International Journal of Computer Engineering and Technology (IJCET)
Volume 15, Issue 4, July-Aug 2024, pp. 577-586, Article ID: IJCET_15_04_051
Available online at https://iaeme.com/Home/issue/IJCET?Volume=15&Issue=3
ISSN Print: 0976-6367 and ISSN Online: 0976-6375
Impact Factor (2024): 18.59 (Based on Google Scholar Citation)
DOI: https://doi.org/10.5281/zenodo.13332748

BUILDING A VULNERABILITY MANAGEMENT FRAMEWORK: A PILLAR TO CYBER DEFENSE

Mukta Sharma
Sr. IT Compliance Analyst, Intercontinental Exchange, Virginia, USA

Krunal Patel
Lead Engineer, StitchFix, Virginia, USA

ABSTRACT

In today's landscape, digital innovation and transformation are occurring at a rapid pace, introducing the risk of vulnerabilities into systems. It is imperative for organizations to build robust cyber defense strategies to safeguard against potential threats. If exploited by attackers, these vulnerabilities can lead to significant financial, regulatory, and reputational losses. An effective vulnerability management program is essential for providing assurance that systems are being monitored and risks are being mitigated, thereby keeping attacks at bay. This paper explores a comprehensive vulnerability management framework that organizations can utilize as a starting point to build their programs, ensuring robust security and resilience against emerging threats.

Keywords: Cybersecurity, Incidents, Software, Threats, Vulnerabilities

Cite this Article: Mukta Sharma and Krunal Patel, Building A Vulnerability Management Framework: A Pillar to Cyber Defense, *International Journal of Computer Engineering and Technology (IJCET)*, 15(4), 2024, pp. 577-586.
https://iaeme.com/MasterAdmin/Journal_uploads/IJCET/VOLUME_15_ISSUE_4/IJCET_15_04_051.pdf

1. INTRODUCTION

A vulnerability is a weakness in the application which can be an implementation bug or a design flaw that allows an attacker to cause harm to the user of the application and get extra privileges. Vulnerability is the potential risk for the system. Attackers use these vulnerabilities to exploit the system and get unauthorized access and information. Vulnerabilities are a big flaw in system security and Information assurance. A vulnerability free system can provide more Information Assurance and system security. Though it is almost impossible to have a 100% vulnerability free system, by removing as many vulnerabilities as possible, we can increase system security [1].

Software vulnerabilities can jeopardize intellectual property, consumer trust, and business operations and services. The Software Engineering Institute estimates that 90 percent of reported security incidents result from exploits against defects in the design or code of software [2]. As per research by Dynatrace, 50% of CISOs are fully confident that the software delivered by development teams has been completely tested for vulnerabilities before going live in production environments [3].

According to projections, cybercrime is forecast to cost the global economy $10.5 trillion by 2025, reflecting a 15% yearly increase. Businesses have never been more vulnerable; even large enterprises with substantial cybersecurity defenses can fall victim [4]. Organizations face a significant challenge to prioritize vulnerabilities because they lack information about the risk these vulnerabilities pose to their environment. Vulnerability management is more difficult because the complexity of their software supply chain and cloud ecosystem has increased [3].

Therefore, it is imperative for organizations to continually enhance their cybersecurity strategies, employ advanced threat detection and prevention technologies, and foster a culture of security awareness to mitigate these risks and protect their valuable assets.

Usually, vulnerability assessment involves scanning a system, software, or network to detect weaknesses and deficiencies that could be exploited by attackers to disrupt the business. These vulnerabilities can serve as backdoors for unauthorized access. Common types of vulnerabilities include access control issues, boundary condition flaws, input validation errors, authentication weaknesses, configuration issues, and exception handling vulnerabilities.

It is crucial to keep vulnerabilities at bay to prevent potential security incidents that can lead to significant consequences. Exploited vulnerabilities can result in data breaches, can lead to cyber incidents such as causing severe disruption to business operations and necessitating the filing of a Securities and Exchange Commission (SEC) Form 8-K (applicable only to public companies) to disclose the incident. Such breaches not only damage an organization's reputation but can also incur substantial regulatory fines. Proactively managing vulnerabilities ensures the integrity, confidentiality, and availability of systems, thereby safeguarding against financial, regulatory, and reputational losses.

The remainder of this paper is organized as follows. Section 2 provides an overview of the types of vulnerabilities that organizations commonly face. Section 3 discusses the vulnerability management framework, emphasizing alignment with the NIST framework and highlighting best practices and guidelines. In Section 4, we delve into what can be tested using the NIST framework for effective vulnerability management. Section 5 concludes the paper by summarizing key findings and offering a high-level overview of the NIST framework's approach to vulnerability management.

2. TYPES OF VULNERABILITIES

Understanding the diverse range of vulnerabilities that can impact systems, networks, and organizations is crucial for effective cybersecurity. From software flaws to human error and supply chain risks, each type of vulnerability presents unique challenges and potential threats. This section provides a comprehensive overview of the most common vulnerabilities, highlighting the importance of vulnerability scanning in identifying and mitigating these risks.

- Software Vulnerabilities: Software vulnerabilities are among the most common and widely discussed. These include flaws, bugs, and weaknesses within software applications. Malicious actors can exploit these vulnerabilities to gain unauthorized access, steal data, or compromise systems. For instance, the "Heartbleed" bug in OpenSSL highlighted how a single software vulnerability could expose sensitive information across the internet.

- Network Vulnerabilities: Network vulnerabilities often occur due to misconfigurations or outdated hardware. Weak passwords, open ports, or unpatched systems can leave a network susceptible to intrusions. The impact of network vulnerabilities can range from data breaches to complete network compromise, affecting both small businesses and large corporations.
- Human Error and Social Engineering: Human error is an often underestimated vulnerability. Employees may accidentally leak sensitive information or fall victim to social engineering attacks. Cybercriminals use tactics like phishing emails to manipulate individuals into disclosing valuable data. This type of vulnerability is particularly dangerous as it leverages human trust, making it difficult to defend against.
- Physical Vulnerabilities: Physical vulnerabilities refer to weaknesses in the physical infrastructure of a system. Unauthorized physical access to a data center, for instance, can lead to data theft or system damage. In some cases, even a misplaced USB drive could serve as an entry point for attackers.
- Hardware Vulnerabilities: Hardware vulnerabilities involve weaknesses in the components of a system, such as CPUs, memory, or storage devices. The infamous "Spectre" and "Meltdown" vulnerabilities in modern CPUs demonstrated how hardware flaws could allow attackers to access sensitive data.
- Zero-Day Vulnerabilities: Zero-day vulnerabilities are the most dangerous type because they are unknown to software vendors and, as such, no patches or fixes are available. Cybercriminals often target these vulnerabilities, as they provide a window of opportunity to exploit systems without detection.
- Supply Chain Vulnerabilities: Supply chain vulnerabilities have gained significant attention in recent years. These vulnerabilities exist when a company's software or hardware supply chain is compromised. For example, a compromised update to a widely used software program can infect countless systems once installed.
- Regulatory and Compliance Vulnerabilities: Organizations must comply with various regulations and standards related to cybersecurity. Failing to meet these requirements can lead to legal consequences, fines, and damage to an organization's reputation.
- Third-Party Vulnerabilities: Organizations often rely on third-party services or products. Vulnerabilities in these third-party components can expose an organization to risks beyond their control. For instance, a data breach at a cloud service provider can affect all of its customers.
- Insider Threats: Employees or trusted individuals within an organization can intentionally or unintentionally compromise security. Insider threats can lead to data leaks, sabotage, or other malicious activities.
- Legacy Systems and Software: Continuing to use outdated and unsupported software or hardware can create vulnerabilities. These systems are more likely to have known security flaws and may lack the latest security updates.
- Cultural Vulnerabilities: An organization's culture and practices can create vulnerabilities. Poor security awareness, lack of accountability, and a culture that does not prioritize cybersecurity can lead to a weaker defense.

Understanding the multitude of vulnerabilities that can impact systems, networks, and organizations is the first step in mitigating their potential risks. Vulnerability scanning plays a pivotal role in identifying and addressing these weaknesses, allowing proactive measures to be taken before cyberattacks occur [5].

3. FRAMEWORK FOR VULNERABILITY MANAGEMENT PROGRAM

The National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), originally published in 2014, is a set of guidelines designed to help organizations improve their cybersecurity posture, better manage IT security risks, and enhance their protection against cyber threats. The 2024 release of version 2.0 of their Cybersecurity Framework represents the first major update since the NIST CSF was initially released [6].

The NIST Cybersecurity Framework (CSF) 2.0 provides a comprehensive guide for managing and reducing cybersecurity risk, encompassing core functions - Identify, Protect, Detect, Respond, Recover, and Govern.

Figure 1: TODO: Add name

In NIST CSF 2.0 there are 22 categories and 106 subcategories. Additionally, NIST provides implementation examples [7] for these categories to ensure effective cybersecurity readiness and resilience.

Table 1: TODO: Add name

NIST Cybersecurity Framework 2.0		
CSF 2.0 Function	**CSF 2.0 Category**	**CSF 2.0 Category Identifier**
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles and Responsibilities	GV.RR
	Policies and Procedures	GV.PO
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Supply Chain Risk Management	ID.SC
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Adverse Event Analysis	DE.AE
	Continuous Monitoring	DE.CM
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

This paper focuses on 11 categories and 21 subcategories relevant to developing a vulnerability management program. This section aims to equip you with the tools to establish a robust vulnerability management program, ensuring a structured approach to identifying, protecting, detecting, responding to, and recovering from vulnerabilities. The table 1 below summarizes the relevant subcategories from the Framework that can be incorporated into your vulnerability management process.

Table 2: TODO: insert table header

FUNCTION	CATEGORY	SUB-CATEGORY
GOVERN (GV)	Roles, Responsibilities, and Authorities (GV.RR)	GV.RR-02: Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced GV.RR-03: Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies It is essential to ensure that roles and responsibilities for managing vulnerabilities are clearly defined and enforced, facilitating efficient identification and remediation. Adequate resources must be allocated, aligning with the cybersecurity risk strategy to support effective vulnerability management.
	Policy (GV.PO)	GV.PO-02: Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission. A policy for managing cybersecurity risks should be regularly reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and the organizational mission. This ensures that the vulnerability management program remains relevant and effective in addressing current and emerging threats.
	Cybersecurity Supply Chain Risk Management (GV.SC):	GV.SC-07: The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship. GV.SC-04: Suppliers are known and prioritized by criticality. The risks posed by suppliers, their products and services, and other third parties should be understood, recorded, prioritized, assessed, responded to, and monitored throughout the relationship. Additionally, suppliers should be known and prioritized by their criticality to ensure effective management of vulnerabilities associated with third-party interactions.
Identify (ID)	Asset Management (ID.AM)	ID.AM-01: Inventories of hardware managed by the organization are maintained. ID.AM-02: Inventories of software, services, and systems managed by the organization are maintained. When a vulnerability is detected, it's crucial to tie it back to impacted assets. Conducting an asset inventory of both hardware and software simplifies mapping vulnerabilities to the affected assets.
		ID.AM-05: Assets are prioritized based on classification, criticality, resources, and impact on the mission. Prioritizing remediation emphasizes the potential business impact of a vulnerability and the likelihood of its exploitation. By identifying critical assets, it can be determined which vulnerabilities to address first, ensuring the most significant threats are mitigated promptly.
	Risk Assessment (ID.RA):	ID.RA-01: Vulnerabilities in assets are identified, validated, and recorded. Once the asset inventory is complete, it should be connected to the identified vulnerabilities, a process known as vulnerability asset mapping. This helps in finding high-priority assets that are both valuable to the business and contain severe, exploitable vulnerabilities.

		ID.RA-02: Cyber threat intelligence is received from information sharing forums and sources Ingesting threat intelligence is vital for security and enhances vulnerability management programs. Integrating threat intelligence sources within program and can provide essential context to vulnerabilities
		ID.RA-04: Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded ID.RA-08: Processes for receiving, analyzing, and responding to vulnerability disclosures are established A modern vulnerability management program prioritizes risk remediation based on a holistic view of the organization's risk profile, considering not just the CVSS score but also the importance of the asset and exploitability conditions. Processes for receiving, analyzing, and responding to vulnerability disclosures are established, adding a critical layer of context and ensuring timely and effective remediation efforts.
Protect (PR)	Platform Security (PR.PS)	PR.PS-06: Secure software development practices are integrated, and their performance is monitored throughout the software development life cycle. Secure software development practices should be integrated, and their performance monitored throughout the software development life cycle to ensure vulnerabilities are identified and addressed early
	Awareness and Training (PR.AT)	PR.AT-02: Individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind. Specialized roles should receive targeted awareness and training to effectively identify, manage, and mitigate vulnerabilities and cybersecurity risks.
	Technology Infrastructure Resilience (PR.IR)	PR.IR-01: Networks and environments are protected from unauthorized logical access and usage. Implement controls to protect networks and environments from unauthorized access and potential vulnerabilities.
DETECT (DE):	Continuous Monitoring (DE.CM)	DE.CM-01: Networks and network services are monitored to find potentially adverse events o DE.CM-02: The physical environment is monitored to find potentially adverse events. DE.CM-03: Personnel activity and technology usage are monitored to find potentially adverse events. Implement monitoring across networks, physical environments, and personnel activities to detect and address potential vulnerabilities and adverse events.
RESPOND (RS):	Incident Analysis (RS.AN):	RS.AN-03: Analysis is performed to establish what has taken place during an incident and the root cause of the incident. RS.AN-06: Actions performed during an investigation are recorded, and the records' integrity and provenance are preserved. In a vulnerability management program, analyze incidents to determine their causes and ensure that all investigative actions and records are thoroughly documented and preserved for integrity.

	Incident Recovery Communication (RC.CO):	RC.CO-03: Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders. In a vulnerability management program, it's crucial to communicate recovery efforts and progress to stakeholders if a vulnerability is exploited. Although prevention is the primary goal, the program should also include contingency measures and alternative controls to mitigate impacts when vulnerabilities are successfully exploited.

The functions and categories from the NIST CSF 2.0 can be used to develop your vulnerability management program.

4. VULNERABILITY MANAGEMENT PROGRAM

An effective vulnerability management program consists of five key steps: 1) Identification of vulnerabilities, 2) Evaluating Risk and Impact, 3) Remediation Action Plan, 4) Reporting Post Remediation and 5) Monitoring and Continuous Improvement. This structured approach ensures systematic management of vulnerabilities from detection through resolution and review.

These four steps will be mapped to the NIST CSF 2.0 analysis to build an effective vulnerability management program. This approach encompasses policy development, adequate training, tool management, vulnerability remediation, incident analysis, and continuous monitoring for ongoing improvement.

4.1. Identifying Vulnerabilities

Vulnerability identification is an ongoing process that should be seamlessly integrated into all critical steps of an organization’s operations. Effective management starts with employing vulnerability management tools and keeping an up-to-date asset inventory. Key practices include staying informed through forums, analyzing past incidents, and conducting comprehensive penetration testing (e.g., red, blue, and purple team exercises, or engaging third-party services and bug bounty programs) to simulate real-world attacks and uncover vulnerabilities. Additionally, SIEM (Security Information and Event Management) tools, such as Splunk and Datadog, aggregate and analyze security data to detect, alert, and respond to potential threats in real-time. Integrating security checks into CI/CD pipelines during software development, through methods like automated code analysis and dependency scans, exemplified by tools such as Ruby Advisor, ensures vulnerabilities are identified and addressed early in the software development lifecycle, reinforcing overall code security.

From the above table 1, applicable NIST Controls: PR.PS-06, ID.AM-01, ID.AM-02, PR.IR-01, GV.SC-07, GV.SC-04

4.2. Evaluating Risk and Impact

Once vulnerabilities are identified, their impact must be assessed based on their criticality to business operations, primarily driven by risk assessment and the CVE score from vulnerability management tools. Start by maintaining an up-to-date inventory of software, hardware, and third-party components to evaluate criticality, triage, and prioritize vulnerabilities. Next, draft a remediation action plan to address the vulnerabilities. This plan should be shared with stakeholders to ensure timely and effective risk mitigation. Proper prioritization and clear communication are crucial for addressing the most significant threats and minimizing potential damage.

From the above table 1, applicable NIST Controls: ID.AM-05, ID.RA-01, ID.RA-02, ID.RA-04, and ID.RA-08

4.3. Remediation Action Plan

Document the remediation actions in a repository used for tracking vulnerabilities, ensuring each entry includes details such as the cause, impact, and next steps. Thorough recording is essential to maintain integrity and provide a clear history of the vulnerability management process, enabling effective follow-up and verification. Set up regular check-ins with remediation owners to get updates, ensure the action plan remains on track, and communicate any roadblocks to leadership.

From the above table 1, applicable NIST Controls: RS.AN-03 and RS.AN-06

4.4. Reporting Post Remediation

Validate that remediation actions were performed and verify that the applicable steps effectively mitigate the risks associated with the vulnerabilities. Assess the severity of the vulnerabilities to determine if additional measures are needed. Engage appropriate stakeholders based on the severity to communicate recovery steps and ensure proper follow-up. Document and review the outcomes to confirm that the vulnerabilities have been addressed appropriately.

From the above table 1, applicable NIST Controls: RC.CO-03

4.5. Monitoring and Continuous Improvement

To strengthen defenses and enhance monitoring, it's crucial to continuously improve oversight across networks, physical environments, and personnel activities to detect and address potential vulnerabilities and adverse events. Specialized roles supporting the vulnerability management program should receive targeted training to stay updated on managing and mitigating cybersecurity risks effectively. At a minimum, the cybersecurity risk management policy must be reviewed, updated, communicated, and enforced annually to adapt to evolving requirements, threats, and technologies, ensuring the program's effectiveness. Clear definitions and enforcement of roles and responsibilities, coupled with adequate resource allocation aligned with the cybersecurity risk strategy, are essential for efficient vulnerability identification and remediation. Emphasizing continuous improvement, the program should integrate feedback and lessons learned to enhance its resilience against emerging threats.

From the above table 1, applicable NIST Controls: DE.CM-01, DE.CM-02, DE.CM-03, GV.RR-02, GV.RR-03, GV.PO-02, PR.AT-02

5. CONCLUSION

In conclusion, this paper has detailed the essential components of constructing a robust vulnerability management program utilizing the NIST Cybersecurity Framework (CSF) 2.0. By examining various types of vulnerabilities that pose threats to organizations and leveraging NIST controls, the paper has outlined a comprehensive approach to vulnerability management. The integration of NIST’s core functions—Identify, Protect, Detect, Respond, and Recover—into the development of a vulnerability management program ensures a structured and effective strategy. Through the identification of critical building blocks and the application of specific NIST categories and subcategories, organizations can create a resilient framework to address and mitigate vulnerabilities.

This structured approach not only helps in managing current risks but also prepares organizations to adapt to emerging threats, ultimately strengthening their overall cybersecurity posture.

REFERENCES

[1] Goel, Jai Narayan, and Babu M. Mehtre. "Vulnerability assessment & penetration testing as a cyber defence technology." *Procedia Computer Science* 57 (2015): 710-715.

[2] Cybersecurity & Infrastructure Security Agency. Software Assurance. https://www.cisa.gov/sites/default/files/publications/infosheet_SoftwareAssurance.pdf

[3] Security Magazine. Fifty percent of CISOs confident that software is completely tested. https://www.securitymagazine.com/articles/99236-fifty-percent-of-cisos-confident-that-software-is-completely-tested

[4] Electric AI Blog. High-Profile Company Data Breaches. https://www.electric.ai/blog/recent-big-company-data-breaches

[5] Faster Capital. Types Of Vulnerabilities and Their Impact. https://fastercapital.com/topics/types-of-vulnerabilities-and-their-impact.html

[6] Beyond trust blog. NIST Cybersecurity Framework 2.0 – What's New & What You Need to Know. https://www.beyondtrust.com/blog/entry/nist-cybersecurity-framework-2

[7] NIST. Implementation Examples for the NIST Cybersecurity Framework 2.0. https://www.nist.gov/system/files/documents/2024/02/21/CSF%202.0%20Implementation%20Examples.pdf

Citation: Mukta Sharma and Krunal Patel, Building A Vulnerability Management Framework: A Pillar to Cyber Defense, International Journal of Computer Engineering and Technology (IJCET), 15(4), 2024, pp. 577-586

Abstract Link: https://iaeme.com/Home/article_id/IJCET_15_04_051

Article Link:
https://iaeme.com/MasterAdmin/Journal_uploads/IJCET/VOLUME_15_ISSUE_4/IJCET_15_04_051.pdf

✉ **editor@iaeme.com**