Common threats

Threat domains

With organizations facing an ever-growing number of cyber threats, it is critical that they have robust security solutions in place.

But in order to protect themselves, organizations first need to know what vulnerabilities exist within their threat domains.

A ‘threat domain’ is considered to be **an area of control, authority or protection that attackers can exploit to gain access to a system**

Attackers can exploit systems within a domain through:

- **Direct, physical access to systems and networks**

- **wireless networking that extends beyond an organization’s boundaries**

- **bluetooth or near-field communication (NFC) devices**

- **malicious email attachments**

- **less secure elements within an organization’s supply chain**

- **an organization’s social media accounts**

- **removable media such as flash drives**

- **cloud-based applications**

Types of cyber threats

**Cyber threats can be classified into different categories.**

This allows organizations to access the likelihood of a threat occurring and understand the monetary impact of a threat so that they can prioritize their security efforts

software attacks

- **successful denial-of-service (DoS attack)** - **a computer virus**

Software errors

- **software bug**

- an **application going offline**

- a **cross-site script or illegal file server share**

Sabotage

- **authorized user successfully penatrating and compromising an organization’s primary database**

- the **defacement of an organization’s website**

Human error

- **inadvertent data entry errors**

- a **firewall misconfiguration**

Theft

- **laptops or equipment being stolen from an unlocked room**

Hardware failures

- **hard drive crashes**

Utility interruption

- **electrical power outages**

- **water damage resulting from sprinkler failure**

Natural disasters

- **severe storms**

- **earthquakes**

- **floods**

- **fire**

Internal vs external threats

Threats can originate from both within and outside of an organization.

Internal threats

Are usually carried out by current or former employees and contract partners

Who **accidentally or intentionally mishandle confidential data or threaten the operations of servers or network**

External threats

Typically stems from amateur or skilled attackers who can **exploit vulnerabilities in network devices or can use social engineering techniques to gain access to an organization’s internal resources**

