COURSE TECHNOLOGY
CENGAGE Learning™

Security Awareness
Fourth Edition

Chapter 1
Introduction to Security

Objectives

After completing this chapter, you should be able to do the following:

- Describe the challenges of securing information
- Define information security and explain why it is important
- Identify the types of attackers that are common today
- Describe how to build a security strategy

Challenges of Securing Information

- No single simple solution exists for protecting computers and securing information
- Different types of attacks
- Difficulties in defending against these attacks

Today's Attacks

- Business experiencing data breach
  - Significant financial loss
    - Average cost $7.2 million
  - Potential for customer loss
- Cybercrime has affected over 400 million adults in one year
  - Estimated cost: $388 billion in time and money losses
- Apple Macs have been infected with malicious software called Flashback

Today's Attacks (cont'd.)

- Personal medical devices could be next target for attackers
- Belgium credit provider had customer information stolen
  - Attackers threatened to publish information if company did not pay
- E-mail account compromised
  - Attacker sent bogus emails to account owner's contacts asking them to wire money

Today's Attacks (cont'd.)

- Threat of preexistent malware on devices imported and sold in the US
- Car hacking
  - Breaking into car's electronic systems
- Nigerian 419 Advance Fee Fraud
  - Top Internet scam
  - Cost victims $41 billion to date

Organization	Description of Security Breach	Number of Identities Exposed
Safe Ride Services, Phoenix	Employee personal information as well as patient demographic and insurance information was exposed.	42,000
American Express Travel	Credit and debit card numbers from American Express, Visa, MasterCard, and Discover were in a man's possession and came from breaking into the computer systems of a restaurant and a restaurant supply business in the Seattle area.	27,257
Yahoo! Voices	Attackers accessed passwords of over 450,000 Yahoo! Voices users and the information was posted online.	453,492
Formspring, San Francisco	Attackers accessed Formspring's development server and posted the passwords of its users online.	28,000,000
University of Texas M.D. Anderson Cancer Center, Houston	A laptop with sensitive patient information was stolen from the home of a faculty member. It contained unencrypted patient names, medical record numbers, treatment and/or research information, and in some instances Social Security numbers.	30,000
The Public Employees Retirement Association (PERA) of New Mexico Albuquerque	A computer containing PERA information was stolen from a consulting agency.	100,000
Bethpage Federal Credit Union, Bethpage, NY	An employee accidentally posted data onto a file transfer protocol site that was not secure. The data contained customer Visa debit card names, addresses, dates of birth, card expiration dates, and checking and savings account numbers.	86,000
University of North Florida (UNF), Jacksonville	Multiple servers exposed Social Security numbers and other sensitive information. Students who submitted housing contracts since 1997 were affected.	23,246

Table 1-1 Selected security breaches involving personal information in a three-month period

Difficulties in Defending Against Attacks

- Universally connected devices
- Increased speed of attacks
- Greater sophistication of attacks
- Availability and simplicity of attack tools
- Faster detection of vulnerabilities
- Delays in security updating
- Weak security update distribution
- Distributed attacks
- User confusion

Reason	Description
Universally connected devices	Attackers from anywhere in the world can send attacks.
Increased speed of attacks	Attackers can launch attacks against millions of computers within minutes.
Greater sophistication of attacks	Attack tools vary their behavior so the same attack appears differently each time.
Availability and simplicity of attack tools	Attacks no longer limited to highly skilled attackers.
Faster detection of vulnerabilities	Attackers can discover security holes and hardware or software more quickly.
Delays in security updating	Vendors are overwhelmed trying to keep pace by updating their products against attacks.
Weak security update distribution	Many software products lack a means to distribute security patches in a timely fashion.
Distributed attacks	Attackers use thousands of computers in an attack against a single computer or network.
User confusion	Users are required to make difficult security decisions with little or no instruction.

Table 1-2 Difficulties in defending against attacks

What Is Information Security?

- What do we need to know?
  - Common information security terminology
    - Helpful when creating defenses for computers
  - The importance of information security

Understanding Security

- Security
  - Necessary steps to protect a person or property from harm
- Example: security for a home
  - Protection from burglary
  - Protection from natural forces (storms, etc.)
- Security is inversely proportional to convenience
  - As security increases, convenience decreases

Understanding Security (cont'd.)

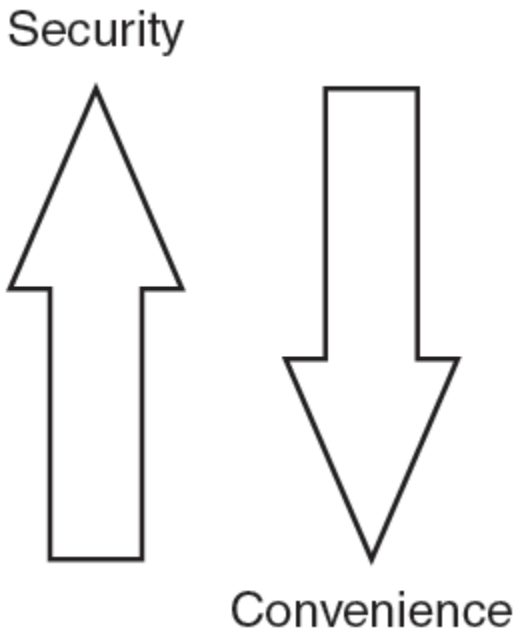

Figure 1-2 Security vs. convenience

Defining Information Security

- Information security
  - Task of securing information in a digital format
  - Ensures protective measures are properly implemented
  - Protects information with value to people and organizations
- Three protections that must be extended
  - Confidentiality
  - Integrity
  - Availability

Defining Information Security (cont'd.)

- Information security must protect devices that store, process, and transmit information
- Information protected by three layers
  - Products
  - People
  - Policies and procedures

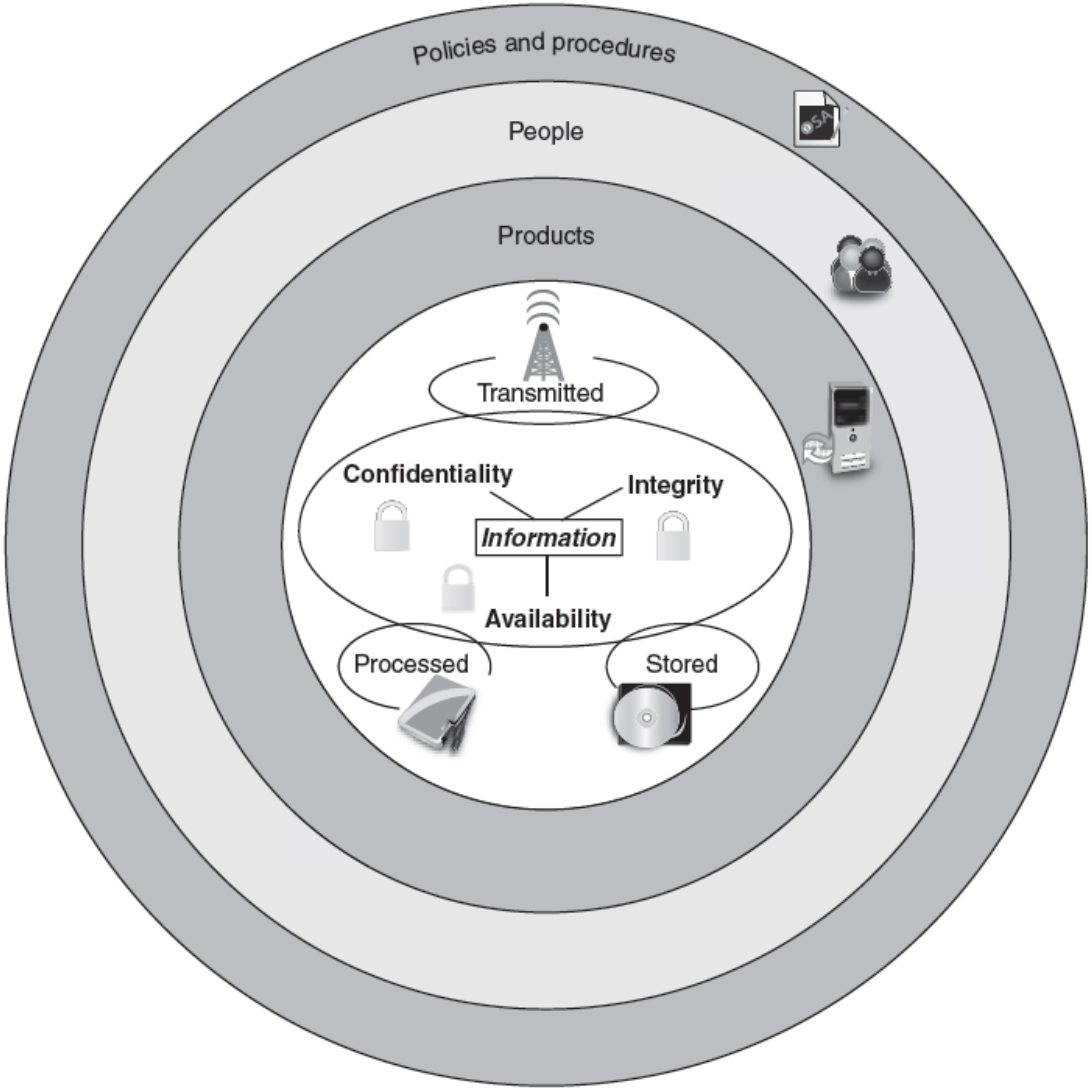

Figure1-3 Information security components

Layer	Description
Products	Form the physical security around the data; may be as basic as door locks or as complicated as network security equipment
People	Those who implement and properly use security products to protect data
Policies and procedures	Plans and policies established by an organization to ensure that people correctly use the products

Table 1-3 Information security layers

Information Security Terminology

- Asset
  - Something of value
- Threat
  - Type of action with potential to cause harm
- Threat agent
  - Person or element with power to carry out a threat
- Vulnerability
  - Flaw or weakness that allows a threat agent to bypass security

Information Security Terminology (cont'd.)

- Exploit the security weakness
  - Taking advantage of the vulnerability
- Risk
  - Likelihood that a threat agent will exploit a vulnerability
  - Some degree of risk must always be assumed
- Three options for dealing with risk
  - Accept
  - Diminish
  - Transfer

Term	Example in Scenario	Example in Information Security
Asset	Rims	Employee database
Threat	Steal rims from car	Steal data
Threat agent	Thief	Attacker, virus, flood
Vulnerability	Hole in fence	Software defect
Exploit	Climb through hole in fence	Send virus to unprotected e-mail server
Risk	Rims will be stolen	Information will be stolen

Table 1-4 Security information terminology

Understanding the Importance of Information Security

- Goals of information security
  - Preventing data theft
  - Thwarting identity theft
  - Avoiding legal consequences
  - Maintaining productivity
  - Foiling cyberterrorism
- Data theft examples
  - Stealing business information
  - Stealing personal credit card number

Understanding the Importance of Information Security (cont'd.)

- Identity theft
  - Stealing a person's information
  - Using information to impersonate the victim
  - Usually motivated by financial gain

Understanding the Importance of Information Security (cont'd.)

- Avoiding legal consequences
  - Laws protecting electronic data privacy
    - The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
    - The Sarbanes-Oxley Act of 2002 (Sarbox)
    - The Gramm-Leach-Bliley Act (GLBA)
    - The California Database Security Breach Act (2003)
- Maintaining productivity
  - Cleaning up after an attack diverts resources

Number Total Employees	Average Hourly Salary	Number of Employees to Combat Attack	Hours Required to Stop Attack and Clean Up	Total Lost Salaries	Total Lost Hours of Productivity
100	$25	1	48	$4,066	81
250	$25	3	72	$17,050	300
500	$30	5	80	$28,333	483
1000	$30	10	96	$220,000	1,293

Table 1-5 Cost of attacks

Understanding the Importance of Information Security (cont'd.)

- Cyberterrorism
  - Premeditated, politically-motivated attacks against computer systems
  - Intended to cause panic, provoke violence, or cause financial catastrophe
- Possible cyberterrorist targets
  - Banking industry
  - Air traffic control centers
  - Water systems

Who Are the Attackers?

- Divided into several categories
  - Cybercriminals
  - Script kiddies
  - Spies
  - Insiders
  - Cyberterrorists
  - Hacktivists
  - Government agencies

Cybercriminals

- Generic definition
  - People who launch attacks against other users and their computers
- Specific definition
  - Loose network of highly motivated attackers
  - Many belong to organized gangs of attackers
- Targets
  - Individuals and businesses
  - Businesses and governments

Characteristic	Explanation
Strong technical universities	Since the demise of the Soviet Union in the early 1990s a number of large universities have left teaching communist ideology and turned to teaching technology.
Low incomes	With the transition from communism to a free market system, individuals in several nations have suffered from the loss of an economy supported by the state, and incomes remain relatively low.
Unstable legal system	Many nations continue to struggle with making and enforcing new laws that combat computer crime.
Tense political relations	Some new nations do not yet have strong ties to other foreign countries, and this sometimes complicates efforts to obtain cooperation with local law enforcement.

Table 1-6 Characteristics of cybercriminals

Script Kiddies

- Attackers who lack knowledge necessary to perform attack on their own
- Use automated attack software
- Can purchase “exploit kit” for a fee from other attackers
- Over 40 percent of attacks require low or no skills

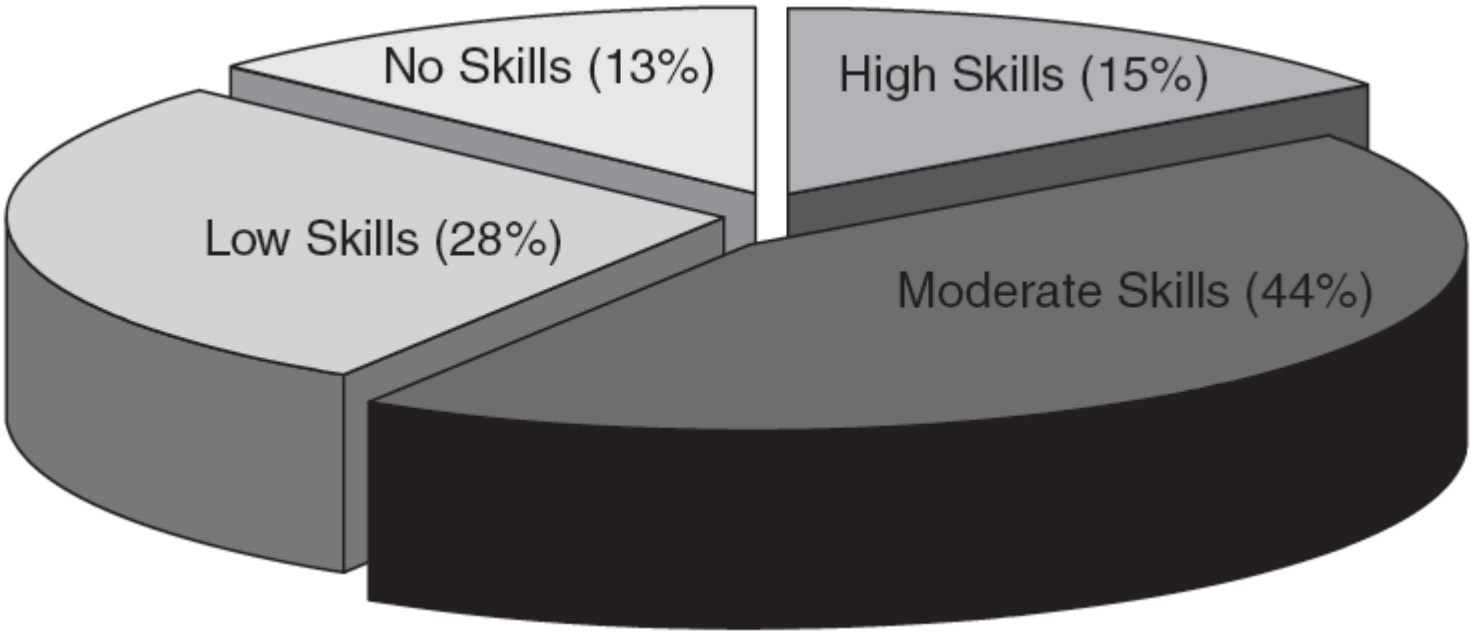

Figure 1-5 Skills needed for creating attacks

Spies

- People hired to break into a computer and steal information
- Do not randomly search for unsecured computers
  - Hired to attack a specific computer or system
- Goal
  - Break into computer or system
  - Take information without drawing attention to their actions
- Generally possess excellent computer skills

Insiders

- An organization's own employees, contractors, and business partners
- One study showed 48 percent of data breaches are caused by insiders accessing information
- Most insider attacks: sabotage or theft of intellectual property
- Most sabotage comes from employees who have recently been demoted, reprimanded, or left the company

Cyberterrorists

- Goals of a cyberattack
  - Deface electronic information
    - Spread misinformation and propaganda
  - Deny service to legitimate computer users
  - Cause critical infrastructure outages and corrupt vital data
- Attacks may be ideologically motivated

Hacktivists

- Motivated by ideology
- Direct attacks at specific Web sites
- May promote a political agenda
  - Or retaliate for a specific prior event

Government Agencies

- May instigate attacks against own citizens or foreign governments
- Examples of attacks by government agencies
  - Malware Flame targeted at computers in Eastern Europe
  - Malware Stuxnet targeted a nuclear power plant near Persian Gulf
  - Iranian government reads e-mail messages of 30,000 citizens
    - Attempt to track down dissidents

Building a Comprehensive Security Strategy

- Four key elements
  - Block attacks
  - Update defenses
  - Minimize losses
  - Send secure information
- Tactics used since Middle Ages

Block Attacks

- Medieval castle designed to block attacks
  - High, protective stone wall
  - Moat filled with water
  - Objective: create a security perimeter
- Strong security perimeter
  - Part of the computer network
  - Data to be secured resides on personal computers attached to the network
  - Local security on computers important
    - Foil attacks that breach perimeter

Update Defenses

- Medieval example: leather shields adequate until flaming arrows invented
- Continually update defenses to protect information against new types of attacks
  - Update defensive hardware and software
  - Apply operating system security updates regularly

Minimize Losses

- Medieval example: bucket of water available to put out fire started by flaming arrow
- Some attacks will get through security perimeters and local defenses
- Actions must be taken in advance
  - Make backup copies of important data
  - Institute business recovery policy

Send Secure Information

- Medieval example: ask for outside help from an ally
  - Send messenger on horseback
- Methods of keeping data secure
  - ‘‘Scramble’’ data so that unauthorized eyes cannot read it
  - Establish a secure electronic link between sender and receiver

Summary

- Attacks against information security have grown exponentially in recent years
- Difficult to defend against today's attacks
- Information security definition
  - Protecting the integrity, confidentiality, and availability of information on devices that store, transmit, and process information
- Information security goals
  - Protect against data theft, identity theft, and cyberterrorism
  - Avoid legal consequences and maintain productivity

Summary (cont'd.)

- Attackers fall into several categories
  - Different motivations, targets, and skill levels
- Elements of a comprehensive security strategy
  - Block attacks
  - Update defenses
  - Minimize losses
  - Send secure information