent

- Increasing complexity increases vulnerability
  - Number of entry points to a network expands continually, increasing the possibility of security breaches
  - **Cloud computing**: Environment where software and data storage are provided via the Internet
  - **Virtualization software**: Operates in a software layer that runs on top of the operating system
    - Enables multiple **virtual machines** to run on a single computer

Why Computer Incidents are So Prevalent

- Higher computer user expectations
  - Not verifying users'
  - Sharing of login IDs and passwords by users
- Expanding and changing systems require one to:
  - Keep up with the pace of technological change
  - Perform an ongoing assessment of new security risks
  - Implementing approaches for dealing with them

Why Computer Incidents are So Prevalent

- **Bring your own device (BYOD)**: Business policy that permits employees to use their own mobile devices to access company computing resources and applications
- Increased reliance on commercial software with known vulnerabilities
  - **Exploit**: Attack on an information system that takes advantage of a particular system vulnerability
  - **Zero-day attack**: Takes place before the security community or software developer knows about the vulnerability or has been able to repair it

Types of Exploits

Virus

- Piece of programming code, disguised as something else, that causes a computer to behave in an unexpected and undesirable manner

Worm

- Harmful program that resides in the active memory of the computer and duplicates itself

Trojan Horse

- Program in which malicious code is hidden inside a seemingly harmless program
- **Logic bomb**: Executes when it is triggered by a specific event

Types of Exploits

Spam

- Abuse of email systems to send unsolicited email to large numbers of people
- **CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Humans Apart)**
  - Generates and grades tests that humans can pass but computer programs cannot

Distributed Denial-of-Service (DDoS) Attack

- Causes computers to flood a target site with demands for data and other small tasks

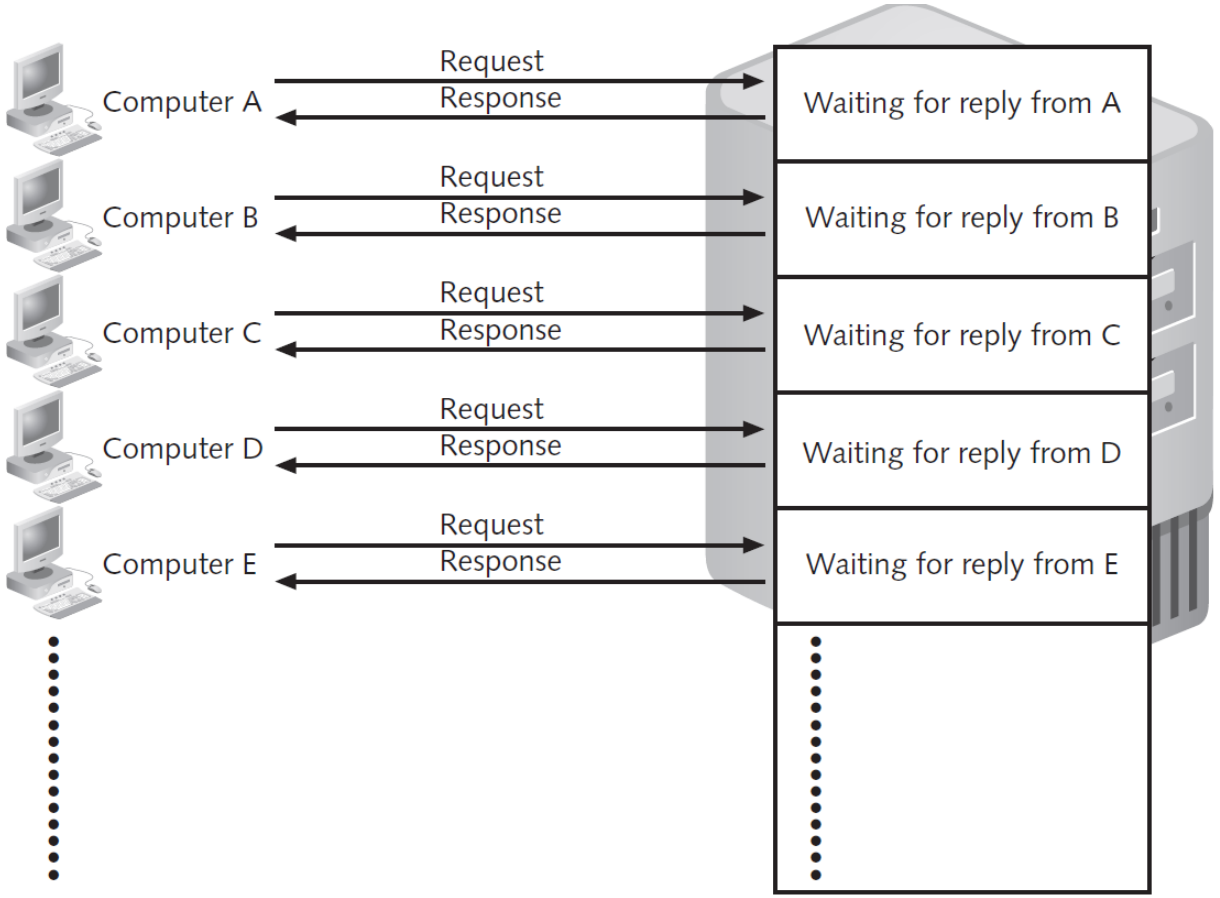
Rootkit

- Enables user to gain administrator-level access to a computer without the end user's consent

Phishing

- Fraudulently using email to try to get the recipient to reveal personal data

Figure 3.2 - Distributed Denial-of-Service Attack



Source Line: Course Technology/Cengage Learning.

Botnet

- Group of computers which are controlled from one or more remote locations by hackers, without the knowledge or consent of their owners
- **Zombies**: Computers that are taken over
- used to distribute spam and malicious code

Rootkits

- **Rootkit:** malicious software that allows an unauthorized user to have privileged access to a computer and to restricted areas of its software.
- **Tools**
  - Keyloggers
  - Banking credentials stealers
  - Password stealers
  - Antivirus disablers

Types of Phishing

- **Spear-phishing**: Phisher sends fraudulent emails to a certain organization's employees
  - Emails are designed to look like they came from high-level executives within the organization
- **Smishing**: Legitimate-looking text message sent to people, telling them to call a specific phone number or to log on to a Web site
- **Vishing**: Victims receive a voice mail telling them to call a phone number or access a Web site

Types of Perpetrators

- Thrill seekers wanting a challenge
- Common criminals looking for financial gain
- Industrial spies trying to gain a competitive advantage
- Terrorists seeking to cause destruction to further their cause

Table 3.5 - Classifying Perpetrators of Computer Crime

Type of perpetrator	Typical motives
Hackers	Test limits of system and/or gain publicity
Crackers	Cause problems, steal data, and corrupt systems
Malicious insiders	Gain financially and/or disrupt company's information systems and business operations
Industrial spies	Capture trade secrets and gain competitive advantage
Cybercriminals	Gain financially
Hacktivists	Promote political ideology
Cyberterrorists	Destroy infrastructure components of financial institutions, utilities, and emergency response units

Source Line: Course Technology/Cengage Learning.

Types of Perpetrators

- **Hackers**: Test the limitations of information systems out of intellectual curiosity
  - **Lamers** or **script kiddies**: Terms used to refer to technically inept hackers
- **Malicious insiders**
  - Employees, consultants, or contractors
  - Have some form of collusion
    - **Collusion**: Cooperation between an employee and an outsider
  - **Negligent insiders**: Poorly trained and inadequately managed employees who cause damage accidently

Types of Perpetrators

- **Industrial spies**
  - **Competitive intelligence**: Legally obtained data gathered using sources available to the public
  - **Industrial espionage**: Using illegal means to obtain information that is not available to the public
- **Cybercriminals**
  - Hack into computers to steal and engage in computer fraud
  - **Data breach**: Unintended release of sensitive data or the access of sensitive data by unauthorized individuals

Strategies to Reduce 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
- Use smart cards
  - **Smart cards**: Memory chips are updated with encrypted data every time the card is used

Types of Perpetrators

- **Hacktivists**: Hack to achieve a political or social goal
- **Cyberterrorists**: Launch computer-based attacks to intimidate or coerce an organization in order to advance certain political or social objectives
  - Use techniques that destroy or disrupt services
  - Consider themselves to be at war
  - Have a very high acceptance of risk
  - Seek maximum impact

Table 3.6 - Federal Laws that Address Computer Crime

Federal law	Subject area
USA Patriot Act	Defines cyberterrorism and associated 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.

Trustworthy Computing

Delivers secure, private, and reliable computing experiences based on sound business practices

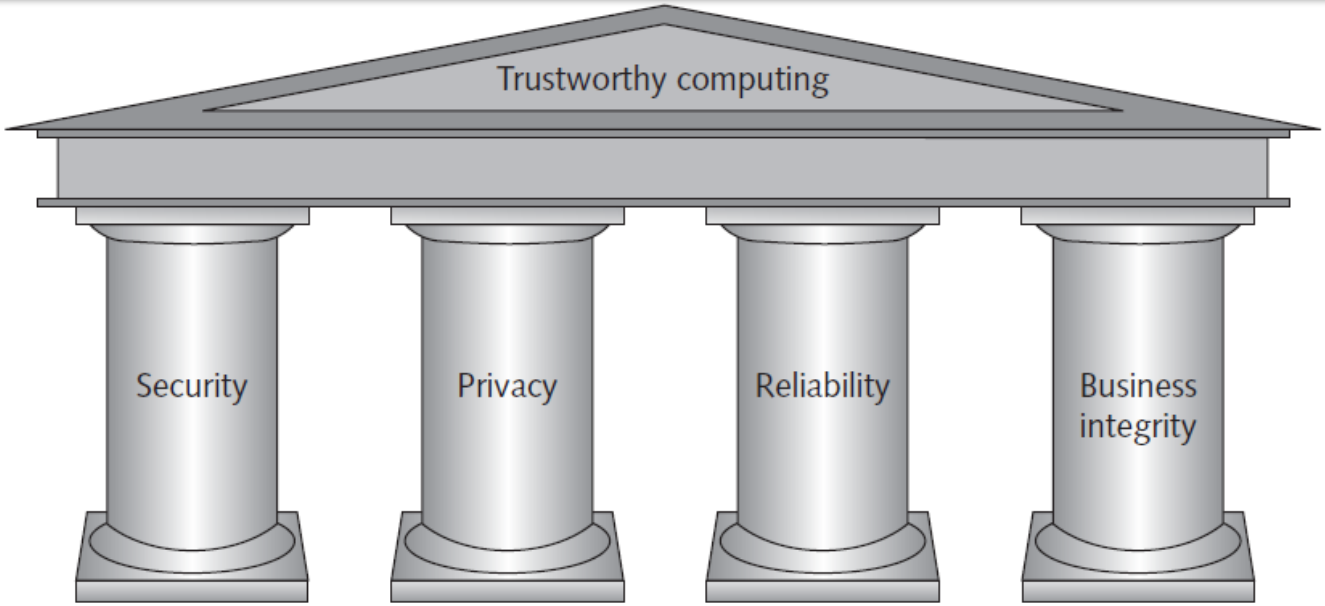


FIGURE 3-4 Microsoft's four pillars of trustworthy computing
Source Line: Course Technology/Cengage Learning.

Trustworthy Computing

TABLE 3-7 Actions taken by Microsoft to support trustworthy computing

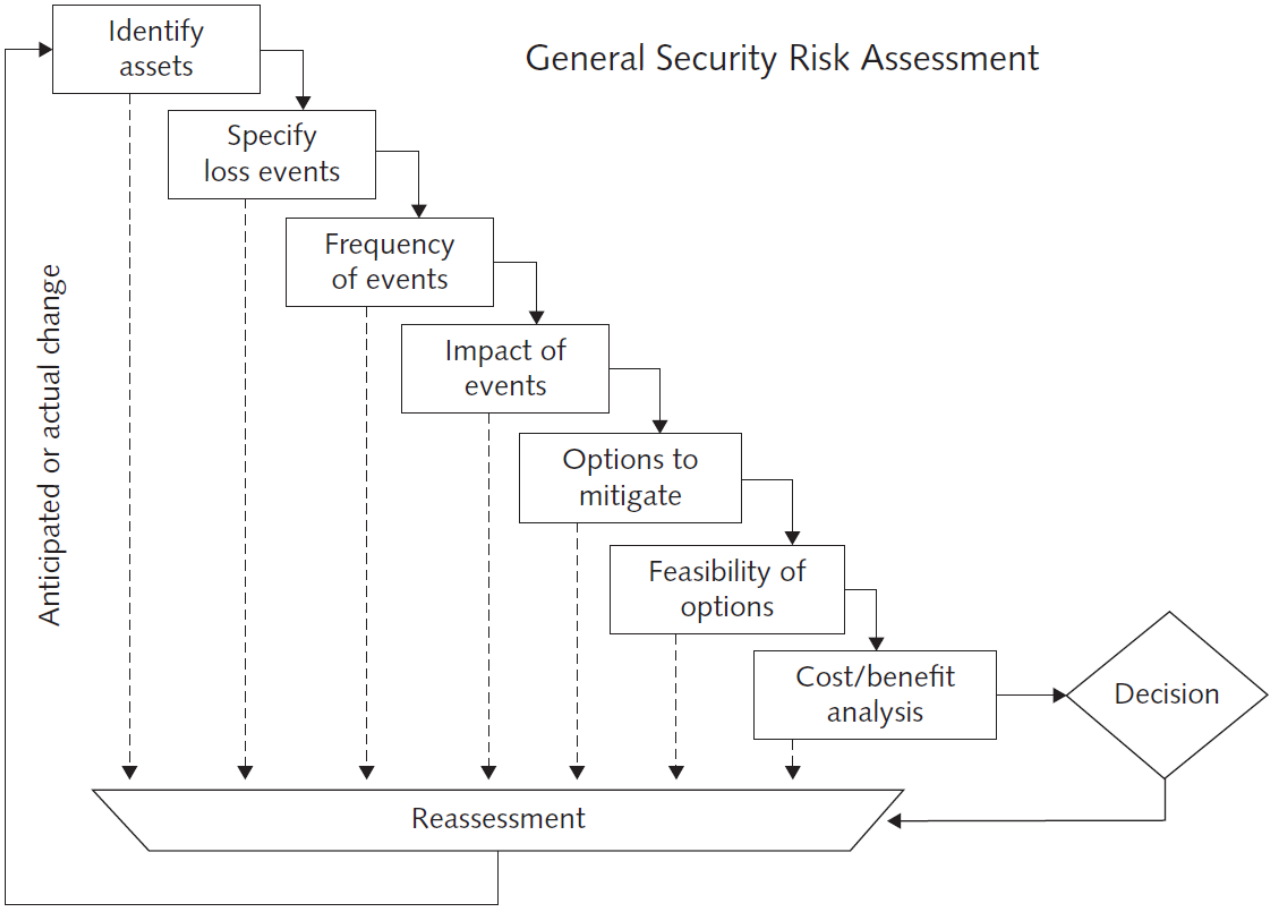
Pillar	Actions taken by Microsoft
Security	Invest in the expertise and technology required to create a trustworthy environment.
	Work with law enforcement agencies, industry experts, academia, and private sectors to create and enforce secure computing.
	Develop trust by educating consumers on secure computing.
Privacy	Make privacy a priority in the design, development, and testing of products.
	Contribute to standards and policies created by industry organizations and government.
	Provide users with a sense of control over their personal information.
Reliability	Build systems so that (1) they continue to provide service in the face of internal or external disruptions; (2) they can be easily restored to a previously known state with no data loss in the event of a disruption; (3) they provide accurate and timely service whenever needed; (4) required changes and upgrades do not disrupt them; (5) they contain minimal software bugs on release; and (6) they work as expected or promised.
Business integrity	Be responsive—take responsibility for problems and take action to correct them. Be transparent—be open in dealings with customers, keep motives clear, keep promises, and make sure customers know where they stand in dealing with the company.

Source Line: Course Technology/Cengage Learning.

Risk Assessment

- Assessing security-related risks to an organization's computers and networks from internal and external threats
- Identify investments that will protect the organization from most likely and serious threats
- Asset - Hardware, software, information system, network, or database used by an organization to achieve its business objectives
- Loss event - Any occurrence that has a negative impact on an asset

Figure 3.5 - General Security Risk Assessment



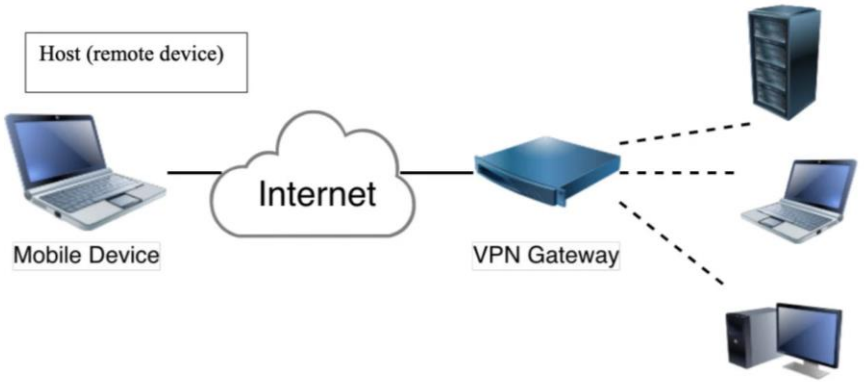
Source Line: General Security Risk Assessment Guidelines, ASIS International (2003). See the Standards and Guidelines page of the ASIS International website (www.asisonline.org) for revisions and/or updates. Reprinted by permission.

Security Policy

- Defines an organization's security requirements and the controls and sanctions needed to meet those requirements
- Delineates responsibilities and expected behavior of members of the organization.
- Outlines what needs to be done and not how it should be done

Establishing a Security Policy

- Areas of concern
  - Use of email attachments
  - Use of wireless devices
- **Virtual private network (VPN)**: Works by using the Internet to relay communications
  - Encrypts data at the sending end and decrypts it at the receiving end



Educating Employees and Contract Workers

- Motivates them to understand and follow the security policies
- Users must help protect an organization's information systems and data by:
  - Guarding their passwords
  - Prohibiting others from using their passwords
  - Applying strict access controls
  - Reporting all unusual activity to the organization's IT security group
  - Ensuring that portable computing and data storage devices are protected

Prevention

Install a corporate firewall (slide 32)

- Limits network access based on the organization's access policy

Intrusion detection system (IDS) (slide 33)

- Monitors system and network resources and activities
- Notifies network security personnel when network traffic attempts to circumvent the security measures

Antivirus software

- Scans for a specific sequence of bytes, known as a virus signature
  - **Virus signature**: Indicates the presence of a specific virus

The Best Free Firewalls of 2020

- Sophos XG Firewall Home Edition
- ZoneAlarm Free Firewall
- AVS Firewall
- Comodo Free Firewall
- TinyWall
- Outpost Firewall
- GlassWire
- Privatefirewall
- OpenDNS Home

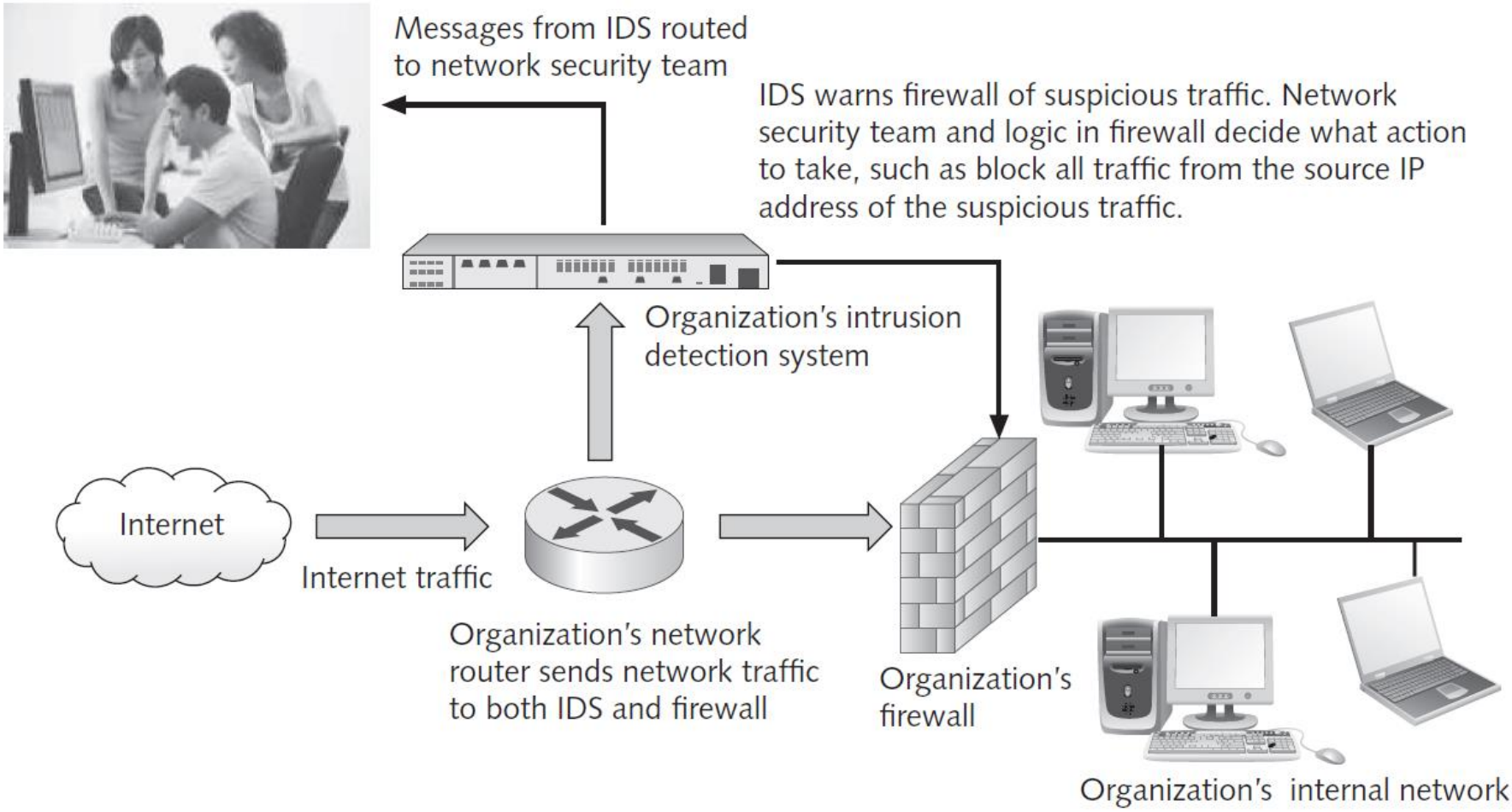


FIGURE 3-6 Intrusion detection system

Credit: © Monkey Business Images/Shutterstock.com.

Prevention

Implement safeguards against attacks by malicious insiders

- Promptly delete the computer accounts, login IDs, and passwords of departing employees and contractors

Defend against cyberterrorism

- **Department of Homeland Security (DHS)**:Aims to secure critical infrastructure and information systems

Address critical internet security threats

- High-impact vulnerabilities should be fixed on priority basis

Conducting periodic it security audits

- **Security audit**: Evaluates whether an organization has a well-considered security policy in place and if it is being followed

Detection Systems

Catch Intruders in the Act

Minimize the Impact of Intruders

Response Plan

- Incident notification
  - Define who to notify and who not to notify
  - Refrain from giving out specific information about a compromise in public forums
- Protection of evidence and activity logs
  - Document all details of a security incident to help with future prosecution and incident eradication
- Incident containment
  - Determine if an attack is dangerous enough to warrant shutting down the systems

Response

- Eradication
  - Collect and log all criminal evidence from the system
  - Verify that all backups are current, complete, and free of any virus
- Incident follow-up
  - Determine how the security was compromised
  - Conduct a review to evaluate how the organization responded
  - Create a detailed chronology of all events
  - Estimate the monetary damage

Computer Forensics

- Combines elements of law and computer science to:
  - Identify, collect, examine, and preserve data from computer systems
  - Collect data in a manner that preserves the integrity of the data gathered so that it is admissible as evidence in a court of law

Summary

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

Summary

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

Summary

- 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