**Risk management**

A primary goal of organizations is to protect assets. An **asset** is an item perceived as having value to an organization. Assets can be digital or physical. Examples of digital assets include the personal information of employees, clients, or vendors, such as:

* Social Security Numbers (SSNs), or unique national identification numbers assigned to individuals
* Dates of birth
* Bank account numbers
* Mailing addresses

Examples of physical assets include:

* Payment kiosks
* Servers
* Desktop computers
* Office spaces

Some common strategies used to manage risks include:

* **Acceptance**: Accepting a risk to avoid disrupting business continuity
* **Avoidance**: Creating a plan to avoid the risk altogether
* **Transference**: Transferring risk to a third party to manage
* **Mitigation**: Lessening the impact of a known risk

Additionally, organizations implement risk management processes based on widely accepted frameworks to help protect digital and physical assets from various threats, risks, and vulnerabilities. Examples of frameworks commonly used in the cybersecurity industry include the National Institute of Standards and Technology Risk Management Framework ([NIST RMF](https://csrc.nist.gov/projects/risk-management/about-rmf)) and Health Information Trust Alliance ([HITRUST](https://hitrustalliance.net/product-tool/hitrust-csf/?utm_term=&utm_campaign=HITRUST_i1_PaidSearch&utm_source=adwords&utm_medium=ppc&hsa_acc=2724012343&hsa_cam=16641331914&hsa_grp=136906352837&hsa_ad=598980848547&hsa_src=g&hsa_tgt=dsa-1659695676388&hsa_kw=&hsa_mt=&hsa_net=adwords&hsa_ver=3&gclid=Cj0KCQiAorKfBhC0ARIsAHDzsluRN5tSpCQal-rYnZLo2wUNppQdUHUba82LMX3JMGOoRPEJ6wG6-LgaAryYEALw_wcB)).

Following are some common types of threats, risks, and vulnerabilities you’ll help organizations manage as a security professional.

**Today’s most common threats, risks, and vulnerabilities**

**Threats**

A **threat** is any circumstance or event that can negatively impact assets. As an entry-level security analyst, your job is to help defend the organization’s assets from inside and outside threats. Therefore, understanding common types of threats is important to an analyst’s daily work. As a reminder, common threats include:

* **Insider threats:** Staff members or vendorsabuse their authorized access to obtain data that may harm an organization.
* **Advanced persistent threats (APTs):** A threat actor maintains unauthorized access to a system for an extended period of time.

**Risks**

A **risk** is anything that can impact the confidentiality, integrity, or availability of an asset. A basic formula for determining the level of risk is that risk equals the likelihood of a threat. One way to think about this is that a risk is being late to work and threats are traffic, an accident, a flat tire, etc.

There are different factors that can affect the likelihood of a risk to an organization’s assets, including:

* **External risk:** Anything outside the organization that has the potential to harm organizational assets, such as threat actors attempting to gain access to private information
* **Internal risk:** A current or former employee, vendor, or trusted partner who poses a security risk
* **Legacy systems:** Old systems that might not be accounted for or updated, but can still impact assets, such as workstations or old mainframe systems. For example, an organization might have an old vending machine that takes credit card payments or a workstation that is still connected to the legacy accounting system.
* **Multiparty risk:** Outsourcing work to third-party vendors can give them access to intellectual property, such as trade secrets, software designs, and inventions.
* **Software compliance/licensing:** Software that is not updated or in compliance, or patches that are not installed in a timely manner