Security Mindset

Why Cyber Security
When you have something of value and there is a risk to it.

What is of value: data
What is the threat: criminals (they can monetize it and profit from it)

Smart Grids- computer controlled electrical grid.

Security Impact Quiz
There are two kinds of companies -- those that have been hacked and know it, and those that have been hacked and don't know it.

You have most likely patronized a company that has been hacked.

Cyber Assets at Risk

We need to develop a security mindset --
- Threat Source:
  - Cyber criminals
  - Hacktivists
  - Nation States

- Vulnerabilities and Attacks:
  - Compromises
  - Security Breach

  - Vulnerabilities are in software, networks, humans

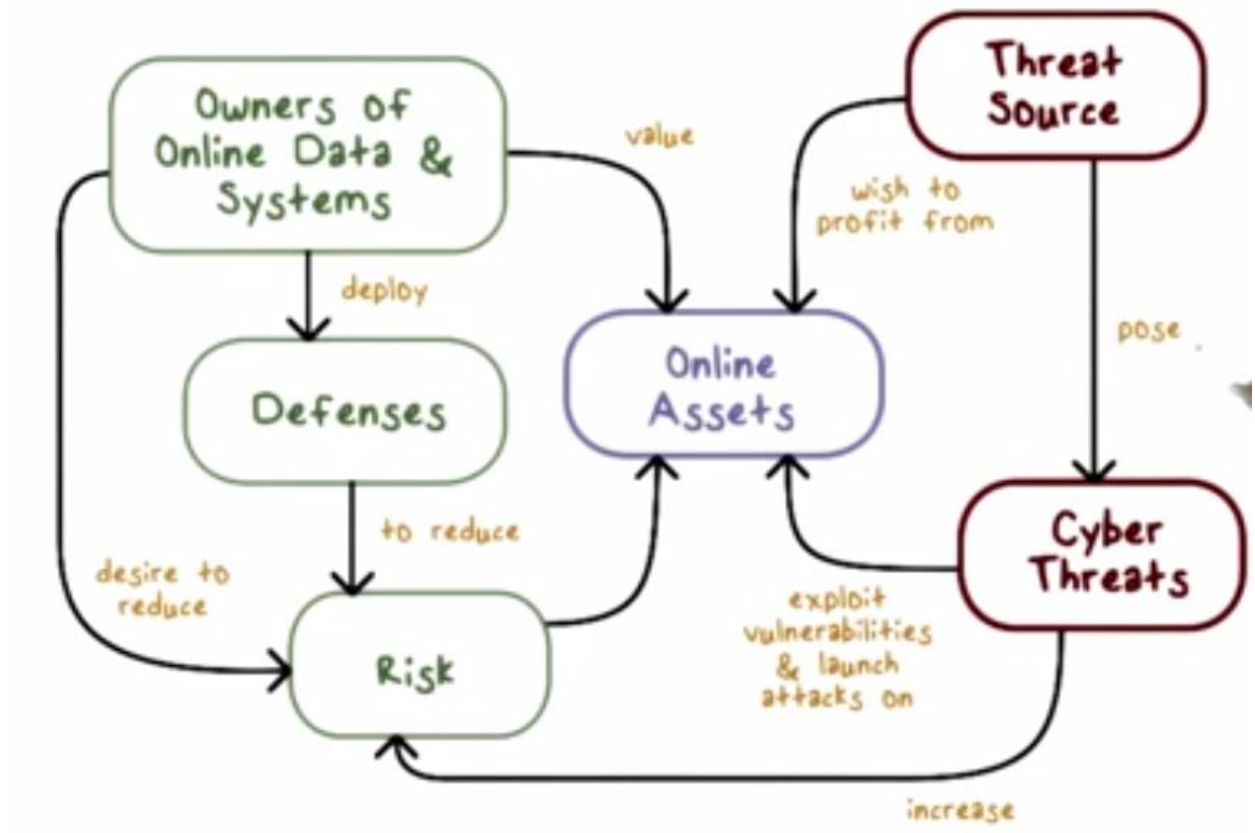
Real World Example: Target Store Breach
- What is of value - credit card data
- What is threat source - criminals
- What was vulnerability - phishing was used to obtain credentials of the network

Sony Pictures Quiz

Threat - Nation states
Goal of attack - stop release of a movie
Attack accomplishment - disclosed sensitive data

Revisiting Threats

Relationship of Threats, Vulnerabilities, Attacks, and Risk



What Should We Do in Cyber Security

Make threats go away - not really practical
Reduce vulnerabilities - will never go away
Strive to meet security requirements of sensitive info:

-**C**onfidentiality - try to achieve this
-Integrity - try to maintain
-**A**vailability - try to always try to keep services available (stop Denial of Services Attacks)

These three are called : CIA

Cyber attacks can have physical consequences - computer systems can be damaged

We need to protect data and systems

Security Requirements Quiz Solution
Data breaches violate CONFIDENTIALITY

What should the good guys do?
Prevention - keep bad guys out. We will never have 100%
Detection - detect the bad guys are in the system
Response - respond to the intrusion
Recovery and remediation - restore corrupted data and stop similar future attacks
Policy vs Mechanism - what vs how will attacks be handled

How do We Address Cyber Security

Reduce vulnerabilities: follow basic design principle for secure systems.

- Economy of mechanism - keep systems simple and small
- Fail-safe defaults - means default access is denial
- Complete mediation - no one should be able to bypass security measures
- Open Design - is good because not counting on secrecy
- Least privilege - only give users the minimum level of access that they need
- Psychological acceptability - don’t expect people to do what is inconvenient