Identify Vulnerabilities

THREAT MANAGEMENT

NIST SP 800-30

Step 1: Prepare for Assessment
Derived from Organizational Risk Frame

Step 2: Conduct Assessment
Expanded Task View

Identify Threat Sources and Events

Identify Vulnerabilities and Predisposing Conditions

Determine Likelihood of Occurrence

Determine Magnitude of Impact

Determine Risk

Step 3: Communicate Results

Step 4: Maintain Assessment

Source: NIST

Identify Vulnerabilities

- During the identification of threats, we generally look external to the organization, but...
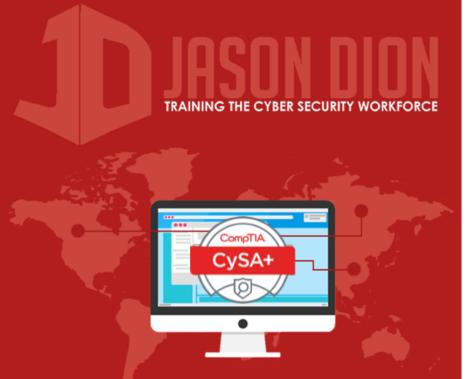
- Identifying vulnerabilities focuses on internal factors

- Our focus it to match up vulnerabilities to the threats identified

Always Remember...

- If you have a threat without a vulnerability, it isn't a risk.

  - Threat
    - Hackers are using a zero-day exploit against Windows XP systems

  - Vulnerability
    - We don't use Windows XP systems

  - Risk
    - NONE

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

CompTIA
CySA+

Always Remember...

- If you have a vulnerability without a threat, it isn't a risk.

  - Threat
    - Hackers haven't found any exploitable coding errors

  - Vulnerability
    - Unpatched operating system software

  - Risk
    - NONE

CompTIA
CySA+