Information Security (CP3404)

Chapter 1 – Introduction to Security

Based on the Fifth Edition of:

M. Ciampa:. *CompTIA® Security + Guide to Network Security Fundamentals*

Department of Information Technology, College of Business, Law & Governance

Learning Objectives

- Describe the challenges of securing information
- Define information security and explain why it is important
- Identify the types of attackers that are common today
- List the basic steps of an attack
- Describe the five (5) basic principles of defense

Outline

Introduction

- Today all citizens forced to continually protect themselves from attacks by invisible foes (e.g., random shootings, suicide car bombings, airplane hijackings, etc.)
- Attacks not just physical but also include attacks on information technology
- Attacks directed at individuals, schools, businesses, and governments through desktop computers, laptops, smart-phones, and tablet computers
- Information security is focused on protecting electronic information of organizations and users

Introduction

Two (2) broad categories of information security personnel are responsible for this protection

1. Information security managerial personnel – administer and manage plans, policies, and people
2. Information security technical personnel – concerned with designing, configuring, installing, and maintaining technical security equipment

Within these two broad categories are four (4) generally recognized security positions:

Introduction

1. Chief Information Security Officer (CISO) – Reports directly to CIO and responsible for assessing, managing, and implementing security
2. Security manager – Reports to CISO and supervises technicians, administrators, and security staff
3. Security administrator – Manages daily operations of security technology; has both technical knowledge and managerial skills
4. Security technician – Provide technical support to configure security hardware, implement security software, and diagnose and troubleshoot problems

Introduction

Computing Technology Industry Association (CompTIA)

- CompTIA Security+ certification is widely recognized and highly respected vendor-neutral credential
- Employees with certifications in security are in high demand
- Security is rarely off-shored or outsourced
- U.S. Bureau of Labor Statistics (BLS) Occupational Outlook Handbook indicates job outlook for information security analysts through end of decade expected to grow by 22%, faster than average growth rate

Quick Quiz

1. The _____ is primarily responsible for assessing, managing, and implementing security.
   (a) security administrator
   (b) security manager
   (c) security technician
   (d) chief information security officer (CISO)

   Answer:

Quick Quiz

1. The _____ is primarily responsible for assessing, managing, and implementing security.
   (a) security administrator
   (b) security manager
   (c) security technician
   (d) chief information security officer (CISO)

   Answer: (d)

Quick Quiz

1. The _____ is primarily responsible for assessing, managing, and implementing security.
   (a) security administrator
   (b) security manager
   (c) security technician
   (d) chief information security officer (CISO)

   Answer: (d)

2. What information security position reports to the CISO and supervises technicians, administrators, and security staff?
   (a) auditor
   (b) engineer
   (c) manager
   (d) inspector

   Answer:

Quick Quiz

1. The _____ is primarily responsible for assessing, managing, and implementing security.
   (a) security administrator
   (b) security manager
   (c) security technician
   (d) chief information security officer (CISO)

   Answer: (d)

2. What information security position reports to the CISO and supervises technicians, administrators, and security staff?
   (a) auditor
   (b) engineer
   (c) manager
   (d) inspector

   Answer: (c)

Challenges of Securing Information

- A silver bullet is a specific and fail-safe solution that very quickly and easily solves a serious problem
- Is there such a silver bullet for securing computers, e.g., by installing a better hardware device or using a more secure software application?
- In reality, no single and simple solution is available
- This is because of different types of attacks that users face today as well as the difficulties in defending against these attacks

Today's Security Attacks

- Balances manipulated on prepaid debit cards
- Home Wi-Fi network attacked
- Twitter accounts exploited
- Ploutus ATM malware
- Manipulate aircraft and ocean vessels
- Computer cluster for cracking passwords
- Apple Mac vulnerabilities
- $\cdots$, and so forth

Today's Security Attacks

Organization	Description of security breach	Number of identities exposed
University of Washington Medicine, WA	An employee opened an email attachment containing malicious software that infected the employee's computer and compromised the information on it. Patient names, Social Security numbers, phone numbers, addresses, and medical record numbers dating back five years may have been affected.	90,000
Maricopa County Community College District, AZ	An unspecified data breach may have exposed the information of current and former students, employees, and vendors. Names, Social Security numbers, bank account information, and dates of birth, as well as student academic information, may have been viewed by unauthorized parties.	2.49 million
University of California, San Francisco, CA	The theft of a physician's laptop from a car may have resulted in the exposure of patient information, including patient names, Social Security numbers, dates of birth, and medical record numbers.	8294
Redwood Memorial Hospital, CA	A USB flash drive was discovered missing that contained patient names, report ID numbers, test indications, ages, heights, weights, and clinical summaries of test findings for patients who were seen over a period of 12 years.	1039
Anthem Blue Cross, CA	The Social Security numbers and tax identification numbers of California doctors were posted in the online provider directory.	24,500
New York City Police Department, NY	A former police detective pleaded guilty to paying attackers to steal passwords associated with the email accounts of other officers. At least 43 email accounts and one cellular phone account were hacked.	30
Adobe Systems, San Jose, CA	The email addresses, encrypted passwords and password hints from Adobe Systems customers were stolen from a backup system about to be decommissioned.	152 million
Target Corporation, Minneapolis, MN	The credit and debit card numbers, expiration dates, and 3-digit CVV ("Card Verification Value") numbers of customers who made purchases during a 3-week period were stolen.	110 million

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

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 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 are no longer limited to highly skilled attackers.
Faster detection of vulnerabilities	Attackers can discover security holes in hardware or software more quickly.
Delays 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.
Introduction of BYOD	Organizations 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.

Table 1-2 Difficulties in defending against attacks

Difficulties in Defending Against Attacks

Figure 1-1 Menu of attack tools

Source: Kali Linux

Quick Quiz

1. Which of the following is NOT a reason why it is difficult to defend against today's attackers?
   (a) increased speed of attacks
   (b) simplicity of attack tools
   (c) greater sophistication of defense tools
   (d) delays in security updating

   Answer:

Quick Quiz

1. Which of the following is NOT a reason why it is difficult to defend against today's attackers?
   (a) increased speed of attacks
   (b) simplicity of attack tools
   (c) greater sophistication of defense tools
   (d) delays in security updating

   Answer: (c)

Quick Quiz

1. Which of the following is NOT a reason why it is difficult to defend against today's attackers?
   (a) increased speed of attacks
   (b) simplicity of attack tools
   (c) greater sophistication of defense tools
   (d) delays in security updating

   Answer: (c)

2. Which position below is considered an entry-level position for a person who has the necessary technical skills?
   (a) security technician
   (b) security administrator
   (c) CISO
   (d) security manager

   Answer:

Quick Quiz

1. Which of the following is NOT a reason why it is difficult to defend against today's attackers?
   (a) increased speed of attacks
   (b) simplicity of attack tools
   (c) greater sophistication of defense tools
   (d) delays in security updating

   Answer: (c)

2. Which position below is considered an entry-level position for a person who has the necessary technical skills?
   (a) security technician
   (b) security administrator
   (c) CISO
   (d) security manager

   Answer: (a)

What is Information Security?

Before defense is possible, one must understand:

- What is security
- What information security is
- Information security terminology
- Why it is important

Understanding Security

- Security is defined as either the *process* (how to achieve security) or the *goal* (what it means to have security).
- In reality security is both: it is the *goal* to be free from danger as well as the *process* that achieves that freedom
- Security is *the necessary steps to protect a person or property from harm.* This harm may come from one of two sources:
  1. Direct action that is intended to inflict damage
  2. Indirect and unintentional action

Understanding Security

Relationship between Security and Convenience

- As security is increased, convenience is often decreased
- Security is inversely proportional to convenience
- The more secure something is, the less convenient it may become to use
- Security is sacrificing convenience for safety or giving up short-term comfort for long-term protection

Understanding Security

Relationship between Security and Convenience

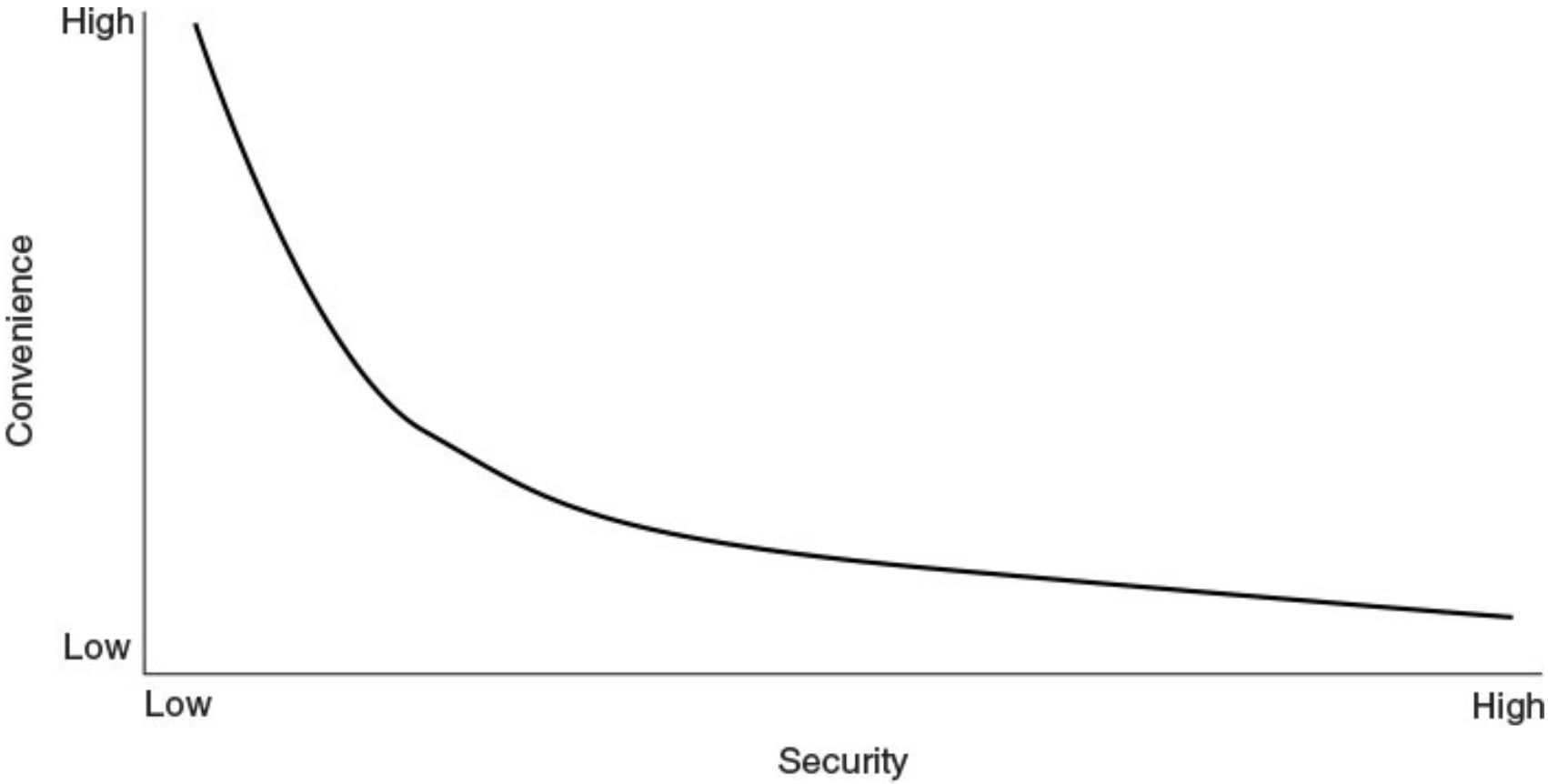

Figure 1-2 Relationship of security to convenience

Defining Information Security

- Information security – Tasks of securing information;
  - Manipulated by a microprocessor
  - Stored on a storage device
  - Transmitted over a network
- Protection – Information security cannot completely prevent successful attacks or guarantee that a system is totally secure
- Protective measures ward off attacks and prevent total collapse of the system when a successful attack does occur

Defining Information Security

The value of information comes from the characteristics it possesses:

Three (3) protections (also known as CIA triangle) that must be extended over information:

1. Confidentiality – Ensures only authorized parties can view information
2. Integrity – Ensures information not altered
3. Availability – Ensures information accessible when needed to authorized parties

Defining Information Security

In addition to CIA, three (3) additional protections must be extended over information (AAA):

- Authentication – Ensures that the individual is who she claims to be (the authentic or genuine person) and not an imposter
- Authorization – Providing permission or approval to specific technology resources
- Accounting – Provides tracking of events (e.g., who accessed the web server, from what location, and at what specific time)

Defining Information Security

Securing Devices

- Information security involves more than protecting the information itself. Information is:
  - Stored on computer hardware
  - Manipulated by software
  - Transmitted by communications
- Each of these areas must also be protected

Defining Information Security

Three Entities

Information security is achieved through protecting information and devices in three layers:

1. Products
2. People
3. Policies and procedures

Policies and procedures enable people to understand how to use products to protect information

Defining Information Security

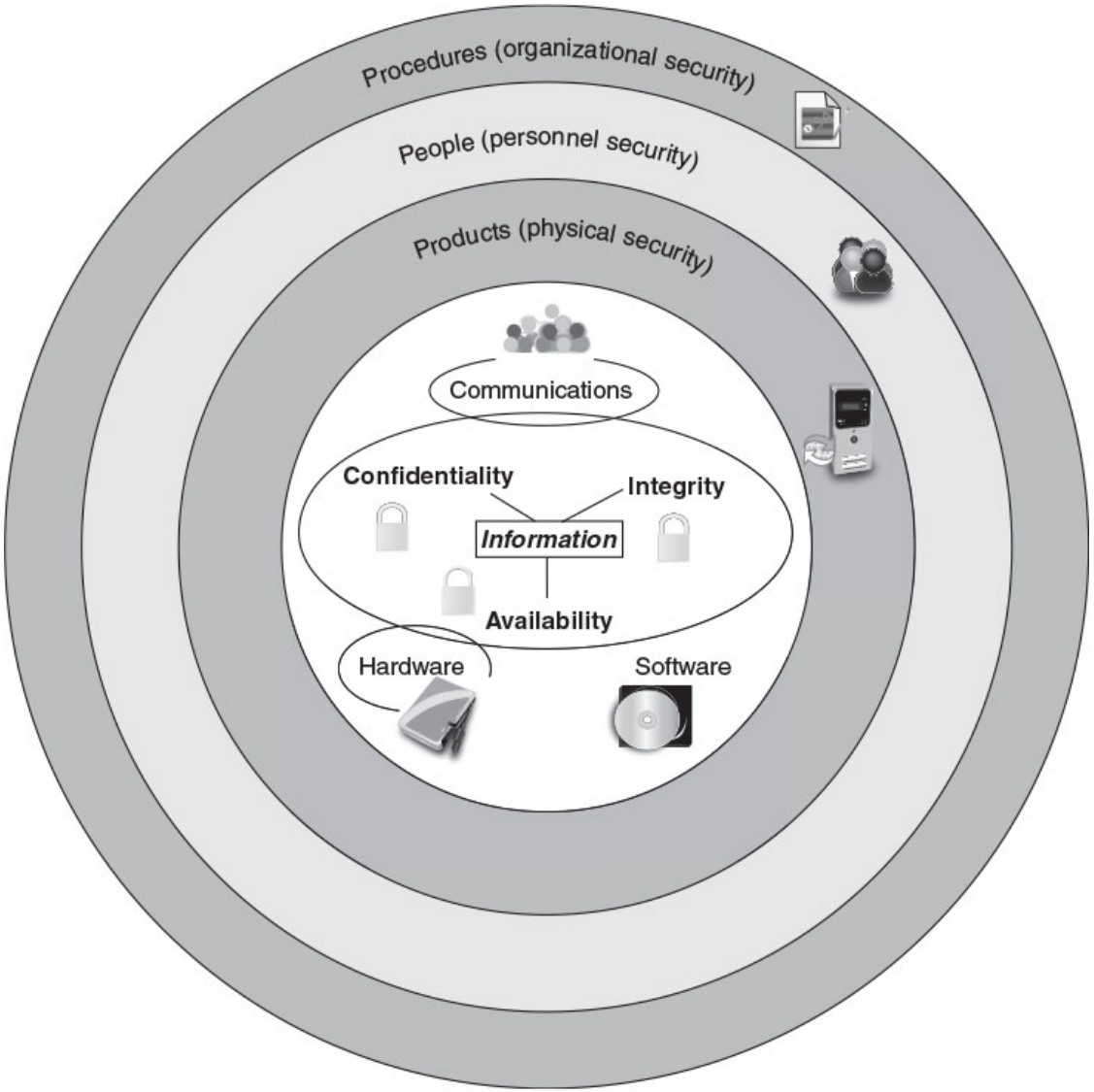

Figure 1-3 Information security layers

Defining Information Security

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 organization to ensure that people correctly use the products.

Table 1-3 Information security layers

Quick Quiz

1. _____ ensures that only authorized parties can view the information.
   Answer:

Quick Quiz

1. _____ ensures that only authorized parties can view the information.
   Answer: Confidentiality

Quick Quiz

1. _____ ensures that only authorized parties can view the information.

   Answer: Confidentiality

2. Which of the following terms best describes ensuring that data is accessible to authorized users?

   (a) Integrity
   (b) Accounting
   (c) Availability
   (d) BYOD

   Answer:

Quick Quiz

1. _____ ensures that only authorized parties can view the information.

   Answer: Confidentiality

2. Which of the following terms best describes ensuring that data is accessible to authorized users?

   (a) Integrity
   (b) Accounting
   (c) Availability
   (d) BYOD

   Answer: (c)

Quick Quiz

1. _____ ensures that only authorized parties can view the information.
   Answer: Confidentiality

2. Which of the following terms best describes ensuring that data is accessible to authorized users?
   (a) Integrity
   (b) Accounting
   (c) Availability
   (d) BYOD

   Answer: (c)

3. **True or False:** Security is the goal to be free from danger as well as the process that achieves the freedom.
   Answer:

Quick Quiz

1. _____ ensures that only authorized parties can view the information.
   Answer: Confidentiality

2. Which of the following terms best describes ensuring that data is accessible to authorized users?
   (a) Integrity
   (b) Accounting
   (c) Availability
   (d) BYOD

   Answer: (c)

3. **True or False:** Security is the goal to be free from danger as well as the process that achieves the freedom.
   Answer: True

Information Security terminology

Asset

- Asset is an item that has value
- In an organization, assets have the following qualities:
  - They provide value to the organization
  - They cannot easily be replaced without a significant investment in expense, time, worker skill, and/or resources
  - They can form part of the organization's corporate identity.

Information Security terminology

Asset

- Asset is an item that has value
- In an organization, assets have the following qualities:
  - They provide value to the organization
  - They cannot easily be replaced without a significant investment in expense, time, worker skill, and/or resources
  - They can form part of the organization's corporate identity.

Example

A faculty desktop computer that can easily be replaced would generally not be considered an asset, yet the information contained on that computer can be an asset.

Information Security terminology

Element name	Description	Example	Critical asset?
Information	Data that has been collected, classified, organized, and stored in various forms	Customer, personnel, production, sales, marketing, and finance databases	Yes: Extremely difficult to replace
Customized business software	Software that supports the business processes of the organization	Customized order transaction application	Yes: Unique and customized for the organization
System software	Software that provides the foundation for application software	Operating system	No: Can be easily replaced
Physical items	Computers equipment, communications equipment, storage media, furniture, and fixtures	Servers, routers, DVDs, and power supplies	No: Can be easily replaced
Services	Outsourced computing services	Voice and data communications	No: Can be easily replaced

Table 1-4 Information technology assets

Information Security terminology

Threat

- Threat: Action that has the potential to cause harm
- Information security threats are events or actions that represent a danger to information assets
- Threat by itself does not mean that security has been compromised; rather, it simply means that the potential for creating a loss is real
- Threat can result in the corruption or theft of information, a delay in information being transmitted, or loss of good will or reputation

Information Security terminology

Threat Agent

- Threat Agent is a person or element that has the power to carry out a threat
- Threat agent can be:
  - Person attempting to break into a secure computer network
  - Force of nature such as a hurricane that could destroy computer equipment, and thus, destroy information
  - Malicious software that attacks the computer network

Information Security terminology

Vulnerability

- Vulnerability is a flaw or weakness that allows a threat agent to bypass security

Information Security terminology

Vulnerability

- Vulnerability is a flaw or weakness that allows a threat agent to bypass security

Example

A software defect in an operating system that allows an unauthorized user to gain control of a computer without the users knowledge or permission

Information Security terminology

Threat Vector

- Threat vector means by which an attack can occur

Example

An attacker, knowing that a flaw in a web server's operating system has not been patched, is using the threat vector (exploiting the vulnerability) to steal user passwords

Information Security terminology

Threat Vector

- Threat vector means by which an attack can occur

Example

An attacker, knowing that a flaw in a web server's operating system has not been patched, is using the threat vector (exploiting the vulnerability) to steal user passwords

Threat Likelihood

- Threat likelihood is the probability that threat will come to fruition

Information Security terminology

Risk

- Risk is a situation that involves exposure to some type of danger.
- There are five (5) options when dealing with risks:
  1. Risk avoidance – Making decision to not engage in the activity
  2. Acceptance – Risk is acknowledged but no steps are taken to address it
  3. Mitigation – Attempts to address the risks by making risks less serious
  4. Deterrence – Warning/Informing attacker of the harm that may come his way if he attacks an asset
  5. Transference – Transfer the risk to a third party

Information Security terminology

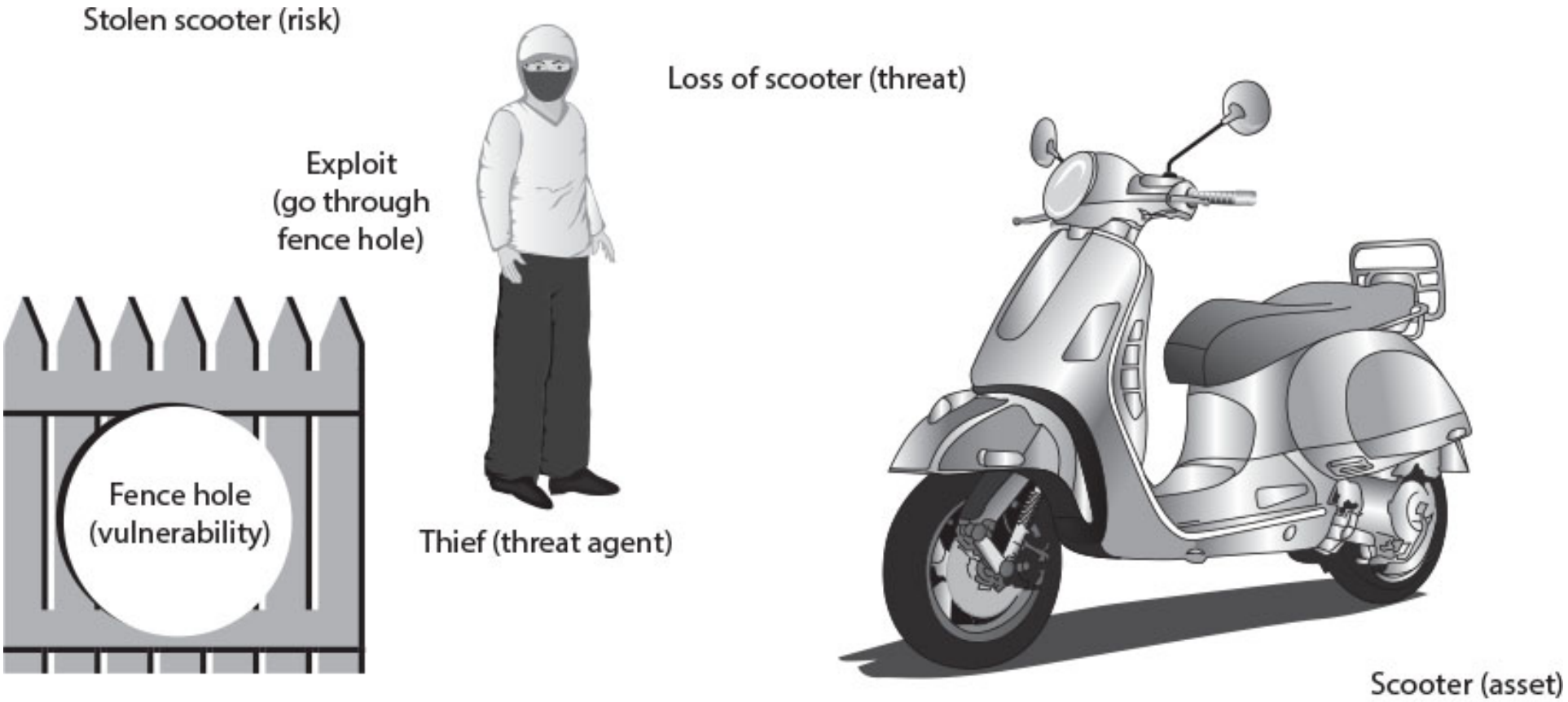

Figure 1-4 Information security components analogy

Information Security terminology

Term	Example in Ellie's scenario	Example in information security
Asset	Scooter	Employee database
Threat	Steal scooter	Steal data
Threat agent	Thief	Attacker, hurricane
Vulnerability	Hole in fence	Software defect
Threat vector	Climb through hole in fence	Access web server passwords through flaw in operating system
Threat likelihood	Probability of scooter stolen	Likelihood of virus infection
Risk	Not purchase scooter	Not install wireless network

Table 1-5 Information security terminology

Understanding the Importance of Information Security

Preventing Data Theft

- Preventing data from being stolen is cited as primary objective of information security
- Business data theft involves stealing proprietary business information (e.g., reserach for a new drug)
- Personal data theft involves stealing credit card numbers that can be used to purchase thousands of dollars of merchandise

Understanding the Importance of Information Security

Thwarting Identity Theft

- Identity theft involves stealing another person's personal information and then using it in unauthorized manner for financial gain. For example:
  - Steal person's Social Security Number (SSN) and then using the information to impersonate the victim
  - Create new bank/credit card account under the victim's name and then large purchases are charged to these accounts
- One rapidly growing area of identity theft involves filing fictitious income tax returns with the U.S. Internal Revenue Service (IRS).

Understanding the Importance of Information Security

Avoiding Legal Consequences

- Businesses that fail to protect data they possess may face serious financial penalties from federal or state laws.

Maintaining Productivity

- Cleaning up after an attack diverts time, money, and other resources away from normal activities
- Employees cannot be productive and complete important tasks during or after at attack because computers and networks cannot function properly

Understanding the Importance of Information Security

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

Table 1-6 Cost of attacks

Understanding the Importance of Information Security

Foiling Cyberterrorism

- Unlike an attack that is designed to steal information or erase a user's hard disk drive, cyberterrorism attacks are intended to cause panic or provoke violence among citizens
- Attacks are directed at targets such as the banking industry, power plants, air traffic control centers, and water systems.
- one of the challenges in combating cyberterrorism is that many of the prime targets are not owned and managed by the federal government

Quick Quiz

1. A(n) _____ is defined as something that has a value.
   Answer:

Quick Quiz

1. A(n) _____ is defined as something that has a value.
   Answer: asset

Quick Quiz

1. A(n) _____ is defined as something that has a value.
   Answer: asset

2. Addressing a risk by making it less serious is known as _____.
   (a) risk avoidance
   (b) ris acceptance
   (c) risk mitigation
   (d) risk deterrence

   Answer:

Quick Quiz

1. A(n) _____ is defined as something that has a value.
   Answer: asset

2. Addressing a risk by making it less serious is known as _____.
   (a) risk avoidance
   (b) ris acceptance
   (c) risk mitigation
   (d) risk deterrence

   Answer: (c)

Quick Quiz

1. A(n) _____ is defined as something that has a value.
   Answer: asset

2. Addressing a risk by making it less serious is known as _____.
   (a) risk avoidance
   (b) ris acceptance
   (c) risk mitigation
   (d) risk deterrence

   Answer: (c)

3. A(n) _____ is the likelihood that a threat agent will exploit a vulnerability.
   Answer:

Quick Quiz

1. A(n) _____ is defined as something that has a value.
   Answer: asset

2. Addressing a risk by making it less serious is known as _____.
   (a) risk avoidance
   (b) ris acceptance
   (c) risk mitigation
   (d) risk deterrence

   Answer: (c)

3. A(n) _____ is the likelihood that a threat agent will exploit a vulnerability.
   Answer: risk

Who Are the Attackers?

- Hacker – Older term referred to a person who used advanced computer skills to attack computers
- Black hat hackers – Attackers who violated computer security for personal gain or to inflict malicious damage
- White hat hackers – (a.k.a. Ethical attackers) who received permission to probe system for any weaknesses
- Gray hat hackers – Attackers who would break into a computer system without permission and then publicly disclose vulnerability

Who Are the Attackers?

Cybercriminals

- Generic term describes individuals who launch attacks against other users and their computers
- Instead of attacking a computer to show off their technology skills (fame), cybercriminals have a more focused goal of financial gain (fortune): cybercriminals steal information or launch attacks to generate income
- These targeted attacks against financial networks and the theft of personal information are sometimes known as cybercrime.

Who Are the Attackers?

Cybercriminals (cont.)

- Financial cybercrime is often divided into two (2) categories:

1. Focuses on individuals and businesses. Steal and use stolen data, credit card number, online financial account information, or SSNs to profit from its victims.
2. Focuses on businesses and governments. Steal research on a new product from business so that they can sell it to an unscrupulous foriegn supplier who will then build an imitation model of the product to sell worldwide

Who Are the Attackers?

Script Kiddies

- Unskilled users with goal to break into computers to create damage
- Download automated hacking software (scripts) to use to perform malicious acts
- Attack software today has menu systems and attacks are even easier for unskilled users
- 40 percent (40%) of attacks performed by script kiddies

Who Are the Attackers?

Script Kiddies (cont.)

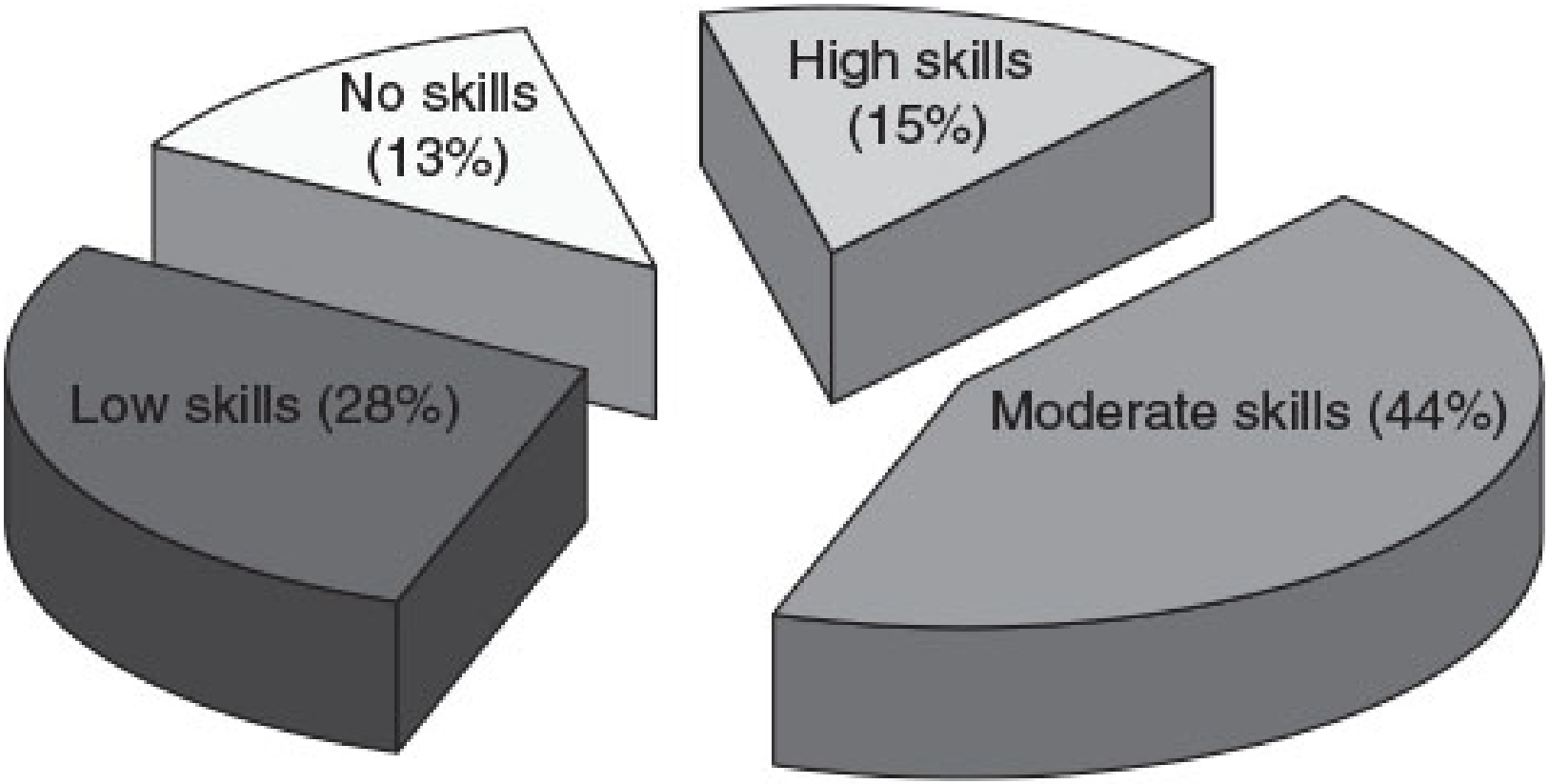

Figure 1-5 Skills needed for creating attacks

Who Are the Attackers?

JAMES COOK UNIVERSITY AUSTRALIA

Brokers

- Individuals who uncover vulnerabilities do not report it to the software vendor but instead sell them to the highest bidder
- These attackers (a.k.a. brokers) sell their knowledge of a vulnerability to other attackers or even governments
- Buyers are generally willing to pay a high price because this vulnerability is unknown

Who Are the Attackers?

Insiders

- Employees, contractors, and business partners (a.k.a. insiders) who steal from employer
- Most malicious insider attacks consist of the sabotage or theft of intellectual property
- Offenders are usually employees who actually believe that the accumulated data is owned by them and not the organization
- Others are employees have been pressured into stealing from their employer through blackmail or the threat of violence

Who Are the Attackers?

JAMES COOK UNIVERSITY AUSTRALIA

Cyberterrorists

- Attackers who have ideological motivation
- Attacking because of their principles and beliefs
- Unlike cybercriminals who continuously probe systems or create attacks, cyberterrorists can be inactive for several years and then suddenly strike in a new way
- Targets may include a small group of computers or networks that can affect the largest number of users, e.g., computers that control the electrical power grid of a state or region

Who Are the Attackers?

Hactivists

- Hactivists (a combination of the words hack and activism) is another group motivated by ideology
- Unlike cyberterrorists who launch attacks against foreign nations to incite panic, hactivists generally not as well-defined.
- Attacks can involve breaking into a website and changing the contents on the site as a means of making a political statement against those who oppose their beliefs
- Other attacks can be retaliatory

Who Are the Attackers?

State-Sponsored Attackers

- Attackers supported by governments for launching computer attacks against their foes (e.g., Flame, Stuxnet)
- Attackers target foreign governments or even citizens of the government who are considered hostile or threatening
- It is expected that more than 300,000 Iranian citizens were having their email messages read without their knowledge by the Iranian government seeking to locate and crack down on dissidents

Who Are the Attackers?

Attacker category	Objective	Typical target	Sample attack
Cybercriminals	Fortune over fame	Users, businesses, governments	Steal credit card information
Script kiddies	Thrills, notoriety	Businesses, users	Erase data
Brokers	Sell vulnerability to highest bidder	Any	Find vulnerability in operating system
Insiders	Retaliate against employer, shame government	Governments, businesses	Steal documents to publish sensitive information
Cyberterrorists	Cause disruption and panic	Businesses	Cripple computers that control water treatment
Hactivists	To right a perceived wrong against them	Governments, businesses	Disrupt financial website
State-sponsored attackers	Spy on citizens, disrupt foreign government	Users, governments	Read user's email messages

Table 1-7 Characteristics of attackers

Quick Quiz

1. The motivation of _____ may be defined as ideology, or attacking for the sake of their principles or belief.
   (a) brokers
   (b) cyberterrorists
   (c) hactivists
   (d) cybercriminals

   Answer:

Quick Quiz

1. The motivation of _____ may be defined as ideology, or attacking for the sake of their principles or belief.
   (a) brokers
   (b) cyberterrorists
   (c) hactivists
   (d) cybercriminals

   Answer: (b)

Quick Quiz

1. The motivation of _____ may be defined as ideology, or attacking for the sake of their principles or belief.
   (a) brokers
   (b) cyberterrorists
   (c) hactivists
   (d) cybercriminals

   Answer: (b)

2. Attackers who do their work by downloading automated attack software from websites and use it to perform malicious acts are known as _____.
   (a) blackhat hackers
   (b) white hat hackers
   (c) gray hat hackers
   (d) script kiddies

   Answer:

Quick Quiz

1. The motivation of _____ may be defined as ideology, or attacking for the sake of their principles or belief.
   (a) brokers
   (b) cyberterrorists
   (c) hactivists
   (d) cybercriminals

   Answer: (b)

2. Attackers who do their work by downloading automated attack software from websites and use it to perform malicious acts are known as _____.
   (a) blackhat hackers
   (b) white hat hackers
   (c) gray hat hackers
   (d) script kiddies

   Answer: (d)

Attacks and Defenses

- A kill chain is a military term used to describe the systematic process to target and engage an enemy
- An attacker who attempts to break into a web server or computer network actually follows these same steps (a.k.a. Cyber Kill Chain (CKC)), which consists of seven (7) steps:

Attacks and Defenses

Steps of an Attack

1. Reconnaissance – Probe for any information about the system to reveal if the system is a viable target for an attack and how it could be attacked
2. Weaponization – Create an exploit and package it into a deliverable payload that can be used against the target
3. Delivery – The weapon is transmitted to the target
4. Exploitation – The exploitation stage triggers the intruders' exploit

Attacks and Defenses

Steps of an Attack (Cont.)

5. Installation – The weapon is installed to either attack the computer or install a remote *backdoor* so the attacker can access the system

6. Command and Control – Often the compromised system connects back to the attacker so that the system can be remotely controlled by the attacker and receive future instructions

7. Actions on Objectives – Now attackers can start to take actions to achieve their original objectives, such as stealing user passwords or launching attacks against other computers

Steps of an Attack

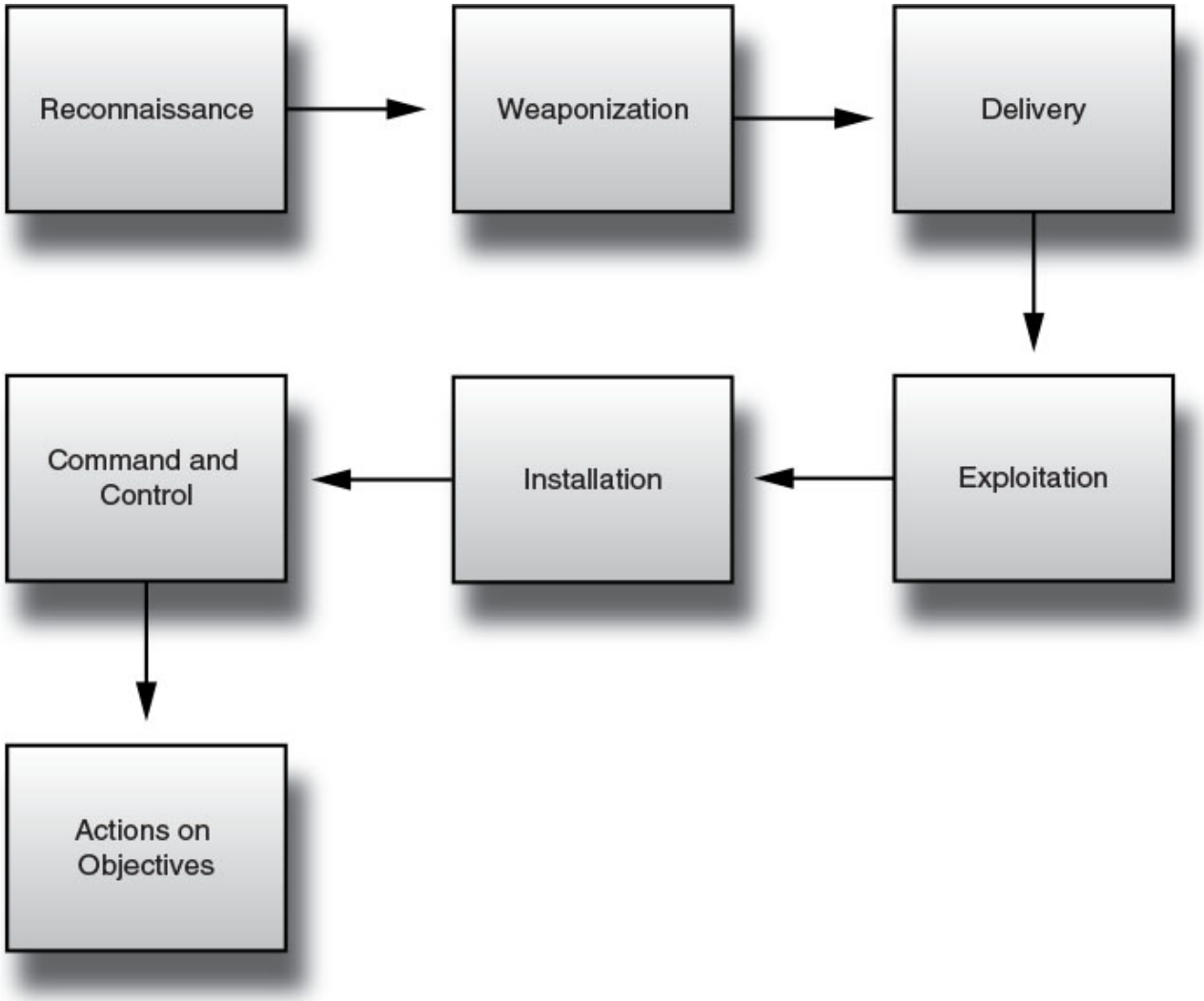

Figure 1-6 Cyber Kill Chain®

Cyber Kill Chain is a registered trademark of Lockheed Martin Corporation.

Defenses Against Attacks

Although multiple defenses may be necessary to withstand an attack, these defenses should be based on five (5) fundamental security principles:

1. Layering
2. Limiting
3. Diversity
4. Obscurity
5. Simplicity

Defenses Against Attacks

Layering

- Information security must be created in layers
- Single defense mechanism may be easy to circumvent
- Unlikely that attacker can break through all defense layers
- Layered security approach
  - Can be useful in resisting a variety of attacks
  - Provides the most comprehensive protection

Defenses Against Attacks

Limiting

- Limiting access to information reduces the threat against it
- Only those who must use data granted access
- Amount of access limited to what that person needs to know
- Methods of limiting access
  - Technology (file permissions)
  - Procedural (prohibiting document removal from premises)

Defenses Against Attacks

Diversity

- Closely related to layering
- Layers must be different (diverse)
- If attackers penetrate one layer then same techniques unsuccessful in breaking through other layers
- Breaching one security layer does not compromise the whole system
- Example of diversity is using security products from different manufacturers

Defenses Against Attacks

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

Defenses Against Attacks

Simplicity

- Complex security systems can be hard to understand, troubleshoot, and even feel secure about
- As much as possible, a secure system should be simple for those in the inside to understand and use
- Keeping a system simple from the inside, but complex on the outside, can sometimes be difficult but reaps a major benefit

Quick Quiz

1. Targeted attacks against financial networks, unauthorized access to information, and the theft of personal information is sometimes known as _____.
   Answer:

Quick Quiz

1. Targeted attacks against financial networks, unauthorized access to information, and the theft of personal information is sometimes known as _____.
   Answer: cybercrime

Quick Quiz

1. Targeted attacks against financial networks, unauthorized access to information, and the theft of personal information is sometimes known as _____.
   Answer: cybercrime

2. The basic steps of an attack are known as _____.
   Answer:

Quick Quiz

1. Targeted attacks against financial networks, unauthorized access to information, and the theft of personal information is sometimes known as _____.
   Answer: cybercrime

2. The basic steps of an attack are known as _____.
   Answer: Cyber Kill Chain

Quick Quiz

1. Targeted attacks against financial networks, unauthorized access to information, and the theft of personal information is sometimes known as _____.
   Answer: cybercrime

2. The basic steps of an attack are known as _____.
   Answer: Cyber Kill Chain

3. An example of _____ in information security would be not revealing the type of computer, version of operating system, or brand of software that is used.
   Answer:

Quick Quiz

1. Targeted attacks against financial networks, unauthorized access to information, and the theft of personal information is sometimes known as _____.
   Answer: cybercrime

2. The basic steps of an attack are known as _____.
   Answer: Cyber Kill Chain

3. An example of _____ in information security would be not revealing the type of computer, version of operating system, or brand of software that is used.
   Answer: obscurity