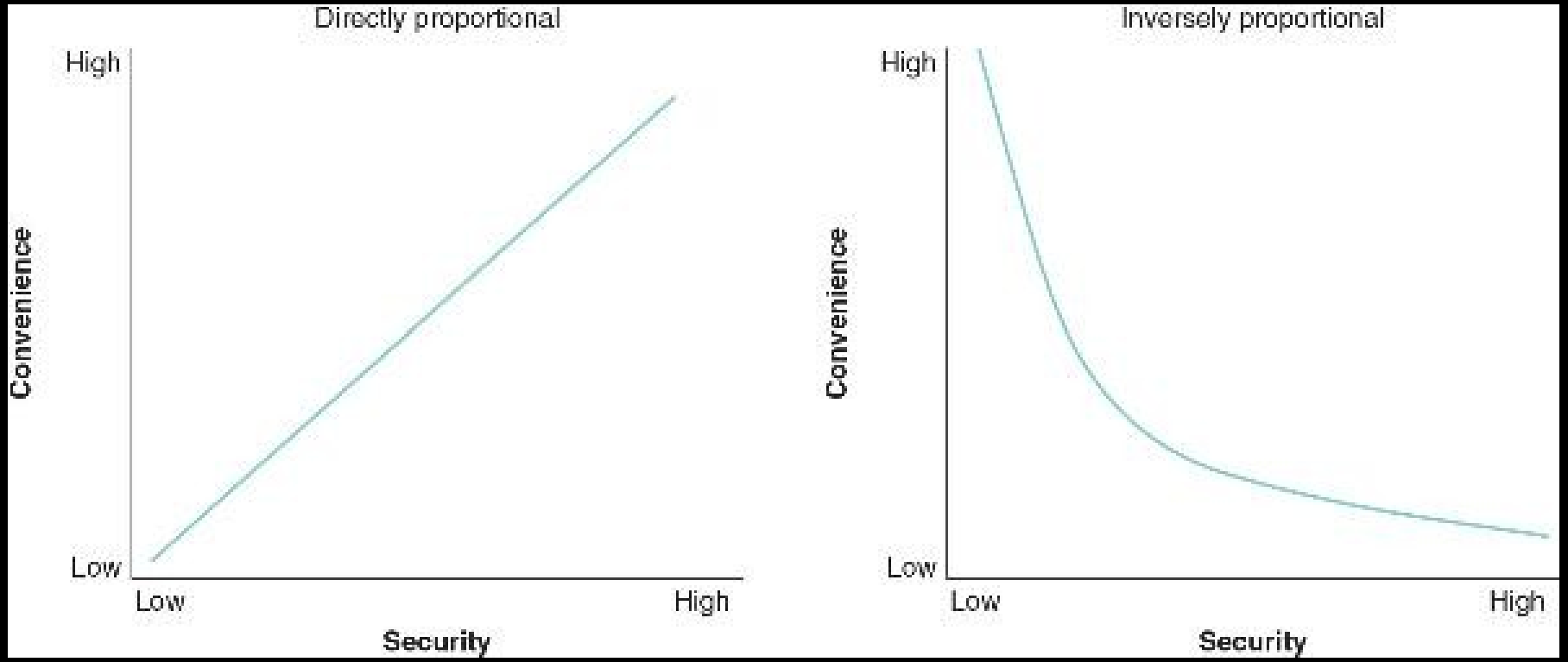
Chapter 1: Introduction to Information Security

Understanding Security

- Security is the state of being free from danger, which is the goal of security
  - It is also defined as the “measures taken to ensure safety”, which is the process of security
- As security is increased, convenience is often decreased
  - The more secure something is, the less convenient it may become to use

Understanding Security



Principles of Security

- The following are three types of security protections (**CIA**):
  - **Confidentiality** ensures that only approved individuals may access information
  - **Integrity** ensures that information is correct and unaltered
  - **Availability** ensures that information is accessible to authorized users

Principles of Security

- Another security principle involves controlling access to information and involves authentication, authorization, and accounting
  - **Authentication** is the act of ensuring a user's credentials as authentic
  - **Authorization** grants permission for a user to take a particular action
  - **Accounting** creates a record that is preserved of who accessed the network, what resources they accessed, and when they disconnected from the network

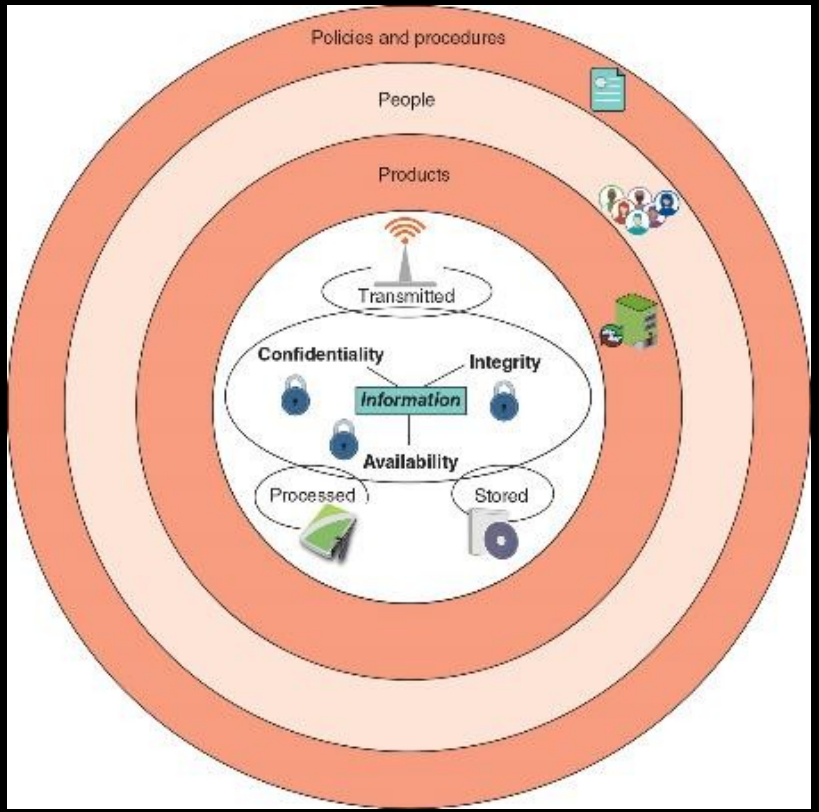
Principles of Security

- A security control is a safeguard that is employed within an enterprise to protect the CIA of information and can include the following:
  - Deterrent controls
  - Preventive controls
  - Detective controls
  - Compensating controls
  - Corrective controls
  - Directive controls

Cybersecurity vs Information Security

- Cybersecurity usually involves a range of practices, processes, and technologies intended to protect devices, networks, and programs that process and store data in an electronic form
- Information security protects “processed data” that is essential in an enterprise environment

Defining Information Security



Question?

- Serafina is studying to take the Security+ certification exam. Which of the following of the CIA elements ensures that only authorized parties can view protected information?

Answer

- Serafina is studying to take the Security+ certification exam. Which of the following of the CIA elements ensures that only authorized parties can view protected information?
- Confidentiality ensures that only authorized parties can view the information. Providing confidentiality can involve several different security tools, ranging from software to encrypt the credit card number stored on the web server to door locks to prevent access to those servers.

Threat Actors and Their Movements

- A **threat actor** is an individual or entity responsible for attacks
  - The generic term *attacker* is also commonly used
- Financial crime is often divided into three categories based on targets:
  - **Individual users**
  - **Enterprises**
  - **Governments**
- Threat actors can be categorized as unskilled attackers, shadow IT, organized crime, insiders, hacktivists, nation-state actors, and others

Unskilled Attackers

- Individuals who want to perform attacks yet lack the technical knowledge to carry them out are sometimes called **unskilled attackers**
- Easy-to-use attacks tools are freely available or can be purchased at a low cost to perform sophisticated attacks
- Unskilled attackers use these types of tools to carry out their attacks
- Their motivation is usually data exfiltration or service disruption

Shadow IT

- The process of bypassing corporate approval for technology purchases is known as **shadow IT**
- The employee’s motivation is often ethical, but it often weakens security

Organized Crime

- Organized crime is a close-knit group of highly-centralized enterprises set up for the purpose of engaging in illegal activities
- In recent years, organized crime has moved into cyberattacks
- They consider this to be less risky and more rewarding than traditional crime
- The motivation is generally financial gain

Insider Threats

- Another threat comes from a company’s own employees, contractors, and business partners, called insiders
- Motivation could be revenge or blackmail
- Attacks from insider threats are hard to recognize

Hacktivists

- Groups or individuals that are strongly motivated by ideology (for the sake of their principles or beliefs) are **hacktivists**
- The types of attacks by hacktivists often involve breaking into a website and changing its contents as a means of a political statement
- Other attacks are retaliatory:
  - Hacktivists have disabled a bank's website that didn't allow online payments deposited into accounts belonging to groups supported by hacktivists
- The motivation is to cause disruption/chaos

Nation-State Actors

- Governments are increasingly employing their own state-sponsored attackers for launching cyberattacks against their foes
  - These attackers are known as **nation-state actors**
- Nation-state actors are often involved in multiyear intrusion campaigns targeting highly sensitive economic, proprietary, or national security information
- A new class of attacks called **advanced persistent threat** (**APT**) use innovative attack tools that silently extract data over an extended period of time

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 a list of current customers to gain a competitive advantage
Brokers	Sell their knowledge of a weakness to other attackers or governments	Individuals who uncover weaknesses do not report them to the software vendor but instead sell them to the highest bidder, who are willing to pay a high price for the unknown weakness
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

Question?

- What is the motivation of an employee who practices shadow IT?

Answer

- What is the motivation of an employee who practices shadow IT?
- The process of bypassing corporate approval for technology purchases is known as shadow IT. The employee’s motivation is often ethical (it has sound moral principles) but nevertheless weakens security.

Threat Vectors and Attacks Surfaces

- An **attack surface** (**threat vector**) is a digital platform that threat actors target for their exploits
- Some attack surfaces can be considered **mainstream** for several reasons:
  - They have been the primary targets of threat actors
  - These attack surfaces are found in all technology settings
  - They continue to bear the brunt of attacks today

Threat Vectors and Attacks Surfaces

- Other threat vectors are more specialized and can be divided into categories such as communications and supply chain
- The most common communication tools are **message-based** and include email, texts, instant messages, and voice calls
- A **supply chain** is a network that moves a product from its creation to the end-user
  - Each link in a supply chain can be a potential threat vector
  - Malware can be injected into a product during its manufacturing, storage, and distribution (called **supply chain infections**)

Threat Vectors and Attacks Surfaces

- Software supply chains have recently been the target of attackers
- An alarming type of supply chain infection targets **open-source software**, which is software where the source code is available for anyone to freely use without restrictions
  - Threat actors add their malicious code to an open-source project, which is then downloaded and installed by unsuspecting victims

Categories of Vulnerabilities

- A **vulnerability** is the state of being exposed to the possibility of being attacked or harmed
- Cybersecurity vulnerabilities can be categorized into software, hardware, misconfigurations, and zero-day vulnerabilities
- Software
  - Vulnerabilities are predominately found in software, with OS software being the chief culprit
  - Attacks may include a **malicious update**

Categories of Vulnerabilities

- Hardware
  - The following hardware vulnerabilities can lead to a successful attack:
    - Difficulty patching firmware, legacy platforms, and end-of-life (EOL) hardware
- Misconfigurations
  - Often configuration settings are not properly implemented, resulting in misconfigurations that can then result in vulnerabilities

Categories of Vulnerabilities

- Zero-day vulnerabilities
  - Vulnerabilities can be exploited by attackers before anyone else even knows it exists
  - This type of vulnerability is called a **zero-day** because it provides zero days of warning
  - Zero-day vulnerabilities are considered extremely serious

Impacts of Attacks

- A successful attack always results in several negative impacts
- These impacts can be classified as the following:
  - Data impacts (see Table 1-8 on the following slide)
  - Overall effects
    - The attack may make systems inaccessible (**availability loss**), which results in lost productivity (**financial loss**)
    - Attacks may affect the public perception of the enterprise (**reputation**)

Impacts of Attacks

Impact	Description	Example
Data loss	The destruction of data so that it cannot be recovered	Maliciously erasing patient data used for cancer research
Data exfiltration	Stealing data to distribute it to other parties	Taking a list of current customers and selling it to a competitor
Data breach	Stealing data to disclose it in an unauthorized fashion	Theft of credit card numbers to sell to other threat actors
Identity theft	Taking personally identifiable information to impersonate someone	Stealing a Social Security number to secure a bank loan in the victim's name

Information Security Resources

- Defenders have the following external cybersecurity resources to help ward off attacks:
  - Frameworks
  - Regulations
  - Legislation
  - Standards
  - Benchmarks/secure configuration guides
  - Information sources

Frameworks

- An information security **framework** is a series of documented processes used to define policies and procedures for implementation and management of security controls in an enterprise environment
- The National Institute of Standards and Technology (NIST) frameworks are divided into three basic parts:
  - **Framework core**
  - **Implementation tiers**
  - **Profiles**

Frameworks


RECOVER
IDENTIFY
CYBERSECURITY
FRAMEWORK
VERSION 1.1
PROTECT
RESPOND
DETECT

Regulations

- The process of adhering to **regulations** is called **regulatory compliance**
- Most organizations must follow multiple regulations from different regulatory bodies
- For information security, there are the following:
  - **Broadly applicable regulations**
  - **Industry-specific-regulations**
  - **U.S. state regulations**
  - **International regulations**

Legislation

- Specific legislation or laws can be enacted by governing bodies that can provide an information security resource
  - These include national, territorial, and state laws
- With the number of different entities involved in passing multiple legislation, this often leads to a “hodge-podge” of legislation and is not always a good cybersecurity resource

Standards

- A standard is a document approved through consensus by a recognized standardization body
  - It provides for frameworks, rules, guidelines, or characteristics for products or related processes and production methods
- One information security compliance standard is the **Payment Card Industry Data Security Standard** (**PCI DSS**)

Benchmarks/Secure Configurations

- **Benchmarks/secure configuration guides** are usually distributed by hardware manufacturers and software developers
  - They serve as a guideline for configuring a device or software so that it is resilient to attacks
- Usually these are platform-/vendor-specific guides that only apply to specific products

Information Sources

- **Requests for comments** (**RFCs**) are document “white papers” that are authored by technology bodies employing specialists, engineers, and scientists who are experts in those areas
- **Data feeds** are continually maintained databases of the latest cybersecurity incidences
- Common cybersecurity data feeds include vulnerability feeds that provide information on the latest vulnerabilities
- The adversary tactics, techniques, and procedures (TTP) is a database of the behavior of threat actors and how they manage attacks

Question?

- What is another name for “attack surface”?

Answer

- What is another name for “attack surface”?
- An attack surface, also called a threat vector, is a digital platform that threat actors target for their exploits.