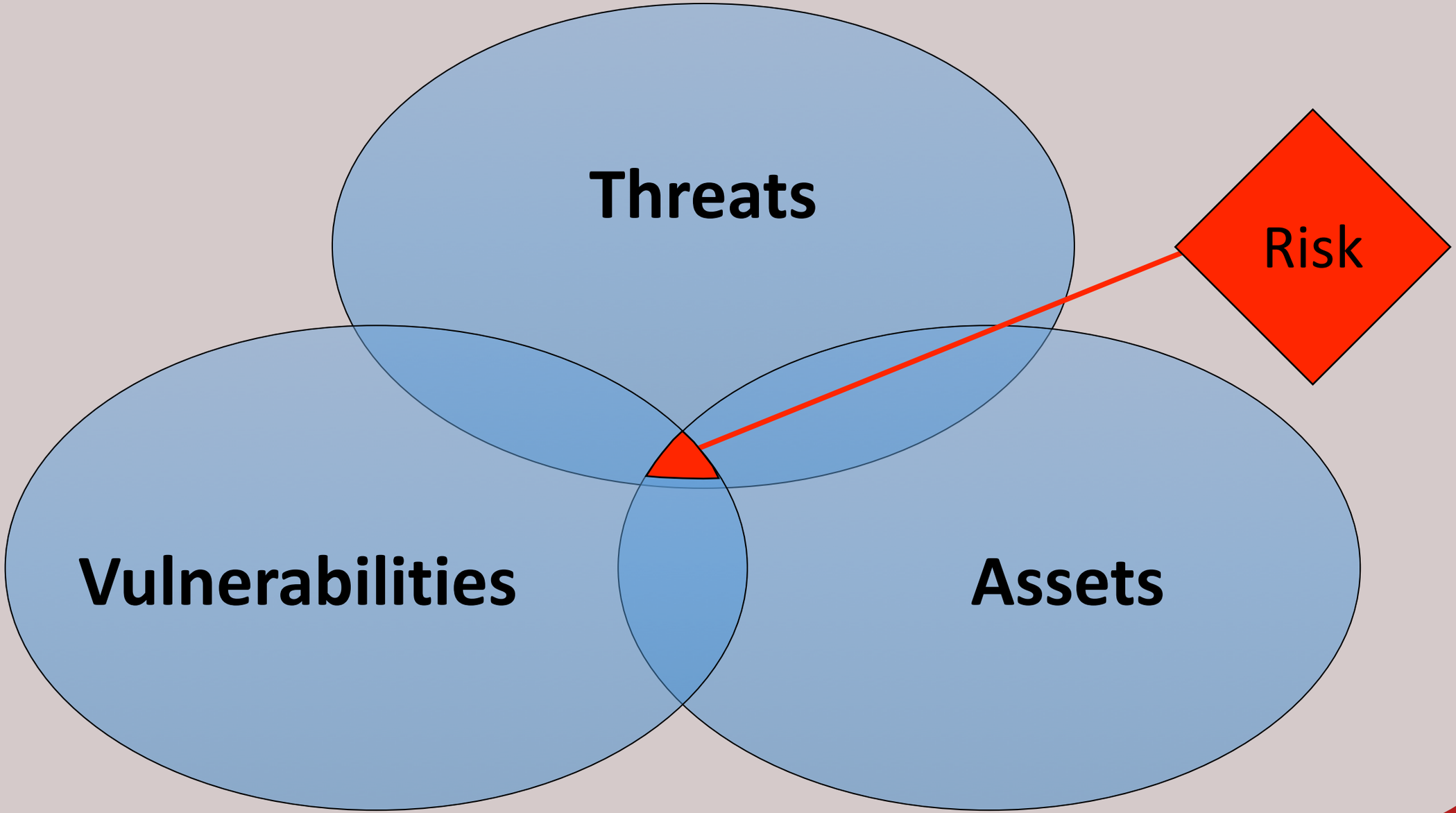
JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Risk Considerations

THREAT MANAGEMENT

WHERE RISK EXISTS...



ASSETS

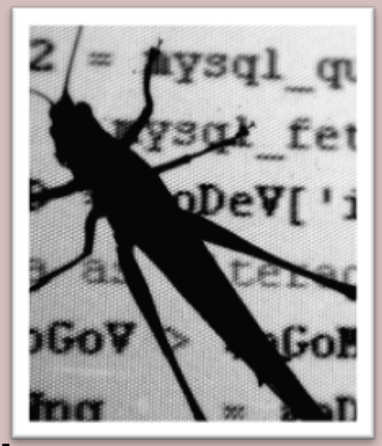
Any item that has a value to the organization

Examples:

- Information or Data
- Network Equipment
- Servers/Computers
- Software
- Personnel
- Processes

VULNERABILITY

Any weakness in the system design, implementation, software code, or lack of preventative mechanisms



Examples:

- Software bugs
- Misconfigured software
- Misconfigured network devices
- Improper physical security

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

VULNERABILITIES

- Cybersecurity professionals control vulnerabilities

- Vulnerabilities are internal factors

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

THREAT

Any condition that can cause harm, loss, damage, or compromise of an asset

Examples:

- Natural Disasters
- Cyber Attacks
- Breach of integrity of data
- Disclosure of confidential data
- Malware

THREATS

- Cybersecurity professionals cannot control threats, but they can be mitigated

- Threats are external factors

RISK

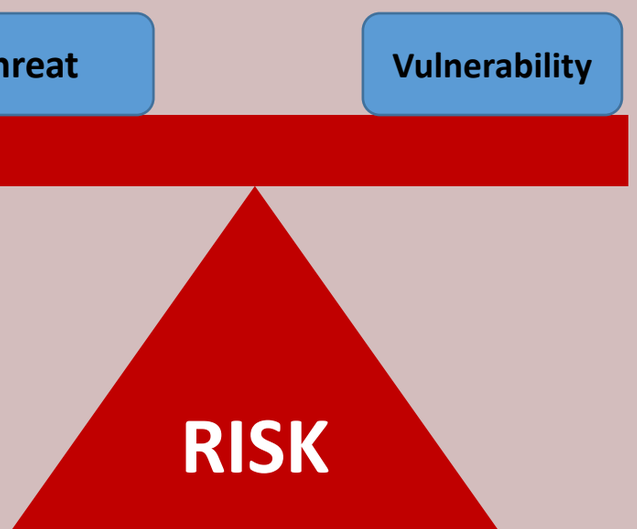
- Probability (or likelihood) of the realization of a threat

- Vulnerability without a threat equates to no risk…

RISK =

Vulnerability

X Threat



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE