

# Secure design

Hi, welcome back! Previously, we discussed frameworks and controls in general. In this video, you'll learn about specific frameworks and controls that organizations can voluntarily use to minimize risks to their data and to protect users. Let's get started!

The CIA triad is a foundational model that helps inform how organizations consider risk when setting up systems and security policies. CIA stands for confidentiality, integrity, and availability.

Confidentiality means that only authorized users can access specific assets or data. For example, strict access controls that define who should and should not have access to data, must be put in place to ensure confidential data remains safe.

Integrity means the data is correct, authentic, and reliable. To maintain integrity, security professionals can use a form of data protection like encryption to safeguard data from being tampered with.

Availability means data is accessible to those who are authorized to access it. As an example, a director may have more access to certain data than a department manager because directors usually oversee more employees.

Let's define a term that came up during our discussion of the CIA triad: asset. An asset is an item perceived as having value to an organization. And value is determined by the cost associated with the asset in question. For example, an application that stores sensitive data, such as social security numbers or bank accounts, is a valuable asset to an organization. It carries more risk and therefore requires tighter security controls in comparison to a website that shares publicly available news content.

As you may remember, earlier in the course, we discussed frameworks and controls in general. Now, we'll discuss a specific framework developed by the U.S.-based National Institute of Standards and Technology: the Cybersecurity Framework, also referred to as the NIST CSF. The NIST Cybersecurity Framework is a voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity risk. It's important to become familiar with this framework because security teams use it as a baseline to manage short and long-term risk.

Managing and mitigating risks and protecting an organization's assets from threat actors are key goals for security professionals. Understanding the different motives a threat actor may have, alongside identifying your organization's most valuable assets is important.

Some of the most dangerous threat actors to consider are disgruntled employees. They are the most dangerous because they often have access to sensitive information and know where to find it. In order to reduce this type of risk, security professionals would use the principle of availability, as well as organizational guidelines based on frameworks to ensure staff members can only access the data they need to perform their jobs.

Threat actors originate from all across the globe, and a diverse workforce of security professionals helps organizations identify attackers' intentions. A variety of perspectives can assist organizations in understanding and mitigating the impact of malicious activity.

That concludes our introduction to the CIA triad and NIST CSF framework, which are used to develop processes to secure organizations and the people they serve.

You may be asked in an interview if you know about security frameworks and principles. Or you may be asked to explain how they're used to secure organizational assets. In either case, throughout this program, you'll have multiple opportunities to learn more about them and apply what we've discussed to real-world situations.

Coming up, we'll discuss the ethics of security. See you soon!

---

Revision #1

Created 1 June 2023 18:34:00 by naruzkurai

Updated 1 June 2023 18:37:03 by naruzkurai