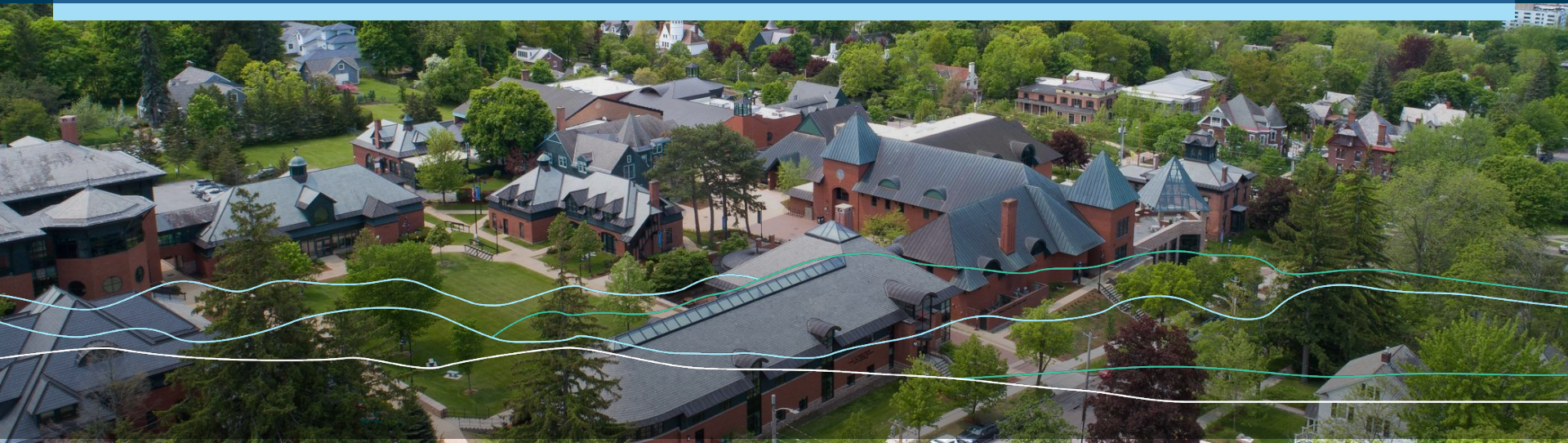
CHAMPLAIN COLLEGE

Mod 3 – Risks, Adversaries, and Threats

SEC-110



Threats, Attacks, and Vulnerabilities

What's the difference?

- **Threat:** a potential for harm or damage by a circumstance, event, or action

- **Attack:** a deliberate attempt to exploit vulnerabilities with malicious intent

- **Vulnerability:** a weakness or flaw in a system, network, or software that can be exploited by an attacker to compromise its security

The Home Security Analogy

Threat: Burglar, natural disaster, forgetful homeowner

Vulnerability: Unlocked door, broken window, weak lock

Attack: A burglar breaks in through the unlocked door

Threat:
Something that can damage or destroy an asset

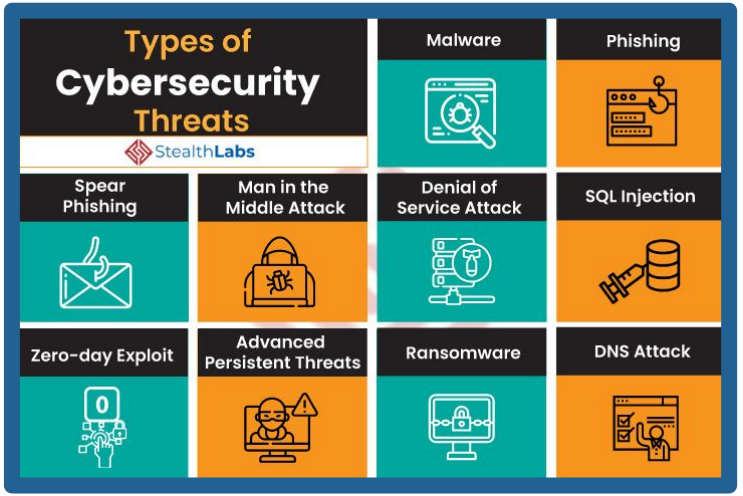
Vulnerability:
A weakness or gap in your protection

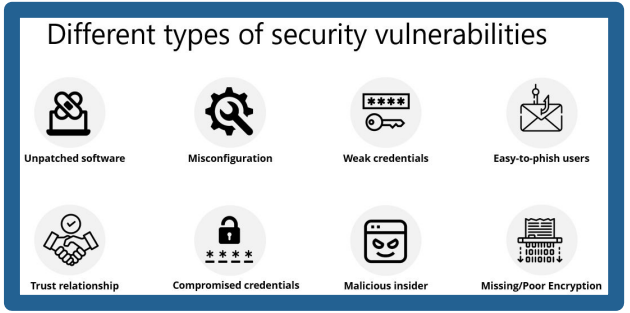
In The Digital World

Threat: Hackers, malware, your little sibling on your computer

Vulnerability: Weak password, unpatched software, clicking random links

Attack: Hackers steal your data through a weak password





Types of Threats

Natural Disasters: earthquakes, floods, hurricanes, tornadoes, wildfires, server storms, pandemics

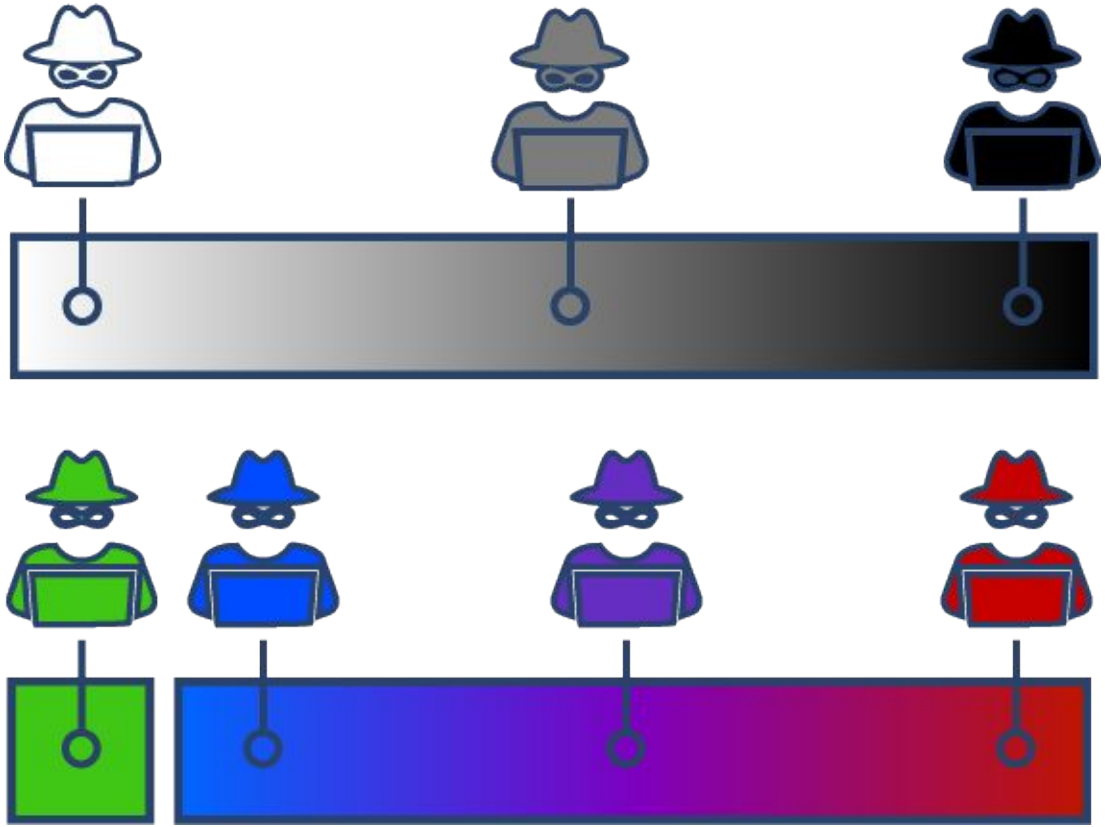
Human Error: accidental deletion of files, misconfiguring systems or networks, losing devices, sending sensitive info to the wrong person, poor password practices, failure to install updates

Intentional Bad Actors: external hackers, insider threats, social engineering attacks, theft of devices or credentials, corporate espionage, DoS attacks

Adversary Spectrum

- **White Hat Hackers:** cybersecurity experts who are hired to recognize and report weaknesses in computer systems and networks (aka ethical hackers).
- **Hacktivists:** an individual who gains unauthorized access to computer files or networks to facilitate social or political ends.
- **Grey Hat Hackers:** work in between the grey areas of ethical and unethical hacking.
- **Black Hat hackers:** cybercriminals who gain unauthorized access to computer systems and networks with malicious intent.
- **Nation-States (APTs):** an advanced, prolonged cyberattack initiated by a nation state or a group acting on their behalf.

Adversary Spectrum



Blue Team: defends systems and responds to incidents (implements security measures, monitors threats, minimizes impact of attacks)

Red Team: simulates attacks to identify vulnerabilities and weaknesses

Purple Team: the bridge between the two teams, helps facilitate communication and identify areas of improvement

Green Hat Hackers: a term used to describe beginner/novice hackers

Hacktivists

Who They Are:

- Hacker + Activist
- Individuals or groups using hacking for political / social causes
- Can be ideologically driven
- Associated with groups like: Anonymous, LulzSec, and RedHack

How They Operate:

- Use cyber attacks for political statements / social causes
- Use tactics like DDos attacks, Data leaks, and social media takeovers
- Often use anonymity tools like Tor and VPNs

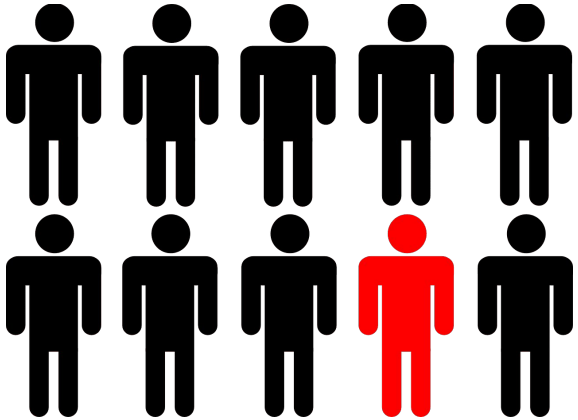
What They Want:

- Raise awareness for their cause
- Expose wrongdoing (governments, corporations)
- Promote freedom of speech
- Embarrass / disrupt targets seen as unethical

Insider vs Outsider Threats

Insider: a risk that originates from within an organization.

Outsider: a risk that originates from outside, external to an organization.



Real examples:

- In 2018, an employee at SunTrust Bank stole Personally Identifiable Information (PII) from over 1.5 million customers.
- In 2021, there was a ransomware attack on the Colonial Pipeline which led to a disruption of the pipelines operations and a shortage of fuel nationwide.

Adversary Terms

IOC: *"Indicator of Compromise"*, evidence of a data breach (ex. malware signatures, unusual net traffic patterns, etc.)

APT: *"Advanced Persistent Threat"*, a prolonged and targeted cyber attack, usually attempting to breach a system repeatedly to reach a goal

TTP: *"Tactics, Techniques, Procedures"*, categorizes hacking methods and a framework to understand and defend against those methods

Persistence: a hacker makes sure they can stay inside a system when if the system restarts or security kicks them out

Adversary Terms

Privilege Escalation: a hacker begins with limited access to a system and then finds a way to gain more access and control

C2: *"Command and Control"*, describes the techniques that malicious actors use to communicate with and control compromised systems

Zero-Day: a new, never-before-seen security flaw or vulnerability that is unknown to the developers or anyone capable of mitigating the threat. Exploits to zero-day vulnerabilities are especially dangerous

Attribution: figuring out what hacker, group, or entity performed a certain cyberattack

Adversary Motives

The most common motives of adversaries are…

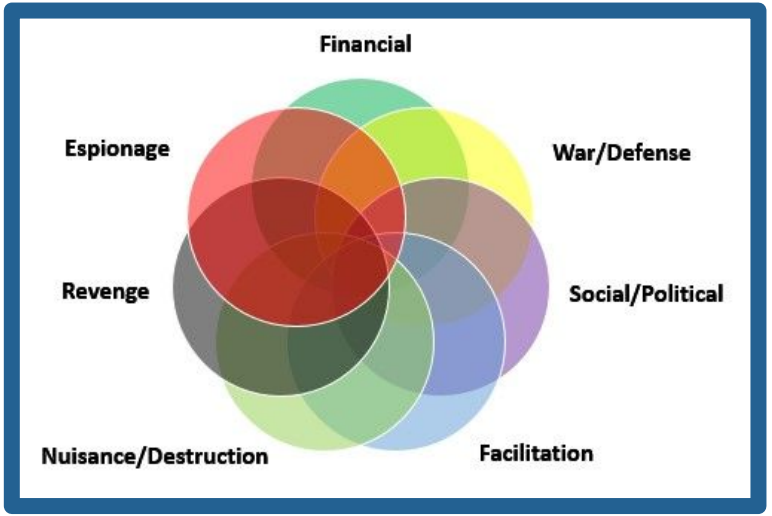
Theft: Stealing money, data, intellectual property

Disclosure: Exposing secrets, embarrassing someone

Disruption: Breaking things, causing chaos

Destruction: Permanently damaging systems or data

Subversion: Taking control, turning systems against their owners



How Adversaries Choose Targets

A hacker might choose...

Easy Targets: weak passwords, no updates

Valuable Targets: rich and/or famous

Symbolic Targets: represents something they hate

The Adversary Mindset Exercise

Think like a hacker:

- If you wanted to hack your school's system what would you try first?
- What about targeting a classmate you didn't like?
- How would you get into someone's Instagram account?

Modern Threat Landscape

Social engineering: when attackers trick people into giving up confidential information or access by pretending to be someone trustworthy.

Supply Chain Attacks: when hackers target a trusted third-party such as a software or vendor or a service provider to sneak into a bigger organization.

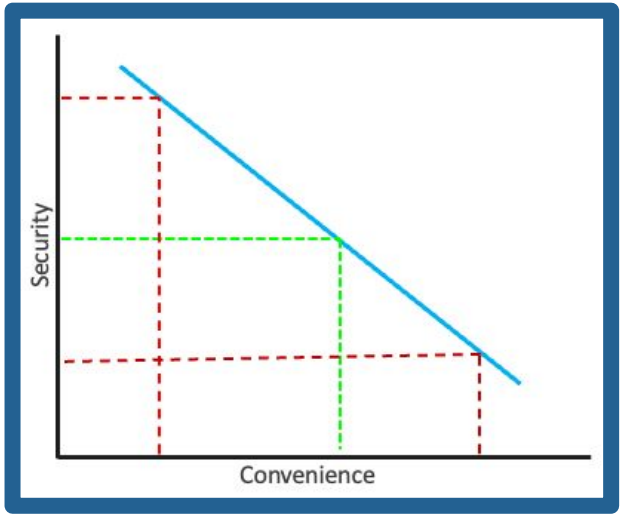
AI-Powered Attacks: cyber attacks that utilize AI to make them faster, smarter, and harder to detect.

Cryptocurrency crimes: cybercrimes where digital currencies such as Bitcoin or Ethereum are used to steal money, hide illegal activity, or scam people.

IoT exploitation: when hackers break into internet of things (IoT) devices such as smart cameras, thermostats, or cars to steal data, spy, or launch larger attacks.

The Balancing Act

Security vs Convenience



- Often, security gets skipped for speed or ease of use
  - Ex: using the same password across multiple platforms and websites because it's easier to remember
- The inverse is also true, a system that is TOO secure would be very user-unfriendly.
  - Ex: a 100-character password would be more secure, but almost impossible to remember

The Defenders Dilemma: Attacks only need to find ONE way in, defenders must protect EVERYTHING

Understanding Risk

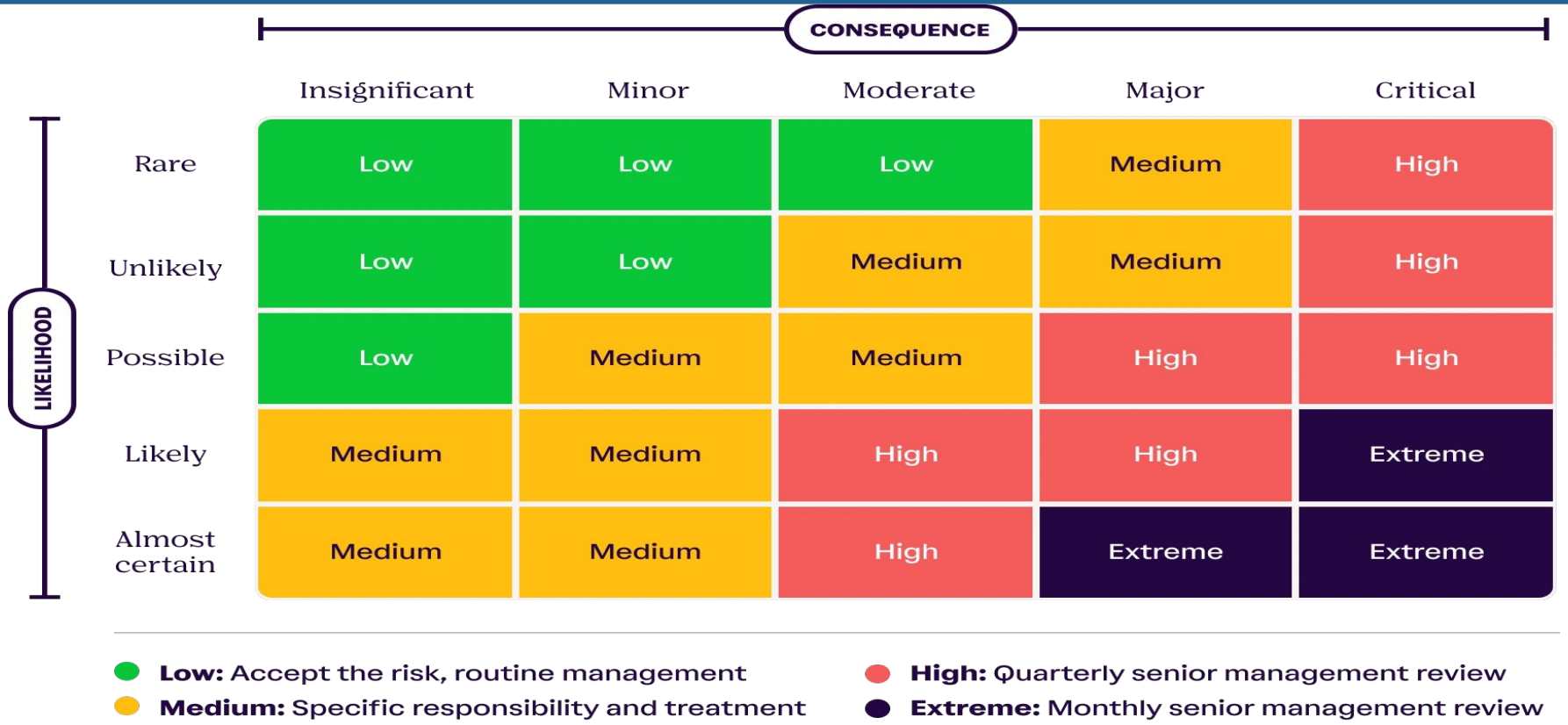
Use this simple formula to calculate risk!

Risk = How Likely (Likelihood) x How Bad (Impact)

Example:

- A company measures the risk of a phishing attack
  - **Likelihood:** 4 out of 5 (major) - employees are not trained against phishing and are likely to click on a malicious link
  - **Impact:** 5 out of 5 (critical)- a successful phish could have severe financial loss and reputational damage
  - **Risk:** 20 (extreme) - the company should definitely take steps to mitigate this risk

The Risk Matrix



Risk Assessments

What are we protecting? What could go wrong? What happens if it does? How likely is it to happen? How do we reduce that risk?

What They Are:

- Process of evaluating potential threats to systems and data
- Helps determine what could go wrong, how likely it is, and what the impact could be

Why and Where They're Used:

- Identify vulnerabilities before attackers do
- Support compliance (NIST, HIPAA, GDPR)
- Reduce the likelihood / impact of cyber incidents.

Types of Risk Assessments:

- **Vendor:** evaluates risk from third party providers
- **Hardware**: physical and virtual infrastructure
- **Application:** focus on risks in web / Mobile apps

Rate the Risk!

Rate these common activities (High/Medium/Low for both Likelihood and Impact)

- Using the same password for Instagram, email, and online shopping
- Clicking links in text messages from unknown numbers
- Sharing your location in every social media post
- Using your real birthday and hometown in online profiles
- Connecting to any available Wi-Fi network
- Posting photos of your driver's license or school ID "for fun"
- Sharing your phone number publicly online.
- Downloading apps from unofficial app stores