Vulnerability Management Technology and its Impact to Healthcare Organizations

Group #2: Brandon McFarlane, Michael Gonzalez, Joe Alequin, and Rashondric Evans

ISM 6575 - Security Risk Management and Organizational Cyber Resilience

Dr. Jesus Arias

Overview

- Vulnerability management technology is critical to healthcare organizations and helps safeguard the (C)onfidentiality, (I)ntegrity, and (A)vailability of information

- Vulnerability scanning and remediation both reduces attack vectors an organization faces and enhances overall security posture

- By effectively managing vulnerabilities, organizations can better protect themselves against cyber threats and maintain strong security defenses, which is often a challenges in the healthcare sector

Introduction

- A system vulnerability refers to a weakness within a system that can be exploited to gain access or perform malicious actions

- The vulnerability management and assessment process involves several key steps:
  - Plan
  - Identify
  - Assessment
  - Prioritization
  - Remediation
  - Verification
  - Reporting

Relevancy

- Protecting organizational assets is vital to maintaining the trust of customers, partners, and shareholders, and it can also save lives in a healthcare environment

- Good vulnerability management practices include regularly updating software, conducting thorough risk assessments, prioritizing vulnerabilities based on potential impact, and implementing enhanced security controls

- A proactive approach to vulnerability management involves anticipating and addressing vulnerabilities before they can be exploited, preventing potential security incidents

Framework

National Institute of Standards and Technology (NIST)

- **NIST**: Created the Cybersecurity Framework (CSF), which contains a set of information security guidelines under several key “functions”, one of which is the **Protect** function.

- Some of the various sections within the Protect function include:
  - *Access Control* - Limit access to information systems based on user roles and responsibilities
  - *Awareness & Training* - Educate employees about safe computing practices and emerging threats
  - *Data Security* - Policies to protect data at rest, in transit, and during processing
  - *Maintenance* - Regular system maintenance, including updates and patches
  - *Protective Technology* - Utilizing tools to detect and manage vulnerabilities proactively
  - *Incident Response* - Define how to prepare to quickly contain and remediate incidents that arise from exploited vulnerabilities

Framework

Other Security Frameworks:

- **ISO/IEC 27002:** Code of practice for information security controls, providing guidelines for selecting and implementing controls based on the ISO 27001 standard, including vulnerability management ones
- **CIS (Center for Internet Security)**: Developed a set of 20 critical security controls that help organizations defend against the most common cyber threats and vulnerabilities
- **COBIT (Control Objectives for Information and Related Technologies)**: Mainly used for developing, implementing, monitoring, and improving IT governance and management practices for vulnerability control
- **MITRE ATT&CK**: Provides a comprehensive knowledge base of adversary tactics and techniques based on real-world observations and uses it for vulnerability threat modeling and detection.
- **SANS Top 20**: SANS Institute provides a prioritized list of the top vulnerabilities and the best practices for mitigating them, guiding organizations to improve their security posture effectively

Technology: Discovery Tools

Vulnerability Scanners & Detection Technology:

- **Tenable Nessus:** A vulnerability management platform developed by Tenable, Inc. which scans for security vulnerabilities in networks, devices, applications, operating systems, and cloud services
- **Qualys:** A vulnerability management platform that helps organizations identify, prioritize, and remediate security vulnerabilities in their networks, systems, and applications
- **Rapid 7:** Products and services available to help businesses protect against, detect, and respond to security incidents. This platform includes tools for threat intelligence, vulnerability management, cloud security, and more
- **Microsoft Defender:** Built into Windows systems helping protect the device against viruses, ransomware, and other vulnerabilities and misconfigurations
- **CrowdStrike Falcon:** Endpoint detection and response (EDR) software that's provides real-time protection from known vulnerabilities

Technology: Threat Intelligence

Threat Intelligence Technology:

- **CISA (Cybersecurity & Infrastructure Security Agency)**: The nation's cyber and infrastructure security agency, CISA was designed not to be another government bureaucracy but something much more akin to a public/private collaborative

- **Vendor Notifications**: Communications directly from a software or system vendor alerting you as the client of an issue or vulnerability with their product that needs to be addressed

- **Other Public and Private Sources**: Online resources that provide software and system vulnerability information to the public, some as part of free services, or on a "paid subscription" model

Risk Classification

Risk

- **Risk**: The potential for harm to the organization (e.g., service disruption, data loss, etc.) were that vulnerability to be exploited by a threat actor
- Two important factors:
  - **Impact**: The effect a successful exploitation would have on the organization
  - **Probability**: Likelihood of the vulnerability being exploited

Risk Assessment

- **Predicting Impact**:
  - Can be simpler to predict given the assumption that the event has already happened
  - However, it requires input from all business stakeholders and subject-matter experts (SME)
- **Predicting Probability**:
  - Quantitative versus Qualitative approach
  - Assessor bias needs to be considered (e.g., *probability neglect*)

Risk Score

- Helps provide a holistic view of the healthcare organization's risk profile
- Can be useful in determining where to start lowering risk ("most bang for your buck")
- Your own methodology or leverage existing ones:
  - Common Vulnerability Scoring System (**CVSS**)
  - Stakeholder Specific Vulnerability Categorization (**SSVC**)
  - Common Weakness Enumeration (**CWE**)
  - **OWASP** Top 10
  - Proprietary Risk Scores (vulnerability scanners)

Response & Prioritization

- Response to Risk:
  - **Avoid:** Discard the use of technology altogether
  - **Transfer:** Shift risk to third-party
  - **Accept:** Accept the risk to the organization
  - **Mitigate (Remediate):** Fix or mitigate the issue through the implementation of controls

- Challenges:
  - In 2023 alone, ***26,447*** vulnerabilities were disclosed public
  - A generic risk score does not take into account your control environment (inherent versus residual risk)
  - You could be stuck trying to “boil the ocean”

Response & Prioritization

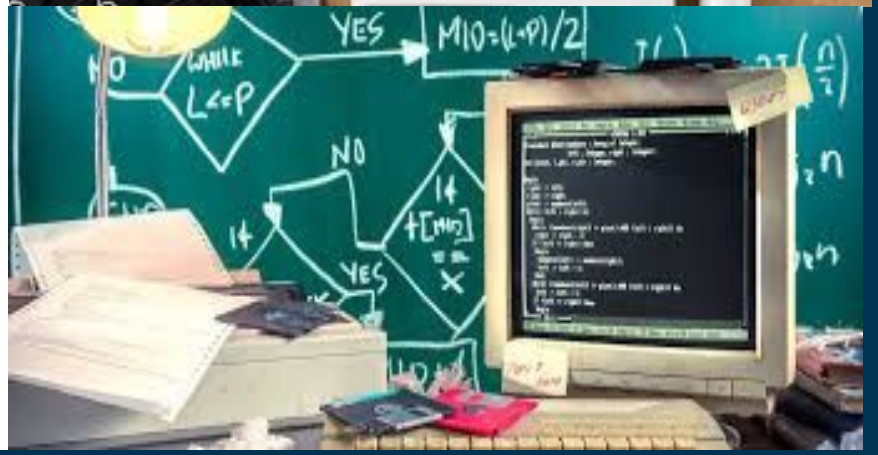
- Healthcare organizations need to consider the **residual risk score** by evaluating things like:
  - Is the affected asset an internal or external (Internet-facing) one?
  - Does the affected asset provide a critical service? Does it directly impact patient care?
  - Is the vulnerability being actively exploited in the wild right now?
  - Does exploitation require having system access or can any unauthenticated user exploit it remotely?

- With this residual risk score, you can come up with a prioritization schedule to define what gets fixed first

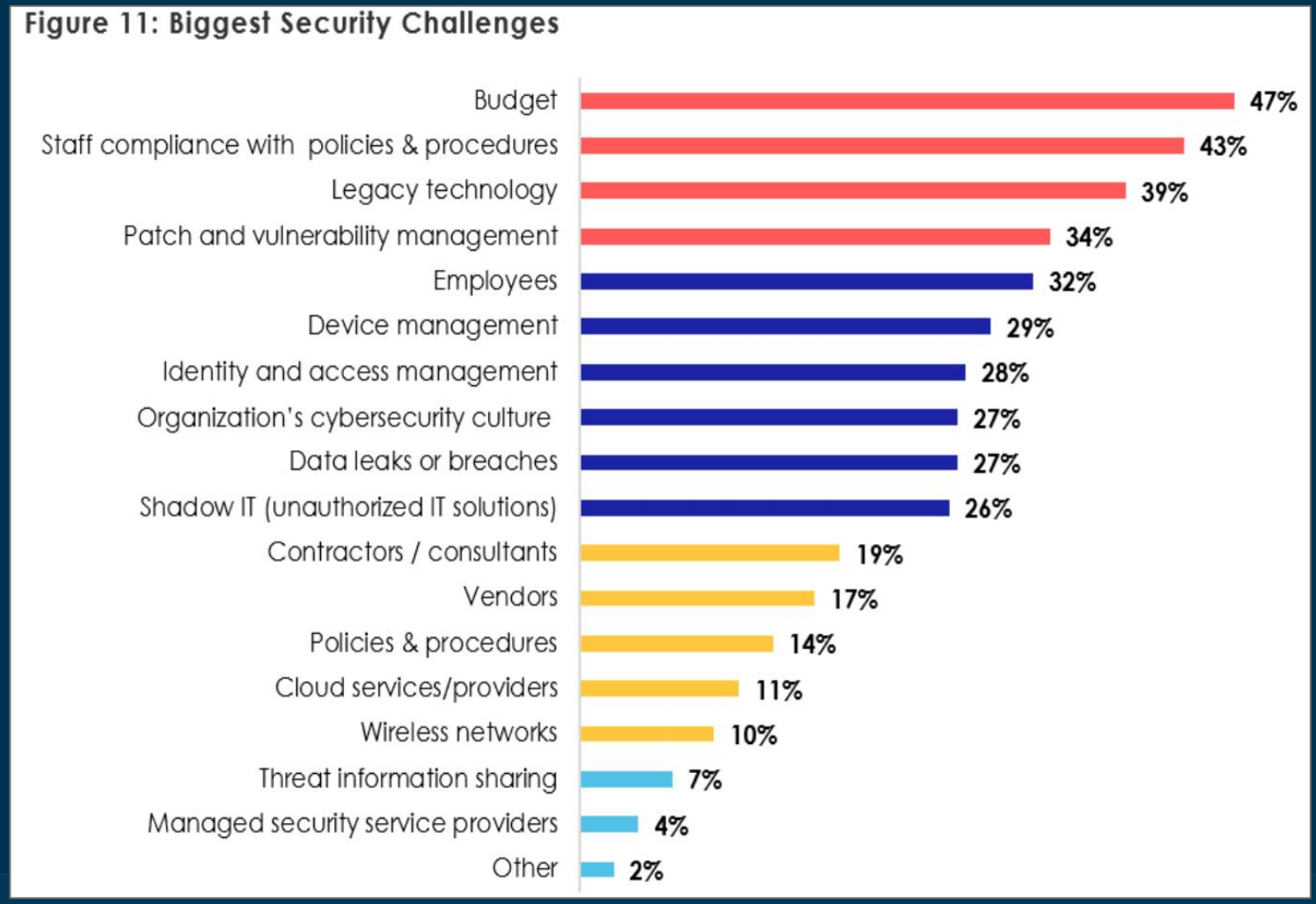
Severity	Timeline
Critical	10 days
High	30 days
Moderate	60 days
Low	90 days

Challenges

- Personnel
- Budget
- Training
- IoT
- Compliance
- Legacy Systems



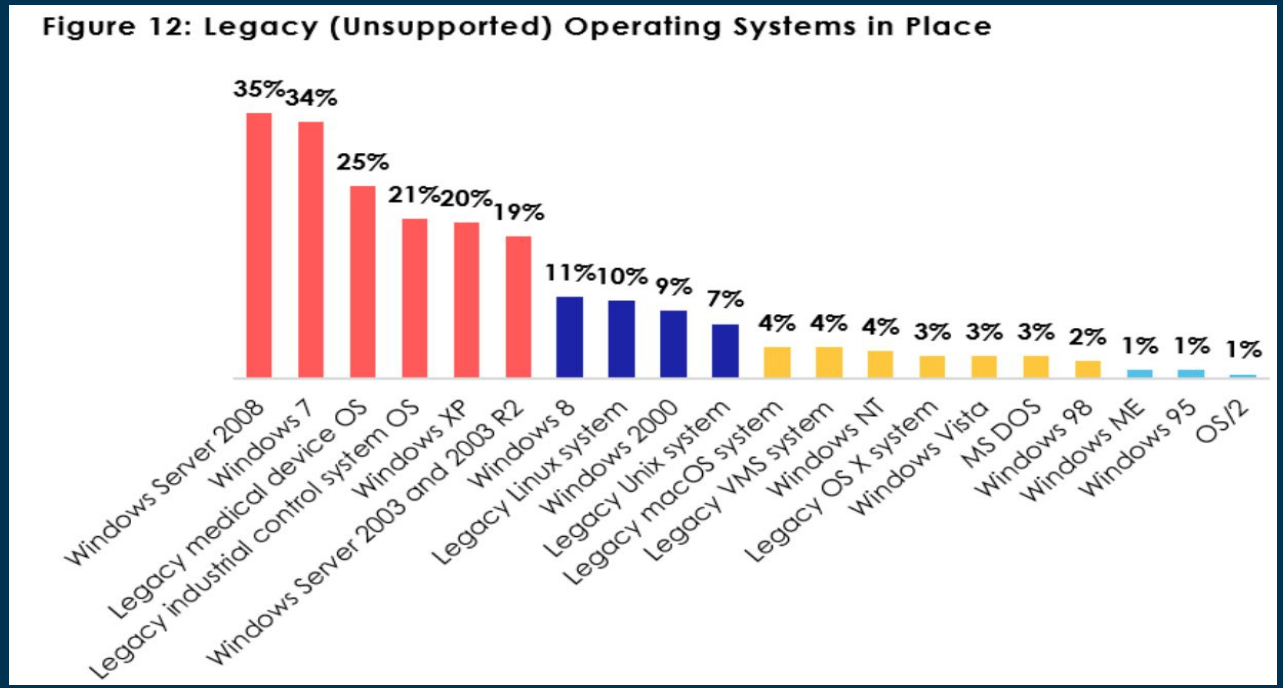
Challenges cont.



Reference: https://www.himss.org/sites/hde/files/media/file/2022/01/28/2021_himss_cybersecurity_survey.pdf

Challenges cont.

Amount of Legacy OS Footprint	Percentage
1-10%	53%
11-20%	23%
21-30%	11%
31-40%	4%
41-50%	3%
More than 50%	6%



Reference: https://www.himss.org/sites/hde/files/media/file/2022/01/28/2021_himss_cybersecurity_survey.pdf

Conclusion

Closing remarks

Thank you!