BEST PRACTICES FOR VULNERABILITY MANAGEMENT IN LARGE ENTERPRISES: A CRITICAL VIEW ON THE COMMON VULNERABILITY SCORING SYSTEM

JAQUELINE HANS & ROMAN BRANDTWEINER
Vienna University of Economics and Business, Austria

ABSTRACT

Over the past decade, enterprises have been increasingly suffering from attacks conducted by cybercriminals. Potential losses are not only reflected on their revenue or stolen data, but also on their damaged reputation. Most often, these attacks were possible due to the successful exploitation of vulnerabilities within the company's system. Many of such attacks could have been mitigated, if responsible actors took the right actions related to the management of such vulnerabilities. This paper aims to summarize good practices regarding vulnerability management, with essential focus on the matter of prioritization. For this, several vulnerability scoring systems such as the Common Vulnerability Scoring System were analyzed according to the way they are portrayed in scientific literature. It will also analyze non-technical, human factors as well by reflecting on organizational aspects. The aim is to provide an overview about the options large enterprises have in this regard and to inform about potential consequences they could face. It will also reflect on the problematic behind the trade-off between investing enough in a cybersecurity foundation, while simultaneously remaining profitable.

Keywords: cybersecurity, e-security, vulnerability scoring system, CVSS, vulnerability management.

1 INTRODUCTION

Due to the increasing digital reliance, enterprises are constantly exposed to the vulnerabilities of their systems. Especially large corporations encounter an incredible number of vulnerabilities on a daily basis and, at some point, struggle to categorize these vulnerabilities prioritize the elimination of those. Automated processes can be a very efficient way to quickly assess the severity of each vulnerability, but most approaches still lack accuracy and trustworthiness. Especially the Common Vulnerability Scoring System (CVSS), is a widely used and accepted standard [1]. However, there is a large disagreement within cybersecurity experts whether using this standard alone should be considered a good practice or even is reliable at all [2]. This arises the question whether and how the CVSS could be improved, if it should be complemented by alternative practices, or if it should not be used at all. Furthermore, it should be reflected on whether vulnerability management is a question of technological kind alone or whether there are several human and organizational factors influencing this matter as well [3].

This literature synthesis aims to provide a summary that does not focus on certain algorithms and methodologies alone, but aims to create a big picture, cybersecurity researchers and practitioners can build upon and derive implications from. In the first section, the context of vulnerability management in large enterprises is explained by emphasizing the consequences of vulnerability exploitations and analysing this topic on the surface. The following section deals with vulnerability prioritization and scoring systems such as CVSS by reflecting on its scope and responsibilities, and by comparing it to different models. Lastly, the final section deals with complementary or alternative approaches and viewpoints which do not necessarily relate to severity scoring alone but might be a good integration to vulnerability management processes in general.

WIT Transactions on The Built Environment, Vol 214, © 2022 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/SSR220101

2 METHODOLOGY AND RESEARCH DESIGN

The methodology applied for this study is a systematic literature review. Hence, the foundation of this research is primary literature found in several digital databases. The aim is to include as many findings as possible in order to obtain a large number of insights regarding vulnerability management in enterprises by including the perspective of cybersecurity researchers as well.

2.1 Quality criteria

The selection of the primary literature is based on several quality criteria: The first criterium is accessibility, which means that a full-text version of each source should at least be available within the WU library network. WU stands for "Wirtschaftsuniversität" (University of Economics and Business) that is the name of our university, i.e. we used this specific library network for our research. The second criterium is that all sources need to be peer-reviewed as this ensures an acceptable amount of trustworthiness and correctness of information. Also acceptable are resources that were published by official sources such as FIRST.org, the creators of the CVSS, Tripwire, OWASP, and NIST. Lastly, the final criterium is relevance. That means that the primary literature must be relevant according to the topic it addresses, but also according to the date it was published.

2.2 Database search and literature screening

The WU library network, which is our main source for finding primary literature, refers to the WU library catalogue and the WU library cataloguePLUS including other digital databases that allow full-text access such as Springer, IEEE, EBSCO, ProQuest, Wiley Online Library, and ScienceDirect. Within these databases, resources were filtered by the following keywords.

General keywords: Vulnerability management, threat management, system vulnerability, network vulnerability, cybersecurity risk management, vulnerability assessment, vulnerability prioritization, patch management, vulnerability severity scoring.

Specific keywords: CVSS, Common Vulnerability Scoring System, FIRST, base metric, temporal metric, environmental metric, Tripwire IP360, Tripwire Vulnerability Scoring System, OWASP Risk Rating Methodology, OWASP Vulnerability Scoring.

The search results based on the aforementioned keywords were further screened based on title, abstract, content, and selected under fulfilment of the previously defined quality criteria: 134 elements were selected, based on title of the paper from these 134 articles 59 were selected based on the content of the abstract and out of them 11 elements were selected based on content and quality criteria. Those 11 articles were the final sample of the study.

3 RESEARCH AIM AND OBJECTIVES

The aim of this systematic literature review is to provide new insights regarding best practices of vulnerability management in enterprises as well as to reflect on the CVSS by analysing as much primary literature as possible. The final deliverable should be a summary that not only highlights the key findings but also the implications they have for future research and practice. Hence, the paper further aims to identify potential research gaps as well.

While there are many papers that introduce certain models for vulnerability prioritization or reflect on certain frameworks alone, the subject of vulnerability management is lacking research contributions that summarize, compare, and reflect on them simultaneously and, hence, provide an overview of many existing, yet unknown solutions. This paper summarizes

good practices, reflects on widely used standards, and aims to introduce new ways of thinking about vulnerability management by paying not only attention to the technical details but also taking financial and organizational factors into consideration. This paper is guided by three specific research questions (RQ):

- RQ1: What is the scope of vulnerability management and what are contemporary issues and consequences enterprises face?
- RQ2: Is the widely accepted CVSS accurate, trustworthy, and reliable? How could it be improved?
- RQ3: What other factors and methodologies should be considered when it comes to vulnerability prioritization? Are there any alternative practices that could or should complement vulnerability severity scoring systems?

4 THE CONTEXT OF VULNERABILITY MANAGEMENT IN ENTERPRISES

In order to dive in into the importance of vulnerability management in enterprises, it is important to obtain an understanding of how the term "vulnerability" is defined. According to Sukaina Bhawani, a senior researcher at the Stockholm Environment Institute, the term vulnerability is referred to as "capacity to be wounded, i.e., the degree to which a system is likely to experience harm due to exposure to a hazard" [4].

While the definition's origin lies within the fields of geography and natural hazards, the concept of it has become applicable for other areas of research as well. Due to the wide range of different disciplines, several definitions have been established based on precisely determined factors such as key attributes, exposure units, and decision scale. Key attributes can be the capacity, sensitivity, and the exposure of such systems. The exposure units relate to the units that are affected by a potential exploitation. This can be individuals, groups of people, but also systems and other units. The decision scale, in its basic definition, mostly refers to the regional scope an exploitation would have [4].

A definition by Haimes, that relates more to the risks infrastructures and nations are exposed to, states that vulnerability interacts with other parameters such as intent, capability, threat, and risk. He underlines that risk modelling needs an integration of these parameters in order to understand the targeted infrastructure based on internal factors such as the current system's state and external factors such as the patterns of criminals selecting their targets [5].

This primarily refers to vulnerabilities/risks of nations' infrastructures. However, it is crucial to understand the similarities and differences between general vulnerability definitions such as the one by Bhawani, and more narrowed-down definitions such as the one of Haimes. This creates a broader understanding about the context of vulnerabilities that enterprises are exposed to due to their IT infrastructure.

Considering that this paper aims to primarily address the term vulnerability in the field of cybersecurity, this term will mostly refer to the exploitability of certain parts of IT systems and networks. However, it is important to recognize that these vulnerabilities also come along with several other consequences for companies, resulting in additional vulnerabilities with other key attributes, exposure units, and decision scales. A successful cyber attack does not only harm IT systems or networks, but it could also potentially harm the company and its stakeholders as well. Furthermore, victims could experience losses in terms of their data, their reputation, or their revenue.

Data that was gathered by Statista, and published by Accenture reveals the consequences of cyber-attacks global companies had to suffer from in 2018. According to the study, companies suffered from an annual average loss of US$5.9 million caused by information loss, US$4 million caused by business disruption, US$2.6 million caused by equipment

damages, and US$0.5 million of revenue loss [6]. Another survey, that collected data from 522 cybersecurity practitioners, reported an average loss of US$288,618 caused by the successful exploitation of computer security vulnerabilities [3]. Considering the exponential growth of digital reliance and IT infrastructures, these numbers can be expected to significantly rise in the upcoming years.

The context of vulnerability management in institutions is further analyzed in a systematic literature review conducted by Uddin et al. [7]. During their analysis of various primary literature sources, they were able to discover essential research gaps and implications. The first research gap they discovered is the lack of knowledge regarding the relationship between operating costs and the exploitation of vulnerabilities. While most institutions understand that it is important to invest a certain amount of money regularly in their cybersecurity infrastructure, they sometimes lack information regarding a budget that is sufficient to achieve the best possible protection and at the same time does not immensely affect the financial return that most managerial decision making is based on. Although there are several policies and guidelines that determine a few of these decisions upfront, they are still considered being too ad-hoc and not fully reliable [7]. Nonetheless, the issue about an appropriate budget remains highly important. According to a pervious study, a lack of funding is, among other organizational factors, a primary non-technical cause of vulnerability exploitation [3].

As can be drawn from these findings, best practices regarding vulnerability management are not easily determined. This is due to enterprises' lack of understanding regarding the vulnerabilities within their systems and the meaning of the term "vulnerability" and its consequences in general. Furthermore, policies and guidelines are not precise enough frameworks to provide them with clear instructions regarding budgeting decisions as well as methods for appropriate vulnerability assessments. While the whole subject itself involves several research gaps and requires various policy adjustments, the following section of this paper aims to look at vulnerability management more precisely, paying essential detail to the prioritization of vulnerabilities by comparing several standards and practices.

5 THE CONTEXT OF VULNERABILITY MANAGEMENT IN ENTERPRISES

The following section will give an outline about the partly automized processes of vulnerability severity scoring. The aim is to define the scope of severity scoring systems by also reflecting on their performance, risks, and responsibilities.

5.1 CVSS

The most frequently used system of vulnerability severity scoring is the CVSS. Despite being criticized to some extent, CVSS has become an accepted standard when it comes to the scoring of vulnerability severities. Within the US National Vulnerability Database, all vulnerabilities are scored based on CVSS and also in many more areas, it is visible that this system seems to be the predominant methodology for vulnerability scoring [2].

The CVSS has been originated by FIRST, an organization that aims to improve incident response and other Internet security related operations. In their mission statement, the organization emphasizes its global position and reach around the globe [8].

Based on the official documentation, it can be noted that the CVSS' primary aim is to assess a vulnerability's severity and reflect on it based on a numerical score it produces. This score reaches from 0 to 10, where 0 represents a vulnerability of very low severity, and 10 represents a vulnerability of high severity and criticality. What should be additionally noted is that the score assigned to each vulnerability is relative to other vulnerabilities' severities

[9]. By this, the CVSS aims to support enterprises and other groups of interest with the prioritization of such vulnerabilities. Considering that the FIRST organization is constantly evolving and improving this severity scoring system, three main versions of it have been established over the years. This paper will, hence, mostly refer to the current version of CVSS, being CVSS v.3.1.

While this paper does not intent to analyse the mechanisms behind the CVSS in close detail, it is important to achieve a basic understanding of what it does and essentially to give an overview about its aim, purpose, and use case.

Simplified, the CVSS is composed of three main metric groups. The first metric group, the base metric group, contains metrics such as the attack vector, privileges required, the scope, or its impact regarding confidentiality, integrity, and availability. Within the base metric group there are also two subgroups, one referring to exploitability and the other one referring to the impact. While the other metric groups are considered optional groups, the base metric group is essential for determining the final severity score as it is constant over time and across user environments. The temporal metric group, on the other hand, does change over time, but not across user environments. Lastly, the environmental metric group refers to metrics that are tailored to the specific user's environment [9]. Summarizing, it can be said that the base metric provides an objective way of assessing vulnerability severities relative to other vulnerabilities, while the optional metric groups enable the user to adjust the scoring based on its unique characteristics.

Capturing these facts is very important when reflecting on some of the critique that CVSS is exposed to. The CVSS has been partly criticized for not sufficiently reflecting on individual and unique characteristics of vulnerabilities that are varying for each organization [2].

While it can be debated on whether the two optional metric groups are portraying these characteristics accurately, it should be noted that during the evolvement of CVSS, the FIRST organization has included additional metrics and accordingly adjusted them to make the assessment of vulnerabilities more individual and, therefore, the scoring more reliable and tailored to the IT infrastructure of the according environment. Hence, it can be assumed that FIRST is aware of potentially missing characteristics and is steadily improving, taking criticism by researchers and practitioners into consideration.

Furthermore, it has to be noted that by the time this paper is written, FIRST has distanced themselves from being entirely responsible for the vulnerability management processes of an organization. On their website, they state that factors such as risks regarding monetary losses or customer being affected by a breach go beyond the scope of CVSS and, therefore, CVSS can only give useful inputs and should not be used alone, but rather as a complementary methodology. The CVSS aims to measure severity and not risk and FIRST acknowledges that CVSS is only an addition to an existing, contextual risk assessment of an IT environment [10].

Reflecting once again on the different metric groups, FIRST suggests that the base score and the temporal score should be conducted by the assigned security professional/analyst, whereas the environmental score is determined by the end-user, for instance, a system administrator. However, while it is good that these various metrics and metric groups exist, they seem to be not much used in practice [2]. In a different study, the assessment difficulty of CVSS' environmental metrics was further analysed. In this controlled experiment that was conducted with the participation of 29 MSc students, the results revealed that for different states and variations of the network layout, the severity assessment using CVSS gets increasingly difficult. This also applies for the configuration of the network, indicating that on a system level, the correctness of the scoring might be impacted [11].

Furthermore, critics claim that the CVSS base score is still relatively unexplored and that its accuracy, whether it be due to overlooked factors or errors in the mathematical formula, is not yet fully proven. Nonetheless, determining the actual severity compared to the severity assigned by CVSS or other systems is a difficult matter. Previous studies tried to improve it using various approaches. Some approaches would additionally measure the time it would take to exploit the vulnerabilities, or by specifically looking at those vulnerabilities that are exploited in practice. These approaches, however, could also be seen as flawed due to many factors that are involved and that do not necessary indicate a higher severity by default [2].

Another method of analysing this subject is, hence, the conduction of expert interviews in which cybersecurity professionals estimate the severity for some vulnerabilities which is then compared to the severity score indicated by the CVSS. The results of one study revealed that some experts indeed assign different values to the vulnerabilities than the CVSS base score. It even claims, that these size of the variance goes beyond a level that actual users of the CVSS would feel comfortable with. According to this study, especially XXS (cross-site-scripting) vulnerabilities received a comparatively too low base score, and SQL injection vulnerabilities received a relatively high base score [2]. However, it should be noted that this particular study was carried out a while back and examined the CVSS v2 and, therefore, could possibly deliver different results if it was conducted nowadays, considering that the CVSS is steadily evolving and improving.

Another, more recent study conducted a survey with students and professionals, estimating vulnerabilities' severity using the methodology by CVSS v.3. The main findings of this study revealed that vulnerability severity scores very much depend on the accessor, even if an industry standard such as CVSS is being used or a very experienced accessor is conducting the scoring [12]. It implies, that using CVSS methodology is not enough, and that the accessor and the people responsible for vulnerability management should not fully rely on the scores depicted by systems and prioritize vulnerabilities also according to the assets and the corporate value that is at stake. This also aligns with the previously mentioned statement by the developers of CVSS, stating that using CVSS alone is not enough for a successful and secure vulnerability management.

A recent paper summarized some potential improvements for CVSS that were proposed in other scientific literature. One method excluded subjective factors of CVSS, however, failed to include the importance of the asset. Another method included a distribution model for evaluating the complexity of an exploitation and the availability of an appropriate way to patch the according vulnerability. However, this methodology failed to consider the affected asset as well. Also, the other two examples that were mentioned did not manage to improve the CVSS properly [13]. This indicates that even small improvements of the CVSS are not easily made.

Summarizing, it can be noted that the CVSS is a widely accepted approach and even considered an industry standard despite having its flaws and being criticized. However, it should be emphasized that the developers of CVSS are constantly evolving and improving this system in order to fulfil the expectations of its users and the responsibilities they indirectly might carry. Furthermore, it should be emphasized that the responsibility also lies within the correct behaviour of the user and within vulnerability managers making the final and appropriate prioritization decisions.

The following section will introduce alternative systems to the CVSS such as the Tripwire score that was created by a specialised company, and vulnerability systems based on open-source communities such as OWASP. The later discussion will compare these different methods and reflect on the scope and responsibilities of such scoring systems.

5.2 Alternative systems

Despite the fact that CVSS scoring is the predominant approach and even considered an industry standard, several organizations and companies have come up with their own methodology for the severity scoring of vulnerabilities. This section will primarily reflect on the solutions offered by Tripwire, a specialized company in the field of vulnerability management, and OWASP, an open-source community for cybersecurity related issues. The choice for these solutions is based on its popularity within the sector and the fact, that it has been mentioned in scientific literature as well [12].

The first alternative the section aims to reflect on is the vulnerability scoring system by Tripwire within their vulnerability management solution known as Tripwire IP360. Tripwire is a specialized company within the field of cybersecurity that offers, apart from their vulnerability management product line, cybersecurity related solutions such as enterprise security foundations and cloud-based infrastructures. It has to be noted that their vulnerability scoring system is based on the CVSS, however, includes additional user specific metrics in order to make the prioritization of vulnerabilities more tailored to the customer's environment. They note that especially large enterprises might suffer from many vulnerabilities with a critical CVSS score what makes the prioritization, despite using an industry standard, incredibly difficult [14]. The Tripwire Vulnerability Scoring System should, hence, not be seen as an alternative, but rather a separate product that makes use of CVSS and adds further information and advanced tools to this methodology. The determination of the risk is clustered into three main categories, so-called parameters being "Risk Class", "Skill Level", and "Vulnerability Age". Risk Class reflects on the potential consequences an exploitation of the vulnerability would have, the user involvement that is required, and, finally, the importance of the target application. Skill Level refers to the difficulty of a potential exploitation based on the availability of potential exploit methods. Lastly, Vulnerability Age refers to old, but well-known vulnerabilities as those are at greater risk to being exploited by automated malware tools. The Tripwire Vulnerability Scoring System is a complement to the CVSS, it is possible that even though all vulnerabilities received the same (critical) score based on the CVSS methodology, the severity of them varies according to the Tripwire Vulnerability Scoring System [15].

Overall, it can be noted that Tripwire provides additional accuracy to the CVSS within their own vulnerability scoring system. It further provides additional value and protection as well as it might result in a more successful vulnerability management. However, these features and tools are not free of charge, indicating that the more companies are willing to pay for their security, the greater the protection they receive. This relates to the points mentioned in the previous section about the context of vulnerability management in large enterprises and the unclear knowledge about cybersecurity budgeting decisions. In order to explore open-source versions of similar tools, the following paragraphs will analyse the solutions offered by the OWASP community.

While there is no explicit information available for a vulnerability scoring system made by OWASP, they, however, came up with an overall Risk Rating Methodology. This approach is split into six steps, with the fourth step labelled "Determining Severity of the Risk". Although it is important to view this rating methodology as a whole model that builds upon each step, this paper will precisely look at the particular step that refers to severity scoring. During this step, the user is required to combine the estimates of the likelihood of exploitation and the ones of the potential impact [16].

Important is the word "estimates", emphasizing that the risk rating methodology is rather a guide or methodology instead of an automized tool. Considering that this approach is

followed by using manual estimates, it is very likely that the accuracy might be lower than the one provided within the Tripwire Scoring System. Furthermore, it does not provide an automized tool which could be necessary for large enterprises encountering lots of vulnerabilities on a frequent basis. However, an essential key aspect is its free usage. Similar to CVSS, the OWASP Risk Rating Methodology is free of charge, and definitely a better solution than not providing any risk methodology at all.

Another important benefit of using the OWASP methodology, compared to the one proposed by FIRST, is its simplicity, considering that there are less metrics/parameters involved for estimating the severity. Furthermore, it takes business factors more into consideration than technical ones, proposing a methodology that is more tailored to the enterprise that uses it. It also includes factors that are not included in the CVSS base score at all [13]. Considering these factors, OWASP might provide a good alternative to the most commonly used CVSS.

6 ORGANIZATIONAL FACTORS AND GOOD PRACTICES

While optimizing the technical operations of vulnerability management is an important task, managers should not underestimate the influence of human and organizational factors. To analyze these factors, common "pathways" to vulnerabilities [3] as well as patch management as a practice was included. These aspects were then reflected within the broader context of ISMS (Information Security Management Systems) which can be viewed as a process or cycle of the cybersecurity program of an organization [17].

There is a common saying that within the field of cybersecurity, the greatest vulnerability are humans. Although it has to be acknowledged that these vulnerabilities are most often interlinked with technological flaws as well, the key point of this statement might be true. These vulnerabilities can be things such as weak password choices, but also errors within organizational policies, incorrect managerial decision making, or a lack of cybersecurity related awareness within the organization. In fact, studies revealed that these aspects might even be correlated with each other. For instance, secure password choices are often correlated with a sufficient amount of awareness training. Another research also suggested that high workload and difficult tasks could negatively affect system states and performance as the appearance of human-errors becomes more likely [3].

Apart from general pathways to vulnerabilities, vulnerability management can also be addressed on a process level and within the context of Information Security Management Systems (ISMS). In this context, the aforementioned policy aspect carries an essential role and is not only a potential pathway to vulnerabilities, but also overall an important element of vulnerability management. Policies define the responsibilities and accountabilities and in order to retain their role as a strategic element, they not only need to be constantly evaluated and adjusted, but also communicated clearly. Further, tactical elements of vulnerability management include guidelines, processes, communication, the development of a plan, and patch management [17]. A document that was published by the National Institute of Standards and Technology (NIST) contains guidelines regarding patch management that enterprises should follow. It states that timing plays an immense role due to the limited resources of enterprises. Especially when it comes to the issue of prioritization, this aspect is of significant relevance. Considering that each patch should be tested before being deployed, the conflict between these three factors is not easily solved and, therefore, should be carefully considered when planning and executing the organization's vulnerability management program. While the document also refers to vulnerability scoring, it has to be noted that this is only a fraction of the whole matter of vulnerability prioritization and management [18]. Another paper that approached patch management by conducting a literature synthesis, also

concluded that in terms of prioritization, enterprises should make decisions not only based on the according scores, but also on the context as this would result in a more accurate depiction of the overall risk [19].

Based on these arguments, it would be wrong to put the blame on organizations such as FIRST for not being able to develop the perfect severity scoring methodology that does all the work in an automized way. This would be a rather utopian way of approaching this matter. Good practices for vulnerability management involve more than technological aspects. Policies, awareness, and the correct measurements taken by non-cybersecurity managers are most likely as important. Furthermore, it should not be seen as separate tasks, but rather as a co-existence between technological methodologies, budgeting decisions, and organizational aspects.

7 DISCUSSION

The following discussion will reflect on both the CVSS and the alternative methods stated such as the Tripwire Vulnerability Scoring System and the OWASP Risk Rating Methodology by also reflecting on the role of the right budgeting decisions and organizational factors.

What can be drawn from the analysis is that the CVSS is the most-widely used methodology for calculating the severity of vulnerabilities. Furthermore, it is free to use and has a pioneering role for other vulnerability scoring systems such as the one by Tripwire. While it is, to some extent, criticized for not including relevant, organizational factors, the organization FIRST clearly emphasized within their user guide that the CVSS should not be used on its own and is not enough for a secure vulnerability management. Furthermore, the CVSS is steadily improving and updated with each new version that is introduced. However, there remains the question whether it is the CVSS' responsibility, as an industry standard, to meet the expectations of its users, considering that tools such as the Tripwire Vulnerability Scoring System seem to be able to provide more accurate results and that the need for accurate vulnerability management, especially in large enterprises, is significantly increasing.

Another point, that builds upon what was written in Section 3, deals with the question about the right budget. Vulnerability management is only a very small fraction of a functioning cybersecurity foundation and enterprises could be overwhelmed by all the optimizing options that exist. For instance, enterprises could manage their vulnerabilities using CVSS only, or by estimating it according to the risk rating methodology by OWASP. However, this would require experts using these methodologies and accordingly make the right decisions using this input. Also, if there is a large number of vulnerabilities, manual estimations and the according prioritization is burdensome. Alternatively, they could invest in solutions such as the one by Tripwire where they profit by more accuracy and automized processes. While Tripwire would most likely bring the most efficient results, enterprises need to make an appropriate decision: Investing enough in their vulnerability management, being in automized software or the right people, while simultaneously remaining profitable. Similar to other risk-related topics, there is this trade-off between the losses that could potentially arise due to these vulnerabilities being successfully exploited, and the expenses that arise when trying to mitigate the risk as much as possible.

While these technological and financial factors need to be considered, there are many other, organizational and human factors that influence the exploitation of vulnerabilities and potential attacks which should not be underestimated. The findings regarding the correlation between training, policies, and vulnerability exploitation, hence, suggest that vulnerability management is a more complex process than the optimization of severity scoring based on a

mathematical formula. The responsibility lies not only within cybersecurity professionals developing appropriate and accurate systems, but also within managers and employees, knowing the value of their assets and the potential consequences of their vulnerabilities. The findings further revealed that even the subject of patch management, which is only a fraction of vulnerability management, is a rather complex issue as well and involves more factors such as timing, prioritization, and testing.

8 LIMITATIONS

The first limitation of this paper is its imbalance between the reflection of vulnerability severity scoring systems and the one about organizational and financial factors. During the research, it seemed that the CVSS and its alternatives have a predominant role and are frequently appearing in research papers when it comes to best practices regarding vulnerability management. Also, a lack of direct comparisons between these systems could be discovered, making a judgement based on scientific literature regarding the "best" system increasingly difficult. The main objectives such as reflecting on the CVSS could be fulfilled, however, the paper failed to provide a complete summary of most methods existing. This might be due to the fact that the field of vulnerability management involves too many factors that cannot be captured within a paper of this size without taking away necessary, detailed information.

9 IMPLICATIONS FOR FUTURE RESEARCH

The paper suggests that there is a lack of a detailed comparison and exploration of existing vulnerability scoring systems, supporting especially large enterprises at choosing an appropriate mean for handling their vulnerability management. It implies, that organizational and budget-related decisions have equal importance, and that the latter aspect seems to be a particularly unclear task for most companies. The question regarding best practices of vulnerability management should be covered as a whole, providing enterprises with essential information about severity scoring methodologies, asset prioritization, patch management practices, a sufficient cybersecurity budget, and the importance of training and policies.

10 CONCLUSION

Overall, there is no doubt that vulnerability management has an important role within the cybersecurity program of large enterprises. What could be discovered during the research, is that companies might struggle to quantify and prioritize their vulnerabilities properly due to the fact that there are many factors that need to be taken into consideration. While methodologies such as the CVSS and the OWASP Risk Rating Methodology remain reliable, free-of-charge solutions, risk-minimizing goals require enterprises to invest into the right people, processes and, ideally, automized software to support them at quantifying their vulnerabilities' severity. Although risk scoring is an important part in vulnerability management, it has to be noted that these methodologies might not take crucial factors into consideration. Despite the fact that these solutions are constantly improving and becoming more and more accurate, organizational factors influence this matter a lot as well. Aspects such as policies, risk related awareness, and communication play a crucial role and come along with benefits that severity scorings alone sometimes fail to provide. Therefore, the findings of this paper suggest an alignment of all these factors, indicating that the application of vulnerability scorings is an important part, however, not sufficient if used on its own. More precisely, vulnerability scoring systems should be embedded within well-designed processes and patch management programs, by taking into account the respective assets.

REFERENCES

[1] Kekül, H., Ergen, B. & Arslan, H., A multiclass hybrid approach to estimating software vulnerability vectors and severity score. *Journal of Information Security and Applications*, **63**, 103028, 2021. DOI: 10.1016/j.jisa.2021.103028.

[2] Holm, H. & Afridi, K., An expert-based investigation of the Common Vulnerability Scoring System. *Computers and Security*, **53**, pp. 18–30, 2015. DOI: 10.1016/j.cose.2015.04.012.

[3] Kraemer, S., Carayon, P. & Clem, J., Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computers and Security*, **28**(7), pp. 509–520, 2009. DOI: 10.1016/j.cose.2009.04.006.

[4] Bharwani, S., Vulnerability definitions. 2020. https://www.weadapt.org/knowledge-base/vulnerability/vulnerabilitydefinitions. Accessed on: 20 Nov. 2021.

[5] Haimes, Y., On the definition of vulnerabilities in measuring risks to infrastructures. *Risk Analysis*, **26**(2), pp. 293–296, 2006. DOI: 10.1111/j.1539-6924.2006.00755.x.

[6] Statista, published by Accenture, Average annual costs for external consequences of cyber attacks on global companies in 2018, 2018. https://www.statista.com/statistics/241255/main-consequences-of-cyber-attacks-in-selected-countries. Accessed on: 20 Nov. 2021.

[7] Uddin, H., Hamid, A. & Hassan, M., Cybersecurity hazards and financial system vulnerability: A synthesis of literature. *Risk Management*, **22**(4), pp. 239–309, 2020. DOI: 10.1057/s41283-020-00063-2.

[8] FIRST, Mission Statement, 2021. https://www.first.org/about/mission. Accessed on: 20 Jan. 2022.

[9] FIRST, Common Vulnerability Scoring System v.3.1: Specification Document – Revision 1, 2021. https://www.first.org/cvss/v3.1/specification-document. Accessed on: 17 Jan. 2022.

[10] FIRST, Common Vulnerability Scoring System: User Guide, 2021. https://www.first.org/cvss/user-guide. Accessed on 17. January 2022.

[11] Allodi, L., Biagioni, S., Crispo, B., Labunets, K., Massacci, F. & Santos, W., Estimating the assessment difficulty of CVSS environmental metrics: An experiment. *Future Data and Security Engineering*, **10646**, Springer: Cham, pp. 23–39, 2017. DOI: 10.1007/978-3-319-70004-5_2.

[12] Allodi, L., Cremonini, M., Massacci, F. & Shim, W., Measuring the accuracy of software vulnerability assessments: Experiments with students and professionals. *Empirical Software Engineering*, **25**(2), pp. 1063–1094, 2020. DOI: 10.1007/s10664-019-09797-4.

[13] Pecl, D., Safonov, Y., Martinasek, Z., Kacic, M., Almer, L. & Malina, L., Manager asks: Which vulnerability must be eliminated first? *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, **12596**, pp. 146–164, 2021. DOI: 10.1007/978-3-030-69255-1_10.

[14] Khimji, I. published via Tripwire, Tripwire vulnerability risk metrics: Connecting security to the business, 2019. https://www.tripwire.com/-/media/tripwiredotcom/files/white-paper/tripwire_vulnerability_risk_metrics_white_paper.pdf?rev=7d6ee34728c24342811273edc cc69619. Accessed on: 20 Jan. 2022.

[15] Tripwire, Advanced vulnerability risk scoring and prioritization, 2019. https://www.tripwire.com/-/media/tripwiredotcom/files/solution-brief/tripwire_advanced_vulnerability_risk_scoring_and_prioritization_solution_brief.pdf?rev=85736590681147dfbc7423df7b9b5436. Accessed on: 20 Jan. 2022.

[16] OWASP, OWASP risk rating methodology, 2021. https://owasp.org/www-community/OWASP_Risk_Rating_Methodology. Accessed on: 20 Jan. 2022.
[17] Nyanchama, M., Enterprise vulnerability management and its role in information security management. *Inf. Secur. J. A Glob. Perspect*., **14**(3), pp. 29–56, 2005.
[18] Souppaya, M. (NIST) & Scarfone, K., Guide to Enterprise Patch Management, 2013. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf. Accessed on: 20 Jan. 2022.
[19] Dissanayake, N., Jayatilaka, A., Zahedi, M. & Babar, M., Software security patch management: A systematic literature review of challenges, approaches, tools and practices. *Information and Software Technology*, **144**, 106771, 2022. DOI: 10.1016/j.infsof.2021.106771.