JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Remediation Priority

VULNERABILITY MANAGEMENT

Remediation Priority

- Man-hours, money, equipment and other items are a limited resource

- Vulnerability Management is all about prioritization of organizational efforts

- *You can’t fix everything right away…*

How critical is the System and Information It Contains?

- Take into account confidentiality, integrity, and availability if the vulnerability was exploited

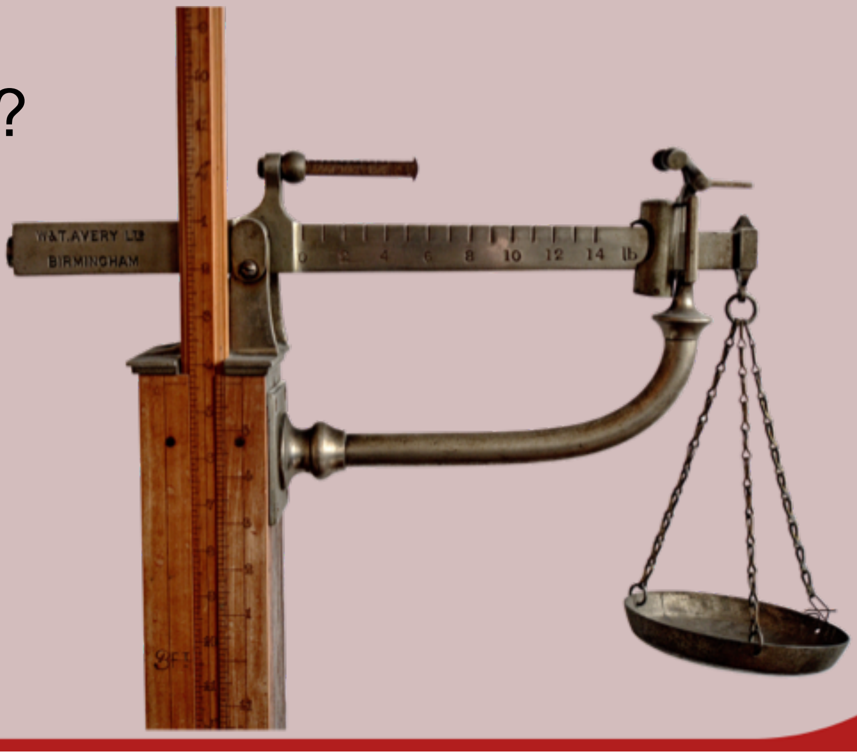
- Example:
  - If an attacker was able to breach your customer database and get all their information…
  - How bad is this?

How Difficult is it to Fix the Vulnerability?

- How much time and money will it cost to fix it?

- Example:
  - I can spend all my time and money fixing the #1 vulnerability, or I can fix vulnerabilities 2, 3, 4, & 5

  - Which should I do?



How Severe is the Vulnerability?

- Each vulnerability is given a criticality value in the Common Vulnerability Scoring System (CVSS)

- Different vulnerabilities are more severe than others

- Example:
    - Known-exploit against a software bug that allows for remote-code execution is very severe
    - Cross-site scripting vulnerability might be less severe if its on an intranet server only

How Exposed is the Server to the Vulnerability?

- External facing servers are more exposed than intranet servers
- Often, you should fix a lower external vulnerability before a higher internal one…

JASON DION

TRAINING THE CYBER SECURITY WORKFORCE