Cybersecurity

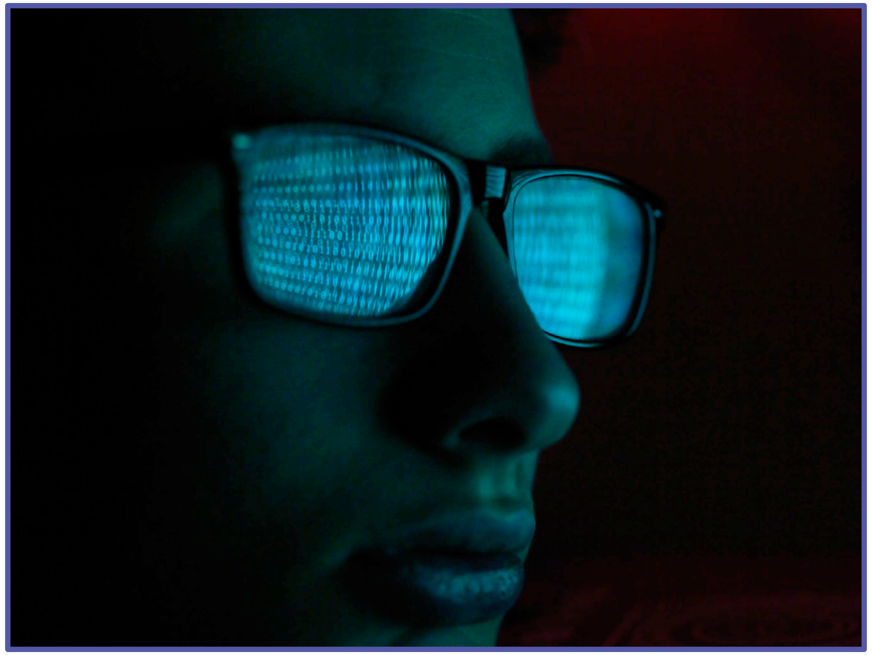
2.1.1 - Threat Actors

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA

CYBER.ORG
THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER

Threat Actors

- Groups of people who pose a threat to the security of software, data, or an organization’s well being.
- Driven by a range of motivations
- Characterized based on their level of skill and potential ability to cause damage to a business, organization, or government.



Types of Threat Actors

- Script Kiddies
- Hacktivists
- Organized criminals
- Nation states/APT
- Insider threats
- Competitors
- Hackers
- Shadow IT

Script Kiddies

- Unskilled attackers
- Least sophisticated group with little expertise or knowledge
- Relies on tools created by others
- Interested in making a name for themselves, vandalizing sites, or causing chaos.
- The term “Script Kiddie” is usually a negative label used by more sophisticated hackers to belittle one another or dismiss someone for not being knowledgeable.

Hacktivist

- Medium skilled professionals who perform exploits and attacks for a cause.
- Driven by their political, commercial, or economic message.
- End goal is to spread their message to a wider audience to raise awareness for their cause.

Organized Crime

- Organized criminals, or criminal syndicates, use exploits to continue their organized crime business
- Sell data on the dark web, hack into devices with the intent to spy, sell trade secrets
- Fueled by money and the desire to gain power to continue their influence.

Nation States and APT

- Also known as state actors or advanced persistent threats.
- Very advanced government or military organizations.
- Argued that Stuxnet malware was carried out by a nation state because of its sophistication.

Insider Threats

- Work within an organization to expose business secrets and data
- Usually carry out low-level attacks
- May act out of vengeance or spite due to an event that happened to them at work that they feel is unfair.

Competition

- Competitors are any business or organization that operates within the same domain as another business.
- Netflix and Hulu or Facebook and Twitter
- Competitors may attempt to steal secrets to undermine profits and drive customers to their businesses.

Hacker

- Authorized hacker (formerly known as white hat)
  - Find vulnerabilities and exploits in a system with the intent to patch them.
- Unauthorized hackers (formerly known as black hat)
  - Malicious users who intend to cause damage and harm to their targets.
- Semi-authorized hackers (formerly known as grey hat)
  - Breaking the law but usually not with malicious purposes.

Shadow IT

- Part of larger organizations that do not follow the IT department rules and attempt to work around them.
- Find a way to work around security utilize locked features without the IT Departments consent

Attributes of Actors

- Internal – Trusted insiders that have permission to be in the organizations network.
- External – Do not have access or special privileges to the network.
- Resources and Funding – How well the threat actor can support their attack.
- Capability – One of the most important factors to determine if a threat actor’s attack is successful.
- Level of sophistication – Highly sophisticated threat actors are more likely to be successful

Motivations

- Data exfiltration
- Espionage
- Service disruptions
- Blackmail
- Financial gain
- Philosophical/political beliefs
- Identify and fix weaknesses
- Revenge