# 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*

## Table of Content:

## OVERVIEW

Vulnerability management and assessment is a critical component to an organization's cybersecurity strategy, designed to safeguard the (C)onfidentiality, (I)ntegrity, and (A)vailability of information. This process involves identifying, evaluating, remediating, and reporting vulnerabilities in systems and software, helping organizations proactively detect and mitigate potential threats before they can be exploited. Vulnerability scanning both reduces attack vectors an organization faces and enhances overall security posture. This study serves to explain the key aspects of vulnerability management, its significance within the healthcare sector, the various frameworks that help shape the internal processes, technology solutions that aid security teams, and overall best practices. By understanding and effectively managing vulnerabilities, organizations can better protect themselves against cyber threats and maintain strong security defenses.

## INTRODUCTION

### Defining System Vulnerability

A system vulnerability refers to a weakness within a system that can be exploited to gain access or perform malicious actions. These vulnerabilities appear in most, if not all, software applications, network and hardware components, operating systems, and other IT tools or services. Common examples include unpatched software, misconfigured access controls, and weak passwords.

### The Vulnerability Management & Assessment Process

The vulnerability management and assessment process is a methodology for identifying, evaluating, remediating, and reporting security vulnerabilities and involves several key steps:

- ***Plan***: This initial step involves formulating a plan for performing the vulnerability scan. Outlining the scope of the assessment grants insight to the components of the network that need to be protected.
- ***Identify***: This phase involves scanning and identifying all assets within the organization's tech environment to uncover vulnerabilities across hardware, software, network devices, and other components. Automated tools such as vulnerability scanners are commonly utilized to ensure coverage, and in many cases, will be an exported file containing a list of machines with Common Vulnerabilities and Exposures, or CVE's.
- ***Assessment***: During the assessment phase, identified vulnerabilities are evaluated to determine their severity and potential impact on the organization. Evaluation is typically based on established criteria, such as the Common Vulnerability Scoring System (CVSS), which provides a standardized method for rating the severity of vulnerabilities.
- ***Prioritization***: At this stage, vulnerabilities are ranked based on the risk they pose to the organization, keeping the criticality of the affected assets, the potential business impact, and risk tolerance in consideration.
- ***Remediation***: The remediation phase involves applying fixes or mitigation measures to address the identified vulnerabilities. Common solutions include applying patches or updates, reconfiguring systems, and enhancing access

controls to mitigate the risk.

- ***Verification***: The verification phase ensures that the vulnerabilities have been effectively addressed, and it is best practice to rescan the modified software, hardware, or network to validate the changes.
- ***Reporting***: Documenting findings and actions taken to provide a clear overview of the security posture.

### Examples of Vulnerability Management

In the IT field, vulnerability management involves regularly patching software to fix security flaws, conducting penetration testing to uncover hidden vulnerabilities, and using automated tools to scan networks for weaknesses. Additionally, non-IT security measures can be taken to prevent exposure, such as conducting regular security audits of campuses to identify access control weaknesses or training employees to recognize and avoid phishing attacks.

## RELEVANCY

### Importance of Protecting Organizational Assets

Protecting organizational assets is vital to maintaining the trust of customers, partners, and shareholders. Good vulnerability management ensures that sensitive information remains confidential, data integrity is preserved, and systems remain available for use. Without proper protection, organizations risk data breaches, financial losses, legal repercussions, and reputational damage.

### Examples of Good and Bad Vulnerability Management Practices

Good vulnerability management practices include regularly updating software, conducting thorough risk assessments, prioritizing vulnerabilities based on potential impact, and implementing robust security controls. Conversely, bad practices involve neglecting updates, failing to perform regular scans, ignoring identified vulnerabilities, and lacking a structured approach to security management.

### Proactive vs. Reactive Approach

A proactive approach to vulnerability management involves anticipating and addressing vulnerabilities before they can be exploited, preventing potential security incidents. Continuous monitoring, regular updates, and employee training are proactive strategies.  A reactive approach, on the other hand, focuses on responding to incidents after they occur, which can lead to greater damage and higher recovery costs. Proactive management is essential for maintaining a strong security posture and minimizing the risk of cyber-attacks.

## FRAMEWORKS

**NIST CSF**:  The National Institute of Standards and Technology (NIST) produced the Cybersecurity Framework (CSF) which contains a set of information security guidelines under several key functions, one of which is the ***Protect*** function. This function emphasizes the development and implementation of appropriate safeguards to ensure the delivery of critical infrastructure services and secure information systems. Within the context of vulnerability management practices, the function includes several relevant processes and procedures that help organizations deal with system vulnerabilities and misconfigurations.  Some of the various sections within the Protect function include:

- ***Access Control -*** Implementing measures to limit access to information systems based on user roles and responsibilities. This is vital in vulnerability management, as it ensures that only authorized personnel can access and modify systems, reducing the risk of exposure to vulnerabilities.
- ***Awareness and Training*** - Conducting security awareness programs to educate employees about safe computing practices and emerging threats. This is essential for vulnerability management, as informed users are more likely to recognize and report potential vulnerabilities or security incidents.
- ***Data Security*** - Establishing policies to protect data at rest, in transit, and during processing. This includes encryption, data classification, and ensuring proper data handling practices are in place to mitigate risks associated with vulnerabilities.
- ***Maintenance*** - Regular system maintenance, including updates and patches, is critical for vulnerability management. The Protect function emphasizes the importance of applying security patches timely and maintaining systems to reduce the risk of exploitation of known vulnerabilities.
- ***Protective Technology*** - Utilizing technology such as firewalls, intrusion detection systems, and automated vulnerability scanning tools to detect and manage vulnerabilities proactively. This aligns with vulnerability management by continuously monitoring for and addressing security gaps.
- ***Incident Response*** - While primarily part of the Response function, the Protect function acknowledges the need for effective incident response planning. Organizations must be prepared to quickly contain and remediate

incidents that arise from exploited vulnerabilities.

NIST's *Protect* function plays a pivotal role in vulnerability management by establishing a holistic security posture that emphasizes prevention, detection, and response strategies. By integrating these practices, organizations can reduce the likelihood of vulnerabilities being exploited and improve their overall security resilience.

**Other Well Known Frameworks:** There are several security frameworks available that organizations can adopt to enhance their security posture and address vulnerabilities. Here are some of the most widely recognized ones in the security sector today:

- **ISO/IEC 27002 -** This is a 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 Controls -** The Center for Internet Security (CIS) has developed a set of 20 critical security controls that provide a prioritized approach to cybersecurity. These controls help organizations defend against the most common cyber threats and vulnerabilities.
- **COBIT (Control Objectives for Information and Related Technologies) -** This is a framework for developing, implementing, monitoring, and improving IT governance and management practices. It includes security and risk management processes, such as vulnerability management.
- **MITRE ATT&CK -** This framework provides a comprehensive knowledge base of adversary tactics and techniques based on real-world observations.

Organizations use it for vulnerability threat modeling and detection.

- **SANS Top 20 -** The 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.

We found that each framework has its strengths and weaknesses, and each is designed to address a specific aspect of the security platform. Which is why healthcare organizations may often choose to align themselves with multiple frameworks to address very specific regulatory requirements, industry standards, or overall security strategy.

## TECHNOLOGY: DISCOVERY TOOLS & THREAT INTELLIGENCE

*Vulnerability scanner technology* is used to check for weaknesses in networks, systems, and applications that could expose them to attacks. They can identify vulnerabilities caused by misconfigurations or outdated applications in organizational assets such as routers, firewalls, servers, endpoints, or Internet of Things (IoT) devices. Some examples we looked at during our analysis includes:

a. **Tenable Nessus** - Tenable Nessus is a vulnerability assessment platform developed by Tenable, Inc. that scans for security vulnerabilities in networks, devices, applications, operating systems, and cloud services. It is used to help enterprise IT teams identify and fix vulnerabilities before attackers can exploit them.

b. **Qualys** - Qualys is a cloud-based cybersecurity and vulnerability management platform that offers a wide range of security and compliance solutions to help organizations identify, prioritize, and remediate security vulnerabilities in their networks, systems, and applications. It is known for its scalability, comprehensive coverage, and ease of use.

c. **Rapid 7** - Rapid7 is a cybersecurity company that provides products and services to help businesses protect against, detect, and respond to security incidents. Their platform includes tools for threat intelligence, vulnerability management, cloud security, and more. Rapid7's mission is to make security tools and practices accessible to everyone, and their products are used by over 9,000 customers in a variety of industries, including energy, financial services, government, education, retail, and healthcare.
d. **Microsoft Defender** - Windows Security, formerly known as Windows Defender Security Center, is an app built into Windows 10 and 11 that helps keep PCs more secure. It includes Microsoft Defender Antivirus, an antivirus tool that helps protect you against viruses, ransomware, and other malware.
e. **CrowdStrike Falcon** - CrowdStrike Falcon is a software that protects systems from cyberattacks by monitoring computers for signs of suspicious activity. It is a type of "endpoint detection and response" (EDR) software that is installed on devices to provide real-time protection. Falcon monitors and records information such as login details, program details, and file details. It then uses this information to detect and remediate potentially malicious activity, analyze internet connections, and identify new patterns of malicious behavior. When Falcon detects a threat, it helps to lock it down.

*Threat intelligence technology* on the other hand includes a variety of data points and feeds that can provide useful information about potential or existing cyber threats and system vulnerabilities. Some sources include:

- **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. Our Core Values reflect this design and underpin everything we do at CISA.
- **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

When we talk about the *risks* associated with a system vulnerability, we are referring to the potential harm to the organization (e.g., service disruption, data loss, etc.) if that vulnerability were to be exploited by a threat actor. When we assess the level of risk introduced by a vulnerability, we consider two important factors:

1. **Probability**: Likelihood of the vulnerability being exploited
2. **Impact**: The effect a successful exploitation would have on the organization

However, while most security standards and frameworks agree on the definition of risk, we found there is less agreement on the correct way to assess risk levels, especially as it relates to a risk's probability and impact.

On one hand, let us consider the impact of a successful exploitation attempt. You could argue that assessing the impact is relatively simple and straightforward, as it merely requires you to consider the aftermath of such an event happening. However this requires collaboration from all key stakeholders throughout the organization as the impact to me and my team may be (and likely is) different from the impact to other areas. And in the healthcare sector, knowing whether a cyber risk can affect patient care is key as it could be the difference between life and death.

On the other hand, let us consider the probability of such an event actually happening. There is undoubtedly going to be a big difference between trying to *estimate* the probability versus *measuring* it. From a purely mathematical standpoint, probability is defined as the ratio of the number of “successful” events to the total number of attempts. So trying to measure the probability of exploitation requires us to know the number of tries versus the successful ones, which is not always easy to obtain, especially when you consider brand new vulnerabilities. Not to mention that data  on successful breaches (from other organizations) is hard to get and would not be a fair comparison since control environments are likely very different. However, *estimating* a risk can also be problematic as we tend to bring a number of biases into the equation, which can lead to *probability neglect*[1].

Having said that, Information Security teams must find effective ways of classifying vulnerabilities and assigning a **risk score** to each one. This helps provide a holistic view of the healthcare organization’s risk profile and can be useful in determining where to start lowering risk (“the most bang for your buck”). While developing your

[1] https://research.tudelft.nl/files/114356210/SAFE21016FU1.pdf

own scoring methodology is an option, we found that many healthcare organizations simply leverage existing scoring tools and resources which already account for many important factors that determine the criticality of a vulnerability (e.g., attack vector, complexity, reports of exploitability, remediation/workarounds, etc.). Some of them include:

1. Common Vulnerability Scoring System (CVSS)
    a. The CVSS captures the principal characteristics of system vulnerabilities and produces a numerical score that reflects their severity. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes. CVSS is a published standard used by organizations worldwide
2. Stakeholder Specific Vulnerability Categorization (SSVC)
    a. The SSVC, developed by CISA, is a customized decision tree model that assists in prioritizing vulnerability response for the United States government (state, local, and territorial), as well as critical infrastructure entities. It uses four scoring decisions: *Track*, *Track**, *Attend*, and *Act*.
3. Common Weakness Enumeration (CWE)
    a. The CWE is used to classify and categorize common software vulnerabilities. There are currently over 600 categories ranging from buffer overflows, cross-site scripting to insecure random numbers. Weaknesses are generally vulnerabilities that may consist of flaws, bugs, or other errors in hardware or software, code, design, or architecture.
4. OWASP Top 10

   a. The Open Web Application Security Project (OWASP) is an international non-profit organization dedicated to web application security. The OWASP Top 10 is a regularly-updated report outlining security concerns for web application security, focusing on the 10 most critical risks. The report is put together by a team of security experts from all over the world.

5. Proprietary Risk Scores
   a. Vendors that develop vulnerability management technology such as the ones previously mentioned often produce their own scoring rubrics, usually leveraging existing scoring tools and integrating them with their own proprietary risk scoring logic. This makes their products more valuable as they can scan for issues and also rate them. For example, Tenable Nessus combines the CVSS score with their own Vulnerability Priority Rating (VPR) to quantify risk and urgency[2].

## PRIORITIZATION & REMEDIATION

Once you have learned about a vulnerability in your environment and were able to assess the level or risk associated with that vulnerability (risk score), the logical next step would be to determine what *action* needs to be taken to address the issue. Security teams and risk managers have several options:

1. **Avoid**: Stop using the system affected by the vulnerability. This is rarely a viable option for healthcare organizations.
2. **Transfer**: Shift the risk to a third-party, such as a vendor or through cyber

[2] https://docs.tenable.com/nessus/Content/RiskMetrics.htm

insurance. However, this does not entirely free the organization from impact, as vendor breaches can anyway result in reputational or legal risks.

3. **Accept**: You can accept the risk and choose not to address the issue. This of course depends on the organization's risk tolerance.
4. **Mitigate**: You can choose to mitigate (remediate) the system vulnerability to eliminate the risk. For purposes of this paper we are going to focus on remediation efforts.

When organizations choose to remediate system vulnerabilities, it can be a daunting task. In 2023 alone, 26,447 vulnerabilities were made public[3]. And while scoring methodologies can tell you the *inherent* risk score of a vulnerability, only the organization knows what the *residual* risk is for them based on factors such as existing/mitigating controls and asset criticality. This is crucial to figure out, especially when dealing with small, poorly-funded security teams that do not have the time or resources to fix every single vulnerability at the same time.

That is why it is recommended to take a risk-based approach to the prioritization and remediation of system vulnerabilities and not try to "boil the ocean." In order to do that, security teams need to be able to look at the inherent risk scores provided by the vulnerability scanners or from the threat intelligence received, and then adjust the score to account for internal factors. Some questions to consider when increasing or decreasing the remediation priority include:

- Is the affected asset an internal or external (Internet-facing) one?
- Does the affected asset provide a critical service? Does it directly impact

[3] https://blog.qualys.com/vulnerabilities-threat-research/2023/12/19/2023-threat-landscape-year-in-review-part-one

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?

Lastly, organizations should assign a service level agreement (SLA) to those remediation tasks based on residual risk score. For example, an organization may decide that *Critical* vulnerabilities must be patched/updated within 15 days, *High* one within 45 days, *Moderate* ones within 90 days, and *Low* ones within 180 days. This should also account for super critical vulnerabilities which may require immediate action (e.g., off-cycle patch). We found that when this approach is followed, vulnerability remediation becomes more manageable, and the easier it is to reduce the overall risk profile.

## CHALLENGES

A unique set of challenges troubles organizations, healthcare in particular, when it comes to vulnerability management. These challenges need not be swept under the rug but rather met with comprehensive strategies and resources to protect the confidentiality, integrity, and availability of patient and hospital staff PII and PHI. To ensure that an organization has the proper personnel, tools, and training, organizations need to have a budget in place to accommodate all of these. Clinics, hospitals, and labs are constantly seeking the aid of advances in technology to better serve their patients. These advances of complex systems to the IT infrastructure in healthcare have proven themselves to be a great asset but at the expense of significantly increasing the attack surface. Although the IT infrastructure is constantly evolving, legacy systems can still be found in the ranks of more modern IT infrastructure. Legacy systems often present issues that modern solutions may not be able to protect healthcare organizations, further complicating efforts to safeguard highly private information. An under-prioritized yet crucial aspect is training and awareness. It is one thing to train and bring awareness to the IT personnel on staff, but it is far more difficult for nurses pulling 12-hour shifts looking after patients. Other challenges faced, to be discussed in greater detail, include IoT devices and staff being reluctant to incorporate change. Bringing these challenges to the forefront is essential in protecting the confidentiality, availability, and integrity of healthcare data.

Budget constraints make it difficult for cybersecurity professionals to safeguard healthcare's IT infrastructure from would-be attackers. Within the healthcare sector, cybersecurity is generally allotted 4-7% of the total IT budget (CDW 2024). This makes it very difficult for the cybersecurity staff to implement the best technological controls, hire experienced staff, and give them the proper training to combat the latest threats to the organization. A dataset taken in 2017 presents a strong case for healthcare organizations to increase their budget. Of cybersecurity claims reported, the healthcare sector accounted for 17%, but the breach costs from these claims represented 28% - $65M (Net Diligence 2018). Increasing the cybersecurity budget would ensure staff are equipped with capable vulnerability management software, training to utilize tools properly, and hiring competent staff.

It is not just a hurdle of hiring knowledgeable staff that will be an asset from day one; it is just as much of a challenge to retain that staff. According to a survey conducted by HIMSS, the Healthcare Information Management and Systems Society, reasons that healthcare organizations struggle to retain staff include insufficient compensation, limited career growth, and an absence of executive support (Southwick 2024). Staff that are able to take advantage of training provided find themselves highly sought after. Vulnerability management tools like Qualys and Tenable Nessus offer certification paths to showcase a person's knowledge of tool utilization. Competing healthcare organizations will look to poach this talent to better equip their team in combating cybersecurity threats. Companies may find that hiring staff from outside the organization is best for preventing complacent and reluctant behavior. It is common to find staff members that are set in their ways of doing things. With a threat landscape that is always changing for a multitude of reasons – to be discussed in greater detail later, it poses a huge risk to the organization if staff members are not willing to adapt to these changes. It is vital for healthcare organizations to hire lifelong learners in their cybersecurity departments.

We have briefly discussed some of the personnel challenges healthcare organizations face in protecting their IT infrastructure with vulnerability management. The focus will now be shifted to the technical challenges. The complexity of IT infrastructure within healthcare organizations makes it a daunting task to protect an organization from vulnerabilities. IoT (Internet of Things) presents a unique challenge to healthcare organizations to secure. A passage from a peer-reviewed article authored by Ramakrishna Dantu, Indika Dissanayake & Sridhar Nerur (2021) is quoted below:

> "It is clear that security and privacy have become critical factors for the

> development and application of IoT in any domain (Ng et al., 2018). The need to address these concerns is even more important in healthcare, as it deals with highly sensitive medical data. Based on our analysis, the core articles in this cluster focus on several topics related to the privacy and security of medical data and biometric devices, including RFID authentication mechanisms, medical data security, and privacy… RFID is one of the key technologies used in IoT deployment in the healthcare domain. For example, RFIDs are used in wearable biometric devices such as patient monitoring systems to identify and access patients' medical records in real-time.”

By implementing IoT devices, healthcare organizations can better serve their patients, but it does increase their attack surface dramatically, further exposing them to more vulnerabilities and monitoring that needs to take place by an already short-handed staff.

It is not a matter of wanting to use legacy systems, but oftentimes it is a matter of reliance within healthcare IT infrastructure. HIMSS conducted a survey in 2021 that disclosed 73% of healthcare providers are reliant on legacy systems (Glynn 2024). These legacy systems include OS (operating systems) such as Microsoft Server 2008, Windows 7, Windows Server 2003, and 2003 R2. Per the same survey, 76% of respondents disclosed that they have a legacy footprint between 1 – 20% (HIMSS 2022). Legacy systems are not limited to OSs; they include devices and applications. This may not seem like a large percentage in terms of footprint, but the danger of having legacy systems incorporated alone can pose catastrophic damage to the healthcare provider. More often than not, legacy systems have lost vendor support and there are no available patches. Cybersecurity personnel conducting vulnerability scans have the responsibility of making the system owners and management aware of these findings. With this information, management and execs can make more informed decisions on how they choose to mitigate the risk.

## CONCLUSION

Vulnerability management is an essential part of any organization, especially healthcare. Challenges like finding and retaining experienced cyber professionals, the use of legacy systems, IoT, and tight budgets are handicapping healthcare executives. However, tools such as Tenable Nessus and Qualys, along with their training, are readily available for professionals to help protect their organization's assets via vulnerability management. Training and monitoring of the systems is a continuous and ongoing process. The threat landscape is forever changing, as well as equipment like IoT and complex IT infrastructure. Healthcare organizations need attentive, detail-oriented professionals. These professionals can stay abreast of the latest trends via threat intelligence resources. Vendors can even send out notifications—for a fee—to organizations, keeping them alert to immediate threats within the healthcare sector. The NIST Cybersecurity Framework 2.0 categorizes vulnerability management under the Protect pillar. This framework and many others provide the foundation for basing our vulnerability management system on a proactive approach. Vulnerability management has been and will remain a relevant aspect within healthcare organizations to ensure the protection of patients PHI and PII.

# REFERENCES

- Dantu, Ramakrishna, Indika Dissanayake, and Sridhar Nerur. “Exploratory Analysis of Internet of Things (IoT) in Healthcare: A Topic Modelling & Co-Citation Approaches.” *Information systems management* 38.1 (2021): 62–78. Web.
- HIMSS. (2021). *2021 HIMSS cybersecurity survey*. Healthcare Information and Management Systems Society. https://www.himss.org/sites/hde/files/media/file/2022/01/28/2021_himss_cybersecurity_survey.pdf
- NetDiligence. (2018). *Healthcare cyber claims study 2018*. https://netdiligence.com/wp-content/uploads/2018/04/NetDiligence_Healthcare-Study_2018-1_PUBLIC.pdf
- *The cost of cybersecurity in Healthcare*. CDW.com. (n.d.). https://www.cdw.com/content/cdw/en/articles/security/the-cost-of-cybersecurity-in-healthcare.html
- Glynn, P. (2024, March 5). *What are Legacy Systems in healthcare? (& how to manage them)*. Insight Global. https://insightglobal.com/blog/legacy-systems-in-healthcare
- Southwick, R. (2024, March 2). *Healthcare cybersecurity budgets are rising, but workers are hard to find*. OncLive. https://www.chiefhealthcareexecutive.com/view/healthcare-cybersecurity-budgets-are-rising-but-workers-are-hard-to-find
- *Enterprise cyber risk & security platform*. Qualys. (n.d.). https://www.qualys.com
- Individual preferences in security risk decision making: An exploratory study under security professionals. Johan J. de Wit, Wolter Pieters, and Pieter H.A.J.M. van Gelder (2021)

  https://research.tudelft.nl/files/114356210/SAFE21016FU1.pdf