Explore the CISSP security domains, Part 1

Welcome back! You might remember from course one that there are eight security domains, or categories, identified by CISSP. Security teams use them to organize daily tasks and identify gaps in security that could cause negative consequences for an organization, and to establish their security posture. Security posture refers to an organization's ability to manage its defense of critical assets and data and react to change.

In this video, we'll discuss the focus of the first four domains: security and risk management, asset security, security architecture and engineering, and communication and network security.

The first domain is security and risk management. There are several areas of focus for this domain: defining security goals and objectives, risk mitigation, compliance, business continuity, and legal regulations. Let's discuss each area of focus in more detail.

By defining security goals and objectives, organizations can reduce risks to critical assets and data like PII, or personally identifiable information. Risk mitigation means having the right procedures and rules in place to quickly reduce the impact of a risk like a breach. Compliance is the primary method used to develop an organization's internal security policies, regulatory requirements, and independent standards. Business continuity relates to an organization's ability to maintain their everyday productivity by establishing risk disaster recovery plans.

And finally, while laws related to security and risk management are different worldwide, the overall goals are similar. As a security professional, this means following rules and expectations for ethical behavior to minimize negligence, abuse, or fraud.

The next domain is asset security. The asset security domain is focused on securing digital and physical assets. It's also related to the storage, maintenance, retention, and destruction of data. This means that assets such as PII or SPII should be securely handled and protected, whether stored on a computer, transferred over a network like the internet, or even physically collected. Organizations also need to have policies and procedures that ensure data is properly stored, maintained, retained, and destroyed. Knowing what data you have and who has access to it is necessary for having a strong security posture that mitigates risk to critical assets and data.

Previously, we provided a few examples that touched on the disposal of data. For example, an organization might have you, as a security analyst, oversee the destruction of hard drives to make sure that they're properly disposed off. This ensures that private data stored on those drives can't be accessed by threat actors.

The third domain is security architecture and engineering. This domain is focused on optimizing data security by ensuring effective tools, systems, and processes are in place to protect an organization's assets and data. One of the core concepts of secure design architecture is shared responsibility. Shared responsibility means that all individuals within an organization take an active role in lowering risk and maintaining both physical and virtual security. By having policies that encourage users to recognize and report security concerns, many issues can be handled quickly and effectively.

The fourth domain is communication and network security, which is mainly focused on managing and securing physical networks and wireless communications. Secure networks keep an organization's data and communications safe whether on-site, or in the cloud, or when connecting to services remotely.

For example, employees working remotely in public spaces need to be protected from vulnerabilities that can occur when they use insecure bluetooth connections or public wifi hotspots. By having security team members remove access to those types of communication channels at the organizational level, employees may be discouraged from practicing insecure behavior that could be exploited by threat actors.

Now that we've reviewed the focus of our first four domains, let's discuss the last four domains. (Required)
en

Revision #1
Created 3 June 2023 05:03:39 by naruzkurai
Updated 3 June 2023 05:04:15 by naruzkurai