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.

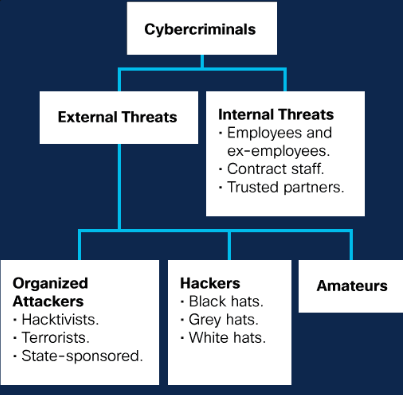
Internal threats

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**



User threats and vulnerabilities

A user domain  
 **Includes anyone with access to an organization’s information system**, including employees, customers and contract partners.

**Users are often considered to be the weakest link in information security systems, posing a significant threat to the confidentiality, integrity, and availability of an organization’s data**.

No awareness of security

**Users must be aware of and understand an organization’s sensitive data, security policies and procedures, technologies and countermeasures that are implemented in order to protect information and information systems**.

Poorly enforced security policies

All **users must be aware of and understand an organization’s security policies**, **as well as the consequences of non-compliance**.

Data theft

**Data stolen** by users **can pose a significant financial threat to organizations**, **both in terms** of the resulting dmg to their reputation and/or the legal liability associated with the disclosure of sensitive info.

Unauthorized downloads and media

**Many network and devices infections and attacks can be traced back to users** who have downloaded unauthorized emails, photos, music, games, apps and videos to their computers, networks or storage devices, or used unauthorized media such as external hard disks and USB drivers.

Unauthorized virtual private networks (VPNs)

**VPNs can hide the theft of unauthorized information** because the encryption normally used to protect confidentiality can stop a network administrator from tracking data transmission.

Unauthorized websites

Accessing unauthorized websites **can pose a risk to a user’s data and devices, as well as the organization itself.**

Often, **these websites prompt users to download scripts or plugins that contain malicious code or adware**. **Some** of these sites can **even take over user devices like cameras and applications**.

Destruction of systems, applications or data

**The accidental or deliberate destruction or sabotage of systems, applications and data poses a serious risk to all organizations.**

**Activists, disgruntled employees or industry competitors** attempt to delete data and destroy or misconfigure devices, to make organizational data and information systems unavailable.

Threats to devices

- any **devices left powered on and unattended pose risk** of **someone gaining unauthorized access** to network resources.

- **downloading** files, photos, music or videos **from unreliable sources could lead** to the  **execution of malicious code on devices**.

- **cybercriminals often exploit security vulnerabilities within software installed on an organization’s devices to launch an attack**.

- an **organization’s information security teams must try to keep up to date** with the daily discovery of new viruses, worms and other malware that pose a threat to their devices.

- **users who insert unauthorized USB drive**s, CDs or DVDs **run the risk of introducing   
 malware, or compromising data stored on their device**.

- **Policies are in place to protect an organization’s IT infrastructure**. A **user can face** serious  **consequences for purposefully violating such policies**.

- **using outdated hardware or software** makes an organization’s **systems and data more vulnerable to attacks**.

Threats to the local area network

Local area network (LAN)

Is collection of devices, typically in the same geographic area, connected by cables or airwaver

**Because users can access an organization’s systems, applications and data from the LAN domain, it is critical that it has strong security and stringent access controls.**

Examples of threats to the LAN includes:

**- unauthorized access to wiring closets, data centers and computer rooms**

**- unauthorized acces to systems, applications and data**

**- network operating system or software vulnerabilities and updates**

**- rogue users gaining unauthorized access to wireless networks**

**- exploits of data in transit**

**- having LAN servers with different hardware or operating sys. Makes managing and troubleshooting them more difficult**

**- unauthorized network probing and port scanning**

**- misconfigured firewalls**

Threats to the private cloud

f