CHAPTER 1

Confidentiality, Integrity, Availability, and Non-repudiation

Objective 1.1 Understand the Security Concepts of Information Assurance

Information plays a vital role in the operations of modern business, and we find ourselves entrusted with sensitive information about our customers, employees, internal operations, and other critical matters. As information technology professionals, we must work with information security teams, other technology professionals, and business leaders to protect the security of that information.

In this chapter, you'll learn about four of the subobjectives of CC objective 1.1. The remaining material for this objective is covered in Chapter 2, "Authentication and Authorization," and Chapter 3, "Privacy." The following subobjectives are covered in this chapter:

- **Confidentiality**
- **Integrity**
- **Availability**
- **Non-repudiation**

THE CIA TRIAD

Cybersecurity professionals have three primary objectives when it comes to protecting information and systems. They want to ensure that private data remains secret (confidentiality), that information isn't altered without permission (integrity), and that information is available to authorized users when they need it (availability). You can remember these three main goals by thinking of the CIA triad, as shown in Figure 1.1. Each side of this triangle covers one of the three main goals.

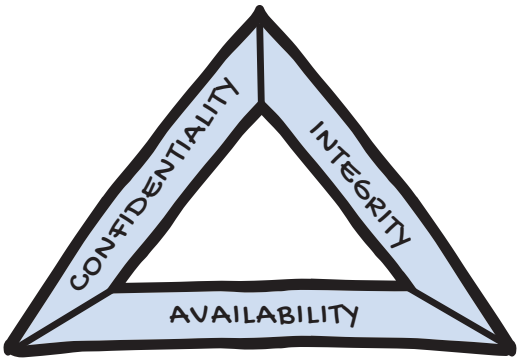

FIGURE 1.1 The CIA triad summarizes the three main goals of information security: confidentiality, integrity, and availability.

Confidentiality

Confidentiality ensures that only authorized individuals have access to information and resources. This is what most people think of when they think about information security—keeping secrets away from prying eyes. And it is, in fact, how security professionals spend the majority of their time.

Confidentiality Risks

As you prepare for the exam, you'll need to understand the main threats against each of the cybersecurity objectives. I'll talk about many different kinds of threats in this book, but I'll begin with the following: snooping, dumpster diving, eavesdropping, wiretapping, and social engineering.

Snooping

Snooping is exactly what the name implies. The individual engaging in snooping wanders around your office or other facility and simply looks to see what information they can gather. When people leave sensitive papers on their desks or in a public area, it creates an opportunity for snooping.

Organizations can protect against snooping by enforcing a clean desk policy. Employees should maintain a clean workspace and put away any sensitive materials whenever they step away, even if it's just for a moment.

Dumpster Diving

Dumpster diving attacks also look for sensitive materials, but the attacker doesn't walk around the office; instead, they look through the trash, trying to find sensitive documents that an employee threw in the garbage or recycling bin.

You can protect your organization against dumpster diving attacks using a simple piece of technology: a paper shredder! If you destroy documents before discarding them, you'll protect against a dumpster diver pulling them out of the trash.

Eavesdropping

Eavesdropping attacks come in both physical and electronic types. In a physical eavesdropping attack, the attacker simply positions themselves where they can overhear conversations, such as in a cafeteria or hallway, and then listens for sensitive information.

You can protect against eavesdropping attacks by putting rules in place limiting where sensitive conversations may take place. For example, sensitive conversations should generally take place in a closed office or conference room.

Electronic eavesdropping attacks are also known as *wiretapping*. They occur when an attacker gains access to a network and monitors the data being sent electronically within an office.

The best way to protect against electronic eavesdropping attacks is to use encryption to protect information being sent over the network. If data is encrypted, an attacker who intercepts that data won't be able to make any sense of it. I'll talk more about how encryption works later in this book.

Social Engineering

The last type of confidentiality attack I'll talk about is *social engineering*. In a social engineering attack, the attacker uses psychological tricks to persuade an employee to give them sensitive information or access to internal systems. They might pretend that they're on an urgent assignment from a senior leader, impersonate an IT technician, or send a phishing email.

It's difficult to protect against social engineering attacks. The best defense against these attacks is educating users to recognize the dangers of social engineering and empower them to intervene when they suspect an attack is taking place.

Integrity

Security professionals are also responsible for protecting the *integrity* of an organization's information. This means that there aren't any unauthorized changes to information. Unauthorized changes may come in the form of a hacker seeking to intentionally alter information or a service disruption accidentally affecting data stored in a system. In either case, it's the information security professional's responsibility to prevent these lapses in integrity.

Integrity Risks

This section covers four types of integrity attacks: the unauthorized modification of information, impersonation attacks, man-in-the-middle (MitM) attacks, and replay attacks.

Unauthorized Modification of Information

The unauthorized modification of information occurs when an attacker gains access to a system and makes changes that violate a security policy. This might be an external attack, such as an intruder breaking into a financial system and issuing themselves checks, or it might be an internal attack, such as an employee increasing their own salary in the payroll system.

Following the principle of *least privilege* is the best way to protect against integrity attacks. Organizations should carefully consider the permissions that each employee needs to perform their job and then limit employees to the smallest set of permissions possible.

Impersonation

In an *impersonation* attack, the attacker pretends to be someone other than who they actually are. They might impersonate a manager, executive, or IT technician in order to convince someone to change data in a system. This is an extension of the social engineering attacks mentioned earlier, and the best defense against these attacks is strong user education.

Man-in-the-Middle Attacks

Sometimes impersonation attacks are electronic. In a *man-in-the-middle (MitM) attack*, the attacker intercepts network traffic as a user is logging into a system and pretends to be that system. They then sit in the middle of the communication, relaying information between the user and the system while they monitor everything that is occurring. In this type of attack, the attacker might be able to steal a user's password and use it later to log in to the system themselves.

Replay Attacks

In a *replay attack*, the attacker doesn't get in the middle of the communication but finds a way to observe a legitimate user logging into a system. They then capture the information used to log in to the system and later replay it on the network to gain access themselves.

The best defense against both replay and MitM attacks is the use of encryption to protect communications. For example, web traffic might use the Transport Layer Security (TLS) protocol to prevent an eavesdropper from observing network traffic. You'll learn more about this technology in Chapter 18, "Encryption."

Availability

As a security professional, you must also understand how to apply security controls that protect the *availability* of information and systems. As the third leg of the CIA triad, availability controls ensure that information and systems remain available to authorized users when needed. They protect against disruptions to normal system operation or data availability.

Availability Risks

This chapter covers five different types of events that can disrupt the availability of systems: denial-of-service attacks, power outages, hardware failures, destruction of equipment, and service outages.

Denial-of-Service Attacks *Denial-of-service (DoS) attacks* occur when a malicious individual bombards a system with an overwhelming amount of network traffic. The idea is to simply send so many requests to a server that it is unable to answer any requests from legitimate users.

You can protect your systems against DoS attacks by using firewalls that block illegitimate requests and by partnering with your Internet service provider to block DoS attacks before they reach your network.

Power Outages Power outages can occur on a local or regional level for many different reasons. Increased demand can overwhelm the power grid; natural disasters can disrupt service; and other factors can cause power outages that disrupt access to systems.

You can protect against power outages by having redundant power sources and backup generators that supply power to your system when commercial power is not available.

Hardware Failures Hardware failures can and do occur. Servers, hard drives, network gear, and other equipment all fail occasionally and can disrupt access to information. That's an availability problem.

You can protect against hardware failures by building a system that has built-in redundancy so that if one component fails, another is ready to pick up the slack.

Destruction of Equipment Sometimes equipment is just outright destroyed. This might be the result of intentional or accidental physical damage, or it may be the result of a larger disaster, such as a fire or a hurricane.

You can protect against small-scale destruction with redundant systems. If you want to protect against larger-scale disasters, you may need to have backup data centers in remote locations or in the cloud that can keep running when your primary data center is disrupted.

Service Outages Finally, sometimes service outages occur. This might be due to programming errors, the failure of underlying equipment, or many other reasons. These outages disrupt user access to systems and information and are, therefore, an availability concern.

You can protect against service outages by building systems that are resilient in the face of errors and hardware failures.

NON-REPUDIATION

Another important focus of some security controls is providing *non-repudiation*. Repudiation is a term that means denying that something is true. Non-repudiation is a security goal that prevents someone from falsely denying that something is true.

For example, you might agree to pay someone $10,000 in exchange for a car. If you just had a handshake agreement, it might be possible for you to later repudiate your actions. You might claim that you never agreed to purchase the car or that you agreed to pay a lower price.

To solve this issue, a signed contract is used when a car is sold. Your signature on the document is the proof that you agreed to the terms, and if you later go to court, the person selling you the car can prove that you agreed by showing the judge the signed document. Physical signatures provide non-repudiation on contracts, receipts, and other paper documents.

There's also an electronic form of the physical signature. *Digital signatures* use encryption technology to provide non-repudiation for electronic documents. You'll learn more about that technology in Chapter 18.

There are other ways that you can provide non-repudiation as well. You might use biometric security controls, such as a fingerprint or facial recognition, to prove that someone was in a facility or performed an action. You might also use video surveillance for that same purpose. All of these controls enable you to prove that someone was in a particular location or performed an action, offering some degree of non-repudiation.

EXAM ESSENTIALS

- The CIA triad references the three main goals of information security: confidentiality, integrity, and availability.
- Confidentiality protects sensitive information from unauthorized access. The major threats to confidentiality include snooping, dumpster diving, eavesdropping, wiretapping, and social engineering.
- Integrity protects information and systems from unauthorized modification. The major threats to integrity include the unauthorized modification of information, impersonation attacks, man-in-the-middle attacks, and replay attacks.
- Availability ensures that authorized users have access to information when they need it. The major threats to availability include denial-of-service attacks, power outages, hardware failures, destruction of equipment, and service outages.
- Non-repudiation uses technical measures to ensure that a user is not able to later deny that they took some action.

Practice Question 1

Which one of the following security risks would most likely be considered an availability issue?

A. Replay attack
B. Power outage
C. Social engineering
D. Snooping

Practice Question 2

What are the three major objectives of cybersecurity programs?

A. Confidentiality, integrity, and availability
B. Confidentiality, integrity, and authorization
C. Confidentiality, infrastructure, and authorization
D. Communications, infrastructure, and authorization

Practice Question 1 Explanation

Availability issues affect the ability of authorized users to gain access to information, systems, or other resources that they need. All of the issues listed here are cybersecurity risks that you need to be aware of when you take the CC exam, but only power outages are classified as an availability risk. This is because a power outage can easily disrupt access to systems and information by causing those systems to be offline.

Replay attacks allow an unauthorized individual to impersonate a legitimate user and are primarily considered integrity risks.

Social engineering and snooping attacks may allow an attacker to gain access to sensitive information and are primarily considered confidentiality risks.

Correct Answer: B. Power outage

Practice Question 2 Explanation

The three major objectives of any cybersecurity program are protecting the confidentiality, integrity, and availability of systems and information.

Confidentiality ensures that only authorized individuals have access to information and resources. Integrity protects information from unauthorized changes. Availability ensures that information and systems are available for authorized use.

Correct Answer: A. Confidentiality, integrity, and availability