Common classification requirements

Asset management is the process of tracking assets and the risks that affect them. The idea behind this process is simple: you can only protect what you know you have.

Previously, you learned that identifying, tracking, and classifying assets are all important parts of asset management. In this reading, you'll learn more about the purpose and benefits of asset classification, including common classification levels.

Why asset management matters

Keeping assets safe requires a workable system that helps businesses operate smoothly. Setting these systems up requires having detailed knowledge of the assets in an environment. For example, a bank needs to have money available each day to serve its customers. Equipment, devices, and processes need to be in place to ensure that money is available and secure from unauthorized access.

Organizations protect a variety of different assets. Some examples might include:

- Digital assets such as customer data or financial records.

- Information systems that process data, like networks or software.

- Physical assets which can include facilities, equipment, or supplies.

- Intangible assets such as brand reputation or intellectual property.

Regardless of its type, every asset should be classified and accounted for. As you may recall, **asset classification** is the practice of labeling assets based on sensitivity and importance to an organization. Determining each of those two factors varies, but the sensitivity and importance of an asset typically requires knowing the following:

- What you have

- Where it is

- Who owns it, and

- How important it is

An organization that classifies its assets does so based on these characteristics. Doing so helps them determine the sensitivity and value of an asset.

Common asset classifications

Asset classification helps organizations implement an effective risk management strategy. It also helps them prioritize security resources, reduce IT costs, and stay in compliance with legal regulations.

The most common classification scheme is: restricted, confidential, internal-only, and public.

- **Restricted** is the highest level. This category is reserved for incredibly sensitive assets, like need-to-know information.

- **Confidential** refers to assets whose disclosure may lead to a significant negative impact on an organization.

- **Internal-only** describes assets that are available to employees and business partners.

- **Public** is the lowest level of classification. These assets have no negative consequences to the organization if they're released.

How this scheme is applied depends greatly on the characteristics of an asset. It might surprise you to learn that identifying an asset's owner is sometimes the most complicated characteristic to determine.

Challenges of classifying information

Identifying the owner of certain assets is straightforward, like the owner of a building. Other types of assets can be trickier to identify. This is especially true when it comes to information.

For example, a business might issue a laptop to one of its employees to allow them to work remotely. You might assume the business is the asset owner in this situation. But, what if the employee uses the laptop for personal matters, like storing their photos?

Ownership is just one characteristic that makes classifying information a challenge. Another concern is that information can have multiple classification values at the same time. For example, consider a letter addressed to you in the mail. The letter contains some public information that's okay to share, like your name. It also contains fairly confidential pieces of information that you'd rather only be available to certain people, like your address. You'll learn more about how these challenges are addressed as you continue through the program.

Key takeaways

Every business is different. Each business will have specific requirements to address when devising their security strategy. Knowing why and how businesses classify their assets is an important skill to have as a security professional. Information is one of the most important assets in the world. As a cybersecurity professional, you will be closely involved with protecting information from damage, disclosure, and misuse. Recognizing the challenges that businesses face classifying this type of asset is a key to helping them solve their security needs.

Mark as completed

👍 **Like**   👎 **Dislike**   🚩 **Report an issue**