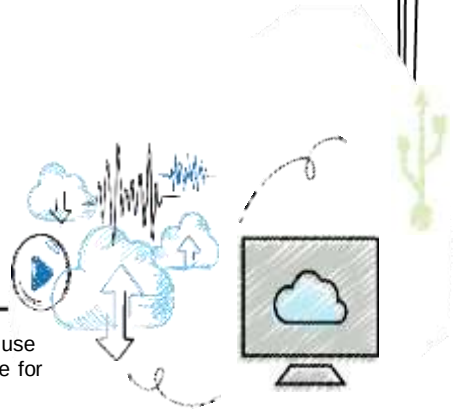
CompTIA Security+ Guide to Network Security Fundamentals, Sixth Edition

Chapter 1

Introduction to Security



Objectives

1.1 Describe the challenges of securing information

1.2 Define information security and explain why it is important

1.2 Identify the types of attackers that are common today

1.3 Describe the five basic principles of defense

Challenges of Securing Information

- Securing information
  - No simple solution
  - Many different types of attacks
  - Defending against attacks is often difficult

Today's Security Attacks

- Examples of recent attacks
  - Remotely controlling a car
  - Tampering with aircraft systems
  - Yahoo accounts compromised by attackers
  - USB flash drive malware/USB Killer
  - WINVote voting machine tampering
  - Vtech security breach
  - Stolen data from the European Space Agency
  - IRS fraud
  - Hyatt Hotels Corporation hacked

Reasons for Successful Attacks

- Widespread vulnerabilities
- Configuration issues
- Poorly designed software
- Hardware limitations
- Enterprise-based issues

Difficulties in Defending Against Attacks

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 computer 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 are no longer limited to highly skilled attackers
Faster detection of vulnerabilities	Attackers can discover security holes in hardware or software more quickly
Delays in security updating	Vendors are overwhelmed trying to keep pace updating their products against the latest attacks
Weak security update distribution	Many software products lack a means to distribute security updates in a timely fashion
Distributed attacks	Attackers use thousands of computers in an attack against a single computer or network
Use of personal devices	Enterprises are having difficulty providing security for a wide array of personal devices
User confusion	Users are required to make difficult security decisions with little or no instruction

What is Information Security?

- Before defense is possible, one must understand:
  - Exactly what security is
  - How security relates to information security
  - The terminology that relates to information security

Understanding Security

- Security is:
  - To be free from danger is the goal
  - The process that achieves that freedom
- As security is increased, convenience is often decreased
  - The more secure something is, the less convenient it may become to use

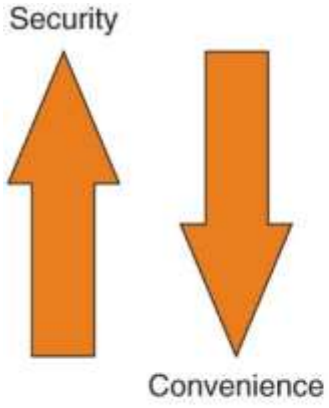


Figure 1-2 Relationship of security to convenience

Defining Information Security (1 of 4)

- **Information security** - the tasks of securing information that is in a digital format:
  - Manipulated by a microprocessor
  - Preserved on a storage device
  - Transmitted over a network
- Information security goal - to ensure that protective measures are properly implemented to ward off attacks and prevent the total collapse of the system when a successful attack occurs

Defining Information Security (2 of 4)

- Three types of information protection (often called CIA) :
  - Confidentiality
    - Only approved individuals may access information
  - Integrity
    - Information is correct and unaltered
  - Availability
    - Information is accessible to authorized users

Defining Information Security (3 of 4)

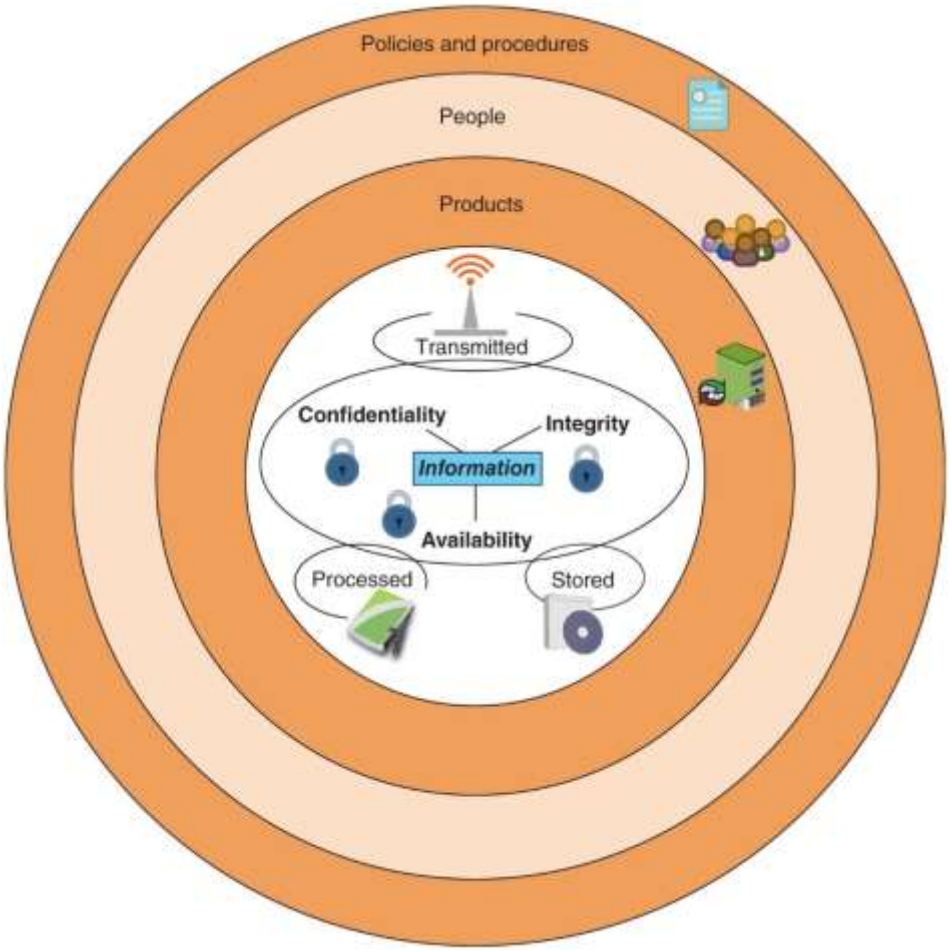


Figure 1-3 Information security layers

Defining Information Security (4 of 4)

Layer	Description
Products	Form the 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 enterprise to ensure that people correctly use the products.

Information Security Terminology (1 of 4)

- **Asset**
  - Item that has value
- **Threat**
  - Type of action that has the potential to cause harm
- **Threat actor**
  - A person or element with power to carry out a threat

Information Security Terminology (2 of 4)

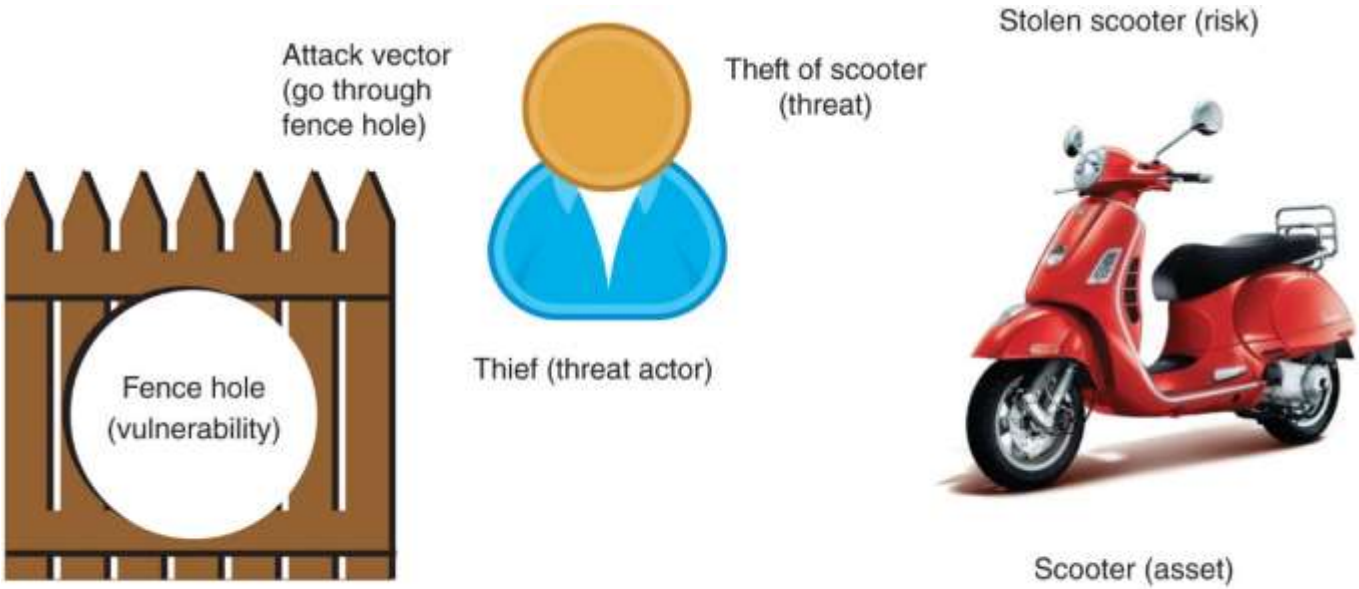


Figure 1-4 Information security components analogy

Information Security Terminology (3 of 4)

- **Vulnerability**
  - Flaw or weakness that allows a threat agent to bypass security
- **Threat vector**
  - The means by which an attack can occur
- **Risk**
  - A situation that involves exposure to some type of danger
- Risk response techniques:
  - **Accept** – risk is acknowledged but no steps are taken to address it
  - **Transfer** – transfer risk to a third party
  - **Avoid** – identifying risk but making the decision to not engage in the activity
  - **Mitigate** – attempt to address risk by making the risk less serious

Information Security Terminology (4 of 4)

Term	Example in Scooter scenario	Example in information security
Asset	Scooter	Employee database
Threat	Steal scooter	Steal data
Threat actor	Thief	Attacker, hurricane
Vulnerability	Hole in fence	Software defect
Attack vector	Climb through hole in fence	Access web server passwords through flaw in operating system
Likelihood	Probability of scooter stolen	Likelihood of virus infection
Risk	Stolen scooter	Virus infection or stolen data

Understanding the Importance of Information Security

- Information security can be helpful in:
  - Preventing data theft
  - Thwarting identity theft
  - Avoiding the legal consequences of not securing information
  - Maintaining productivity
  - Foiling cyberterrorism

Preventing Data Theft

- Preventing data from being stolen is often the primary objective of an organization's information security
- Enterprise data theft involves stealing proprietary business information
- Personal data theft involves stealing credit card numbers

Thwarting Identity Theft

- Identity theft
  - Stealing another person's personal information
  - Usually using it for financial gain
- Example:
  - Steal person's SSN
  - Create new credit card account to charge purchases and leave them unpaid
  - File fraudulent tax returns

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)
  - Payment Card Industry Data Security Standard (PCI DSS)
  - State notification and security laws
    - California's Database Security Breach Notification Act (2003)

Maintaining Productivity

- Post-attack clean up diverts resources away from normal activities
  - Time, money, and other resources
- Table 1-6 shows the cost of attacks

Number of 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	$4066	81
250	$25	3	72	$17,050	300
500	$30	5	80	$28,333	483
1000	$30	10	96	$220,000	1293

Foiling Cyberterrorism

- Cyberterrorism
  - Any premeditated, politically motivated attack against information, computer systems, computer programs, and data
- Designed to:
  - Cause panic
  - Provoke violence
  - Result in financial catastrophe
- May be directed at targets such as the banking industry, military installations, power plants, air traffic control centers, and water systems

Who Are the Threat Actors?

- Threat actor – a generic term used to describe individuals who launch attacks against other users and their computers
  - Most have a goal of financial gain
- Financial cybercrime is often divided into two categories:
  - First category focuses on individuals as the victims
  - Second category focuses on enterprises and government
- Different groups of threat actors can vary widely, based on:
  - Attributes
  - Funding and resources
  - Whether internal or external to the enterprise or organization
  - Intent and motivation

Script Kiddies (1 of 2)

- **Script kiddies** - individuals who want to attack computers yet they lack the knowledge of computers and network needed to do so
- They download automated hacking software (scripts) from websites
- Over 40 percent of attacks require low or no skills

Script Kiddies (2 of 2)

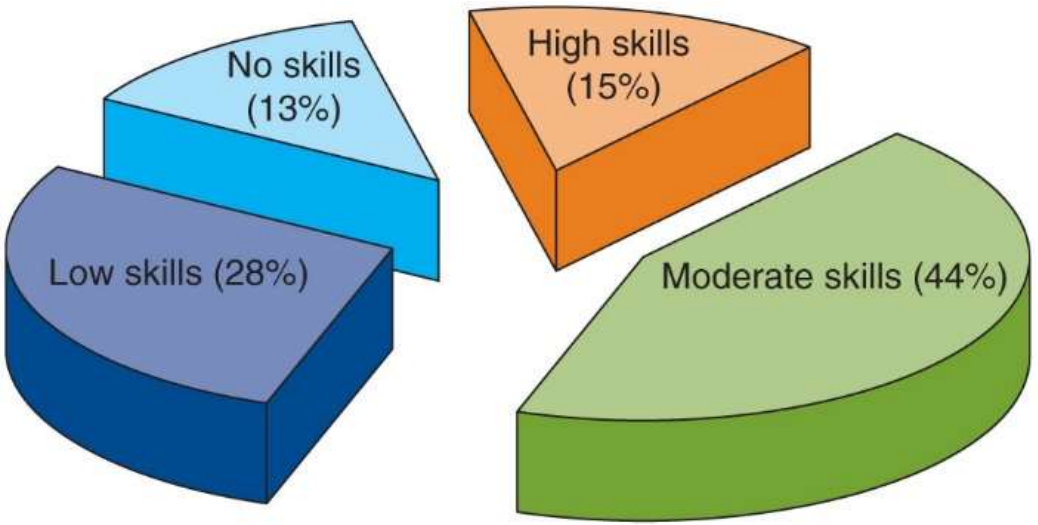


Figure 1-5 Skills needed for creating attacks

Hactivists

- Hactivists - attackers who attack for ideological reasons that are generally not as well-defined as a cyberterrorist's motivation
- Examples of hactivist attacks:
  - Breaking into a website and changing the contents on the site to make a political statement
  - Disabling a website belonging to a bank because the bank stopped accepting payments that were deposited into accounts belonging to the hactivists

Nation State Actors

- **Nation state actor** - an attacker commissioned by the governments to attack enemies' information systems
  - May target foreign governments or even citizens of the government who are considered hostile or threatening
  - Known for being well-resourced and highly trained
- **Advanced Persistent Threat (APT)** - multiyear intrusion campaign that targets highly sensitive economic, proprietary, or national security information

Insiders

- Employees, contractors, and business partners
- Over 58 percent of breaches attributed to insiders
- Examples of insider attacks:
  - Health care worker may publicize celebrities' health records
    - Disgruntled over upcoming job termination
  - Stock trader might conceal losses through fake transactions
  - Employees may be bribed or coerced into stealing data before moving to a new job

Other Threat Actors

Threat Actor	Description	Explanation
Competitors	Launch attack against an opponent's system to steal classified information	Competitors may steal new product research or list of current customers to gain a competitive advantage
Organized crime	Moving from traditional criminal activities to more rewarding and less risky online attacks	Criminal networks are usually run by a small number of experienced online criminal networks who do not commit crimes themselves but act as entrepreneurs
Brokers	Sell their knowledge of a vulnerability to other attackers or governments	Individuals who uncover vulnerabilities do not report it to the software vendor but instead sell them to the highest bidder
Cyberterrorists	Attack a nation's network and computer infrastructure to cause disruption and panic among citizens	Targets may include a small group of computers or networks that can affect the largest number of users, such as the computers that control the electrical power grid of a state or region

Defending Against Attacks

- Five fundamental security principles for defenses:
  - Layering
  - Limiting
  - Diversity
  - Obscurity
  - Simplicity

Layering

- Information security must be created in layers
  - A single defense mechanism may be easy to circumvent
  - Making it unlikely that an attacker can break through all defense layers
- Layered security approach (also called defense-in-depth)
  - Can be useful in resisting a variety of attacks
  - Provides the most comprehensive protection

Limiting

- Limiting access to information:
  - Reduces the threat against it
- Only those who must use data should be granted access
  - Should be limited to only what they need to do their job
- Methods of limiting access
  - Technology-based - such as file permissions
  - Procedural - such as prohibiting document removal from premises

Diversity

- Closely related to layering
  - Layers must be different (diverse)
- If attackers penetrate one layer:
  - Same techniques will be unsuccessful in breaking through other layers
- Breaching one security layer does not compromise the whole system
- Example of diversity
  - Using security products from different manufacturers
  - Groups who are responsible for regulating access (control diversity) are different

Obscurity

- Obscuring inside details to outsiders
- Example: not revealing details
  - Type of computer
  - Operating system version
  - Brand of software used
- Difficult for attacker to devise attack if system details are unknown

Simplicity

- Nature of information security is complex
- Complex security systems:
  - Can be difficult to understand and troubleshoot
  - Are often compromised for ease of use by trusted users
- A secure system should be simple from the inside
  - But complex from the outside

Frameworks and Reference Architectures

- Industry-standard frameworks and reference architectures
  - Provide a resource of how to create a secure IT environment
  - Give an overall program structure and security management guidance to implement and maintain an effective security program
- Various frameworks/architectures are specific to a particular sector (industry-specific frameworks)
  - Such as the financial industry
- Some frameworks/architectures are domestic
  - While other s are world wide

Chapter Summary (1 of 2)

- Information security attacks have grown exponentially in recent years
- There are many reasons for the high number of successful attacks
- It is difficult to defend against today's attacks
- Information security protects information's integrity, confidentiality, and availability:
  - On devices that store, manipulate, and transmit information
  - Using products, people, and procedures

Chapter Summary (2 of 2)

- Main goals of information security
  - Prevent data theft
  - Thwart identity theft
  - Avoid legal consequences of not securing information
  - Maintain productivity
  - Foil cyberterrorism
- Threat actors fall into several categories and exhibit different attributes
- Although multiple defenses may be necessary to withstand the steps of an attack, these defenses should be based on five security principles:
  - Layering, limiting, diversity, obscurity, and simplicity