Literature Review of Vulnerability Management Best Practices in Cybersecurity

Aleksi Ruotsalainen

2024 Laurea

Laurea-ammattikorkeakoulu

Literature Review of Vulnerability Management Best Practices in Cybersecurity

Aleksi Ruotsalainen

Business Information Technology

Bachelor’s thesis

12/2024

Laurea University of Applied Sciences **Abstract**
Business Information Technology
Bachelor of Business Administration

Aleksi Ruotsalainen
Literature review of vulnerability management best practices in cybersecurity
Year 2024 Pages 17

The objective of this bachelor's thesis was to create a list of recommendations of vulnerability management best practices with focus on IT environments. This thesis was carried out as a commission for Nordic IT company.

A qualitative meta-synthesis and content analysis was applied in this thesis to analyze vulnerability management publications and literature to examine existing best practices and recommendations.

The main conclusion is that efficient vulnerability management programs require engagement of multiple stakeholders from leadership to other internal teams and should be aligned with organization's existing processes, tools and business objectives. It was found also that many publications recommend a risk-based approach to vulnerability management.

Keywords: vulnerability management, cybersecurity

Table of contents

1 Introduction

New threats emerge every day in the cyber landscape, requiring organizations to stay vigilant to secure their business and IT environments. New vulnerabilities are introduced daily, and organizations must prioritize the remediation of existing vulnerabilities while also addressing emerging zero-days or actively exploited vulnerabilities. In 2023, the most frequently exploited vulnerabilities were initially zero-day vulnerabilities, with adversaries exploiting more zero-day vulnerabilities compared to 2022 (CISA 2024). Therefore, an efficient vulnerability management program is an essential aspect of cybersecurity and risk management for organizations.

This thesis was commissioned by a Nordic IT company, which will be referred to as "Company X" hereafter. Company X identified vulnerability management as an important topic for their business and operations, which is why this was chosen as the focus of this thesis.

The primary aim of this thesis is to conduct an analysis of the current literature on vulnerability management and its best practices. Based on this analysis, the thesis seeks to provide recommendations for company X about the best practices of vulnerability management. The scope of this research is confined to the vulnerability management of IT environments, although many of the discussed concepts are applicable in various other contexts.

Throughout this thesis, Microsoft Copilot has been used to improve sentence structures, clarify text, and check for grammatical errors.

2 Terminology

Main concept in this thesis is vulnerability management, which is the ongoing process of identifying, assessing and managing vulnerabilities in organization’s operating environment. That covers all the aspects related to management of vulnerabilities such as remediation and accepting risk that certain vulnerability poses to an organization. (Carnegie Mellon University 2016; Palmaers 2013).

Vulnerability assessment, typically vulnerability scanning, is a part of vulnerability management where vulnerabilities are identified across the organization’s environment, usually utilizing vulnerability scanning tool (Palmaers 2013; Carnegie Mellon University 2016). Vulnerability management and assessment are often used interchangeably, but at least in the context of this thesis, the terms refer to two different concepts.

Another term that is mentioned in this thesis is patch management, which is the process of identifying, prioritizing, acquiring, installing and verifying the installation of updates and patches on organization's technology assets (Souppaya & Scarfone 2022). This concept is closely related to vulnerability management of IT assets, so it is also an important concept in this thesis.

3 Research methodology

This thesis is conducted as a literature review, aiming to map out the available information on the topic addressing the specified research question. Literature reviews can be categorized into narrative literature reviews, systematic reviews, and quantitative or qualitative meta-analyses. Regardless of the type, literature reviews generally involve the following phases: searching for literature, critically reviewing the literature, and conducting an analysis based on the collected literature (JAMK, 2023).

For this thesis, a qualitative meta-synthesis was identified as the most appropriate method to explore the best practices of vulnerability management. Qualitative meta-synthesis examines similar studies and research on a given topic, providing an overview by identifying similarities and differences among the studies. This method is suitable for this purpose as it can also be applied to non-academic literature (Mannila, 2021; Salminen 2023).

Metasynthesis as a process goes as follows:

1. Defining the topic, research question or problem and objective
2. Finding relevant texts for this purpose
3. Decision what is included in
4. Review of the literature
5. Analysis of the literature, such as examining differences and similarities of these texts
6. Writing synthesis based on analyzed materials.

The objective of metasynthesis is to carefully examine the relevant publications and literature and highlight key concepts which then are compared to each other, trying to find any unifying factors from the literature. In the end, the objective is to unify all the findings from the literature into one synthesis. (Salminen 2023).

In this thesis, qualitative content analysis was employed to examine the literature with the aim of identifying commonalities among vulnerability management publications and articles. Content analysis is a method that involves scrutinizing text-based data to uncover similarities and differences within the analyzed materials and to summarize the findings. The goal of

content analysis is to create a concise summary of the researched phenomenon and contextualize it within a broader framework (Saaranen-Kauppinen & Puusniekka, 2006).

4 Conducting research

When selecting materials for analysis, the Laurea Finna library was utilized, and vulnerability management-related publications from well-known, vendor-agnostic institutions such as SANS, NIST, the Center for Internet Security, Gartner, and OWASP were searched. Additionally, searches were conducted on Google using the keywords 'vulnerability management', 'vulnerability management guide', and 'vulnerability management process'. The focus was placed solely on vendor-agnostic publications that emphasize vulnerability management processes and best practices rather than specific tools. Consequently, articles and publications from known cybersecurity vendors, or those focusing on specific technologies like various vulnerability scanners and their features, were excluded.

Inclusion criteria	**Exclusion criteria**
Freely available	**Fee required**
Publisher vendor-agnostic party / institution	**Vendor published article or publication**
Considers vulnerability management process, or part of it or best practices	**Considers specific technologies related to vulnerability management, such as vulnerability scanners**
E-books, e-articles, white papers, guides	Theses, newspapers

Table 1 Inclusion / Exclusion criteria

Based on inclusion criteria and exclusion criteria, eight publications were chosen for analysis, where each of them had a bit different angle on vulnerability management program or part of it. Below is a table of all publications chosen and what aspects of vulnerability management were examined in each of the publications. Qualitative content analysis was used as an analytical approach for all the publications.

Publication	**Aspect of vulnerability management**

NIST SP 800-40 Revision 4: Guide to Enterprise Patch management planning: Preventive maintenance for technology (2022)	Software vulnerability management lifecycle from preventive perspective
Cybersecurity Tech Basics: Vulnerability management overview (Atkinson 2018)	Overview of cyber vulnerability management program and core processes for decreasing cyber-related risks in organizations.
CRR Supplemental Resource Guide Volume 4: Vulnerability management (Carnegie Mellon University 2016)	Development and implementation of vulnerability management program.
CIS Critical Security Controls Version 8 (2021)	Critical security controls for vulnerability management based on Center for Internet security recommendations.
Gartner's article "How to Set practical time frames to remedy security vulnerabilities' (Moore 2021).	Gartner's recommendations for establishing and implementing effective remediation time frames.
OWASP Vulnerability management guide (2020)	Comprehensive overview of OWASP's approach to repeatable vulnerability management process.
SANS White paper: 'Implementing a Vulnerability management process' (Palmaers 2013)	White paper focusing on how vulnerability management process could be designed and implemented.
Modern Vulnerability Management: Predictive cybersecurity, E-book (Roytman & Bellis 2023)	History of vulnerability management and how to plan and implement risk-based vulnerability management program.

Table 2 Selected literature for analysis

Selected publications were analyzed by examining each of them individually looking for answers for following questions:

- What vulnerability management practices or recommendations can be extracted from the text?

- What are the rationales behind each presented recommendation or best practice?
- How do the examined recommendations or best practices compare to those in other publications? Do other publications support these recommendations, and what are the key similarities or differences?

Results from each of the publication were then compared, summarized and unified into list of best practices were at minimum two separate publications are supporting the best practice to establish list of vulnerability management best practices with rationale why they are considered as best practices and how they support efficient vulnerability management program.

5 Recommendations

Most emphasized theme across the analyzed publications was that vulnerability management activities and recommendations are risk-based. Recommendations were selected based on how well they were supported in the literature but since all publications had a different angle to vulnerability management, many of the best practices and recommendations were not included since they were specific to that single publication. For example, NIST's publication 'Guide to Enterprise Patch management planning' had specific scope for its publication and many of the recommendations were specific to patch management planning and were not covered in other publications and therefore were not included in this list.

Whenever possible, similar recommendations from multiple publications were summarized as one to this list as publications may have same idea but different rationalization for it. For example, how organizations should implement metrics for vulnerability management had different approaches across publications, but bottom line was that meaningful metrics should be implemented for vulnerability management.

5.1 Vulnerability management program must have leadership buy-in

Vulnerability management program to succeed, it requires buy-in and support from leadership since the program itself requires collaboration and engagement of multiple stakeholders and internal teams, depending on the scope (OWASP 2020; Roytman & Bellis 2023). As mentioned in the publications, this may require showing data and highlighting the risks of ineffective or non-existent vulnerability management program for the leadership to gain their support but as leadership can also accelerate the implementation and adoption of vulnerability management program, it is important to do (OWASP 2020; Roytman & Bellis 2023).

5.2 Organization should establish scope for its vulnerability management program.

Many of the publications acknowledges the need of clear scope for vulnerability management program since after all that sets clear boundaries on what are the areas of concern and what assets needs to be in the scope of vulnerability assessment (Carnegie Mellon University 2016). Scope document should consider the organization's capability to perform vulnerability assessment and possible technical constraints (OWASP 2020). For example, an organization's vulnerability assessment tool may not be capable of scanning cloud assets or containers.

5.3 Organizations should align vulnerability management processes with existing internal processes and teams.

Vulnerability management program should be aligned with existing processes and internal teams should be on board and aligned with common objective of vulnerability management program. Every organization may have different objectives for their vulnerability management program but ultimately every team should understand and thrive towards the same goal as this helps everyone understand their role in the big picture (Roytman & Bellis 2023).

As collaboration of different teams is essential, it is also important to align the program with existing processes. Organizations may have regular patching day or window when assets are being patched so vulnerability management team can run assessment and provide vulnerability analysis before that date when they can be remediated (OWASP 2020). In ideal situation, teams would be aligned with one common goal that everyone thrives for, e.g. reducing the overall risk of the organization, with processes and methodology that are aligned across essential teams so the whole vulnerability management process functions efficiently (Roytman & Bellis 2023).

5.4 Organization should define its role and responsibilities regarding vulnerability management.

Organization should define clearly roles and responsibilities regarding its vulnerability management program, including personnel responsible for monitoring and assessing found vulnerabilities, personnel responsible for remediating the vulnerabilities and other necessary roles, like asset owners (Palmaers 2013; Carnegie Mellon University 2016). Since efficient vulnerability management programs in most cases require coordination and collaboration of multiple teams, it is necessary that everyone understands their own responsibilities and accountability is set. This can be for example a RACI chart that defines the roles and responsibilities of different teams.

When any work is assigned, whether it is remediation work, approval of remediation work and what not, work should be always be assigned to some entity or individual, preferably with

deadline so there is clear audit trail for each performed remediation work, usually through some ticketing system for example (OWASP 2020).

5.5 Organization should identify their most essential assets

This is a common recommendation across publications. As priorization efforts should be based on the risk that specific vulnerability poses to an organization, it should understand what assets are most critical to its business and operations (OWASP 2022; Atkinson 2018; Carnegie Mellon University 2016). NIST's Guide to enterprise patch management (2022) and Sean Atkinson (2018) also state that organizations should establish inventory of assets since 'you can't protect assets you do not know you have'. Having inventory of enterprise assets is also highlighted in Center for Internet Security's (2021) Critical Security controls publication. From asset management point of view, organization should further divide those assets into groups based on those technical characteristics, business characteristics, environment and so on (Roytman & Bellis 2023; Souppaya & Scarfone 2022; OWASP 2020),

To summarize this, an organization should have both visibility and understanding of its assets and their criticality to its business and operations. That can be achieved by having inventory of enterprise assets, and as recommended by NIST's guide to enterprise patch management (2022) inventory should also contain information about each asset's technical and business charasteristics, which further help identifying what are the critical assets.

5.6 Organization should conduct regular vulnerability assessment activities

Vulnerability assessments are the cornerstone of a vulnerability management program. Three general ways to assess vulnerabilities in an organization's environment are network vulnerability scans or port scans, authenticated vulnerability scans, and asset inventory. Additionally, methods such as penetration testing or red team engagements can be used. The most effective vulnerability management programs utilize a variety of methods, leveraging the strengths of each method and compensating for their weaknesses with other methods (Carnegie Mellon University 2016; Roytman & Bellis 2023; OWASP 2020).

This is arguably the most important part of the program since here the actual vulnerabilities are identified. But so, this vulnerability assessment works efficiently, organization needs to define right tooling for the vulnerability assessments, what scanning methods are being used for which systems and assets and so on (Palmaers 2013; OWASP 2020).

5.7 Vulnerability priorization should be based on risk.

Based on the literature, organizations should implement a risk-based approach to vulnerability management. Decision over which vulnerability should be remediated next should be based on the risk that vulnerability poses to an organization (Carnegie Mellon University 2016). So that

organization can assess the risk each vulnerability, it needs to understand the information about the vulnerability itself, its assets in the environment, including business criticality and exposure, and possible associated threat intelligence regarding that specific vulnerability. (Roytman & Bellis 2023; Moore 2021). Vulnerability priorization should be aligned with an organization's risk appetite, the amount of risk organization is ready to accept, since that is also key information when deciding what to prioritize (Moore 2021).

Upcoming NIS2 directive (2022) has also acknowledged the potential impact of vulnerabilities and identified swift remediation action of vulnerabilities that may cause significant impact to an organization as an important factor in reducing risk.

5.8 Organization should identify sources of vulnerability information

To support its vulnerability management decision making and remediation work, organization should follow important vulnerability information channels to the organization, for example vulnerability feeds by vendors whose solutions organization is using (Carnegie Mellon University 2016; OWASP 2020). Organization should follow news on new identified zero-day vulnerabilities or other exploited vulnerabilities which may affect organization's operations and more importantly risk levels and use that information on prioritizing remediation work.

5.9 Organization should aim to utilize automation in vulnerability management activities

Automation as part of vulnerability management wasn't covered as widely but a couple publications did cover this area in some way. Bottom line is that organization should aim to automate vulnerability assessment activities, for example performing automated scanning of external and internal systems, and if possible, automate parts of vulnerability analysis activities to improve remediation times (Moore 2021; Center for Internet Security 2021). CIS Critical Controls version 8 (2021) even provides recommendation to automate operating system and application patch management, but that is highly dependent of organization's operational environment since pushing patch to production systems automatically may cause unexpected disruptions or issues.

Additionally, organizations should aim to utilize automation in reporting metrics as much as possible for time-efficiency in measuring performance of the program (Roytman & Bellis 2023). As to what kind of metrics an organization should produce based on literature, those will be covered in the next section.

5.10 Organization should implement meaningful metrics to monitor its vulnerability management program's performance

Meaningful metrics are an important aspect of the vulnerability management program since that provides some sort of sense of the performance of an organization's vulnerability

management. That requires; however, careful thinking of what metrics provide value to the organization and moreover, help organization to make better decisions (Roytman & Bellis 2023).

NIST (2022) recommends an approach where organizations should develop metrics that reflect on the relative importance of each vulnerability. What this means in practice, that instead of reporting the number of vulnerabilities patched, metrics should communicate on for example mitigation metrics based on relative importance of the asset and vulnerability, like in the picture below:

Vulnerability Importance	Asset Importance		
	Low	Moderate	High
Low	By deadline: 64.7 % Average time: 80.4 days Median time: 75.2 days	By deadline: 72.4 % Average time: 34.7 days Median time: 33.7 days	By deadline: 85.0 % Average time: 14.6 days Median time: 8.1 days
Medium	By deadline: 66.5 % Average time: 75.1 days Median time: 70.7 days	By deadline: 68.7 % Average time: 33.2 days Median time: 31.6 days	By deadline: 71.4 % Average time: 12.9 days Median time: 10.5 days
High	By deadline: 68.6 % Average time: 62.1 days Median time: 58.0 days	By deadline: 78.8 % Average time: 26.8 days Median time: 22.1 days	By deadline: 85.5 % Average time: 8.8 days Median time: 8.1 days
Critical	By deadline: 81.4 % Average time: 44.4 days Median time: 41.3 days	By deadline: 92.3 % Average time: 21.2 days Median time: 23.9 days	By deadline: 95.2 % Average time: 5.2 days Median time: 5.1 days

Figure 1 Vulnerability Mitigation Time Summary Matrix (Souppaya & Scarfone 2022).

Roytman and Bellis (2023) also argue in their book 'Modern vulnerability management' that even that metrics should improve when organization takes right actions, driving the numbers up should not be the priority. The goal should be to lower the organization's risk and metrics just provide information on how well the organization is doing.

OWASP's guide (2020) does acknowledge that organization should use KPIs that matter to the organization's risk and compliance as well but provides more generic guidance on those meant metrics such as number of new vulnerabilities and amount of vulnerable assets but emphasizes more on aggregating the vulnerability data based on severity, CVSS, type of environment, maintenance group, type of vulnerability and so on.

Bottom line is that organizations should identify and implement metrics that matter to the organization's risk and compliance. Organization may benefit from having very granular reporting based on different environments, assets, severity if that allows organization to more effectively prioritize remediation work and drive down the overall risk of the organization. By examining the publications, consensus is that risk-based approach for reporting should be implemented as well, numbers should reflect on how well organization is prioritizing and managing vulnerabilities and thus lowering the risk they pose.

6 Conclusion

This thesis achieves its objective of providing a list of vulnerability management recommendations based on literature review. Results did not provide particularly new information, more summarized recommendations that were supported by multiple publications, so the list is not comprehensive. Since all the selected publications had slightly different angle to vulnerability management, there were multiple recommendations that weren't covered in other publications and therefore did not get included to the list of recommendations presented in this thesis.

A list of recommendations could be utilized to review existing vulnerability management programs or processes and evaluate whether improvements are needed. It can also provide some information for organizations starting to implement their vulnerability management program to see what is considered important across a variety of literature.

As this thesis aims to cover the entire vulnerability management lifecycle, challenges for further research could include more focused literature reviews on specific aspects of vulnerability management, such as assessment, remediation, or patch management. Since automation and the use of AI in vulnerability management were not extensively covered, these could also be interesting topics for future research.

References

Digital

Atkinson, S. 2018. Cybersecurity Tech basics: Vulnerability management overview. Practical Law. PDF. Referred to 23.10.2024. https://www.cisecurity.org/-/media/project/cisecurity/cisecurity/data/media/files/uploads/2018/07/Cybersecurity-Tech-Basics-Vulnerability-Management-Overview.pdf

Carnegie Mellon University. 2016. CRR Supplemental Resource guide Volume 4: Vulnerability management. Referred to 3.10.2024. https://www.cisa.gov/sites/default/files/publications/CRR_Resource_Guide-VM_0.pdf

Center for Internet Security. 2021. CIS Critical Security Controls version 8. Referred to 23.10.2024. https://learn.cisecurity.org/CIS-Controls-v8-guide-pdf

CISA. 2024. 2023 Top Routinely exploited vulnerabilities. Referred to 20.11.2024. https://www.cisa.gov/sites/default/files/2024-11/aa24-317a-2023-top-routinely-exploited-vulnerabilities.pdf

European Union. 2022. DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. Referred to 23.9.2024. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555&from=EN

JAMK. 2023. Kirjallisuuskatsaukset. Referred to 23.9.2024. https://help.jamk.fi/opinnaytetyon-ohjaus/fi/kirjallisuuskatsaukset/

Mannila, M. 2021. Kirjallisuuskatsaus opinnäytetyön muotona. Energiaa – Vaasan ammattikorkeakoulun verkkolehti. Referred to 23.9.2024. https://energiaa.vamk.fi/artikkelit/osaaminen/kirjallisuuskatsaus-opinnaytetyon-muotona/

OWASP. 2020. OWASP Vulnerability management guide. Referred to 23.10.2024. https://owasp.org/www-project-vulnerability-management-guide/OWASP-Vuln-Mgm-Guide-Jul23-2020.pdf

Palmaers, T. 2013. Implementing a Vulnerability management process. SANS Institute. Referred to 3.10.2024. https://sansorg.egnyte.com/dl/2IL7fioFhM

Panetta, K. 2021. Gartner Top 10 Security projects for 2020-2021. Gartner. Referred to 21.11.2024. https://www.gartner.com/smarterwithgartner/gartner-top-security-projects-for-2020-2021

Roytman, M. & Bellis, E. 2023. Modern vulnerability management: Predictive Cybersecurity. E-book. Referred to 11.11.2024.

Saaranen-Kauppinen, A. & Puusniekka, A. 2006. KvaliMOTV - Menetelmäopetuksen tietovaranto [verkkojulkaisu]. Tampere: Yhteiskuntatieteellinen tietoarkisto. Referred to 7.12.2024. https://www.fsd.tuni.fi/menetelmaopetus/kvali/L7_3_2.html

Salminen, A. 2023. Mikä kirjallisuuskatsaus? Johdatus kirjallisuuskatsauksen tyyppeihin ja joihinkin hallintotieteellisiin sovelluksiin. Vaasan yliopisto. Referred to 23.9.2024. https://osuva.uwasa.fi/bitstream/handle/10024/15470/978-952-395-081-8%20(PDF).pdf?sequence=2

Souppaya, M & Scarfone, K. 2022. Guide to Enterprise patch management planning. NIST. Referred to 3.10.2024. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r4.pdf