ICIT Institute for Critical Infrastructure Technology
The Cybersecurity Think Tank

Nikki Robinson DSc, PhD,

ICIT Fellow and Professor, Capitol Technology University

Concise and Consolidated Language in Vulnerability Management Programs

AN ICIT FELLOW PERSPECTIVE
APRIL 2022

Contents

Vulnerability Management Terminology

Vulnerability management has a long and complex history of definitions throughout the cybersecurity industry. As organizations and systems became increasingly intricate, the true definition of vulnerability management became more obscure. Yet, without speaking the same language, it is difficult for organizations to understand the roles and responsibilities of vulnerability management. This section reviews industry-specific guidance and terminology.

The National Institute of Standards and Technology

The National Institute of Standards and Technology (NIST) has several guidelines to review the vulnerability management components within a cybersecurity program. Since NIST publications are a staple of cybersecurity guidance, it is essential to review two of their documents to understand vulnerability management:

- Special Publication (SP) 800-40 Revision 3 (Guide to Enterprise Patch Management Technologies) (Souppaya & Scarfone, 2013)
- SP 800-53 r5 (Security and Privacy Controls for Information Systems and Organizations) (Joint Task Force, 2020)

The NIST SP 800-40 was last updated in July 2013 and primarily speaks to patch management for vulnerability management programs. Patch management is a core function required by multiple frameworks and policies (Souppaya & Scarfone, 2013). However, there is a need for updated guidance that shows the differences between patch management and vulnerability management, as the document lacks a clear definition of vulnerability management.

The NIST SP 800-53 r5 provides a comprehensive list of security controls and their applications throughout an environment. It provides security, privacy, and risk management control guidelines intended for the public sector to use but remains incredibly useful in the private sector to understand baseline security requirements (Joint Task Force, 2020). While it does include several controls to consider when monitoring and scanning networks for vulnerabilities, it also lacks a clear, overall definition for vulnerability management. Controls include authentication mechanisms and settings, encryption, auditing and change management, to name a few.

The Common Vulnerability Scoring System

The Common Vulnerability Scoring System (CVSS) is used to understand components of vulnerabilities and provide a numerical score that allows for a standard score across the industry (FIRST, n.d.). It has become an initial factor for security tools and scanners to identify concerning aspects of vulnerabilities and prioritize them by severity so system owners and security analysts can conduct remediation activities. CVSS measures risks associated with vulnerabilities, though FIRST mentions that this score alone should not be used to calculate risk.

There is no specific definition for vulnerability management used by CVSS, but vulnerabilities and associated metrics are explored in depth. Attack vectors, escalated privileges, the exploit lifecycle, and vulnerability chaining are all defined. The base, temporal, and environmental metrics that comprise the score are also defined. Each component is shown in the final calculation, allowing users to prioritize vulnerability management processes and remediation activities (FIRST, n.d.).

The National Vulnerability Database

The National Vulnerability Database (NVD) is a repository of vulnerability management data, including common vulnerabilities and exposures (CVE) identifications and descriptions for every vulnerability (NISTa, n.d.). The NVD defines CVE as part of the unique identification process for vulnerabilities (NISTb, n.d.). There are also clear definitions for severity, weakness enumeration, and known affected software configurations (NISTc, n.d.). While multiple definitions are provided for vulnerability management components of scoring and identification, there is no clear definition provided for vulnerability management itself in the NVD.

MITRE

MITRE is responsible for identifying vulnerabilities and CVEs for disclosed vulnerabilities (MITRE, n.d.). The MITRE website for CVE identification includes guidance and rules for understanding CVE identification and numeration but does not have a standard list of definitions. It also defines the CVE Numbering Authority as a component of understanding how vulnerabilities are identified as part of the scoring lifecycle.

These organizations are all key components to understanding what is applicable and important about vulnerabilities. Unfortunately, none of them explicitly define vulnerability management, instead choosing to explain related terms.

The Field of Etymology

Etymology is the study of how words came to be, investigating how the meaning and use of individual words have changed over time. Etymology includes relationships between languages, word form, and the history of a word (Durkin, 2009), which is of particular interest because of how much the meaning of the phrase vulnerability management has changed over time. Vulnerability management is defined as "an ISCM capability that identified vulnerabilities on devices that are likely to be used by attackers to compromise a device…" from the NISTIR 8011, Volume 1 (Dempsey et al, 2017). However, an article by Crowdstrike from May, 2021 defines vulnerability management as the "ongoing, regular process of identifying, assessing, reporting on, managing and remediating cyber vulnerabilities across endpoints…" (Crowdstrike, 2021).

How Do We Use the Term Vulnerability Management?

The lack of a clear definition in industry-standard guidance shows that the cybersecurity industry does not use one definition of vulnerability management. In some cases, the terms vulnerability management and patch management are interchangeable (Afifi-Savet, 2021). In other places, vulnerability management may be a program containing vulnerability scanning, prioritization, and remediation as a siloed function. Vulnerability management can focus on the metrics associated with identifying and remediating vulnerabilities with or without discussing how to securely configure components (Foreman, 2019). It can also either exist as a separate component of cybersecurity programs or a distinct objective for a different team. Vulnerability management programs may include patch management strategies, secure configuration implementation, continuous monitoring, remediation activities, or reporting metrics for assessments or audits (Foreman, 2019).

Given the breadth and possibilities of a vulnerability management program, there may not be one clear definition that makes sense to all organizations. However, this also indicates a need for more precise terminology to describe the different components of vulnerability management concepts. As the cybersecurity industry rapidly changes, language needs to keep up with the new and unexplored phenomena within the field.

Current Language Research

There is limited research available on the study of etymology and language in cybersecurity, which indicates a need for more qualitative research on the subject. However, Althonayan and Andronache (2018) noted concerns with different definitions and meanings for the same terminology. The researchers focused on how the interchangeable nature of terminology within cybersecurity can become a major issue within cybersecurity, leading to insecure system configurations, thus increasing internal and external threats within an organization.

Nugent and Collar (2015) took a different approach to how terminology affects cybersecurity, focusing on what a ‘hero’ is and what it means to cybersecurity programs. The authors explored the archetype of a hero in popular culture, as both defender and protector, and tied it back to what it means to be a cybersecurity hero. The authors made an interesting point about the ‘attacker vs. defender’ idea in cybersecurity and how this changes the perception of cybersecurity defenders. This is another area where understanding how terminology is defined is incredibly important when building a cybersecurity program.

Scott and Mason (2022) have the most up-to-date research, reviewing six different cybersecurity education frameworks, including the ASD Cyber Skills Framework and CyBOK, to examine the lack of research and solutions available to address the challenges faced by English as an additional language (EAL) student. They also noted the etymology of the word cyber traces back to cybernetics but that there is confusion around what it means. Even with numerous studies investigating the lack of standardization, which is confusing for EAL students and the cyber industry, there is still limited information on how to combat the confusion.

Proper Context Clarifies Concepts

Without proper terminology and definitions, it is difficult for experts to discuss the complex challenges they face. It is also increasingly difficult to train new cybersecurity hires when various educational programs use terminology differently. This misunderstanding can lead to insecure configurations, increasing risk and ultimately leading to incidents. Understanding how etymology plays into cybersecurity, specifically vulnerability management, could raise awareness of common threats, like the inability to review multiple vulnerabilities in combination, known as vulnerability chaining blindness (Robinson, 2021)).

What Are the Concerns with the Current Language in Vulnerability Management Programs?

The lack of consistent terminology across cybersecurity programs causes misconceptions about what vulnerability management means across organizations, even outside cybersecurity teams. For example, an IT professional may see vulnerability management activities as patch management or applying security controls to their systems. In contrast, a cybersecurity professional may see vulnerability management as associated with risk management across the organization. Multiple definitions can make it increasingly difficult to see the entire risk picture, making all other detection and remediation steps less effective.

Vulnerability Management

Consider an organization with on-premises systems, virtual servers, and systems in the cloud. The organization has multiple levels of operating systems, legacy and specialty applications, and multiple cybersecurity frameworks they must follow to implement security controls. If IT and security groups do not understand vulnerability management within the same context, it becomes more difficult to identify assets and implement continuous monitoring across the tech stack. Since vulnerability management includes identification, detection, reporting, and monitoring for vulnerabilities, when any one piece of the lifecycle is misunderstood, the consequences can ripple across the rest organization.

Vulnerability Chaining vs. Exploit Chaining

Using different terms to describe the same phenomenon increases confusion and worsens the lack of awareness of the issue's root. The CVSS User Guide (n.d.) identifies vulnerability chaining as exploiting multiple vulnerabilities during a single attack. However, Hill (2022) explained exploit chaining as cyberattacks using multiple exploits to compromise symptoms. Essentially, the two terms describe the same type of attack. This confusion could lead to a lack of awareness, the inability to protect, and frustration between teams.

Cyber Kill Chain

The word 'chain' is increasingly used within cybersecurity to encourage cybersecurity professionals to see how attackers use multiple vulnerabilities to conduct attacks. Lockheed Martin (n.d.) created the Cyber Kill Chain framework to help identify and ultimately prevent cyberattacks. In this instance, the word 'chain' describes how malicious actors conduct an attack. Most red teams and penetration testers understand attack and vulnerability chains, but network defenders typically do not. Vulnerabilities are typically viewed as singular objects instead of threat avenues to be remediated in combination.

General User vs. Security Practitioner

General users understand cybersecurity practices and principles quite differently than cybersecurity practitioners. If general users see vulnerability management as patching that makes their machine unavailable, they may view it negatively. In contrast, cybersecurity practitioners understand vulnerability management as essential to understanding and mitigating the threat landscape. Without awareness of the multiple perspectives on vulnerability management, each group of users has different expectations and understanding of their responsibilities and requirements.

How Can We Resolve This?

While more research needs to be done, both the industry and individual organizations can already take steps to provide more comprehensive language about vulnerability management programs. First, companies could encourage technical practitioners in both IT and security to research and create awareness of this issue within their organizations. Additionally, academic institutions and security researchers could work together to understand how language affects their cybersecurity programs.

Vendor-Released Terminology Must Align With Regulation Standards

There are many security tools, security awareness training organizations, and security professionals authoring books. Because every security practitioner has their own perspective, biases, and experience within the industry, the industry should not rely on one persons' experience to create definitions and terminology. While industry professionals should create new terminology to describe new phenomena, the industry at large should agree on set definitions for industry-wide terminology to reduce confusion and ultimately mature vulnerability management programs.

Use Common Terminology

The author of the article who defined exploit chaining aimed to comprehensively describe the phenomenon. But ultimately, the more terminology that describes combining vulnerabilities, the more confusing it may be to the industry. Instead, one term should be selected and consistently used.

Create a Single Standard

Another possible contributor to the confusion about language and terminology is that the industry does not agree on one standard or set of controls. While it is necessary to distinguish what vulnerability management and secure configurations mean across countries and industries, there is no specific standard that the private sector exclusively uses. There will always be room for unique environments and situations, but basic practices and standards should guide vulnerability management programs across sectors. Major cybersecurity tech companies and federal organizations, like NIST and the Cybersecurity and Infrastructure Security Agency, should create a specific taxonomy on vulnerability management to clear up any lingering confusion for practitioners.

Focus on Simplicity

The cybersecurity industry has grown tremendously in the last five to ten years. It has expanded from patch management and secure configuration to attack path management, vulnerability chaining and remediation, and securing micro-applications and services. With emerging technology growing at an intense rate, it is critical to simplify those systems' security requirements and controls, particularly because many organizations have hybrid cloud environments that make vulnerability management insanely complicated. Agreeing on a standard set of practices and concepts for vulnerability management could remove unnecessary terms, reduce policy guidance, and ultimately improve prioritization and remediation efforts. Simple solutions for complex systems will make vulnerability management easier to adopt.

Looking Ahead

The increased academic research around etymology, human factors within cybersecurity programs, and technical solutions provide many options for improvements in vulnerability management. Private sector and academic partnerships will help reduce the complexity surrounding vulnerability management terminology, practices, and guidance. Academic researchers can also aid technical practitioners by identifying problems and providing a roadmap to address those problems. For example, researchers can identify where terminology may affect an organization and provide a map to address those issues in the policies and the tools used by practitioners.

Creating Standards

If a standardized organization creates new terminology, taxonomies, or ontologies for vulnerability management concepts, private sector organizations should adopt them and create coordinated vulnerability management programs. For fundamental concepts like vulnerability chaining, it could also raise awareness of this topic. However, if the industry continues to develop new terminology for the same phenomena, it will be increasingly difficult to coordinate remediation efforts.

Vetting New Phenomena and Terminology

Even without one standard accreditation body that standardizes terminology, it is possible to create a board of experts to discuss and agree on terminology for the industry, allowing technology industries to handle large-scale issues within vulnerability management programs. Without the industry or organizations taking this seriously, vulnerability management programs may have difficulty encouraging risk management compliance in non-security groups. This could ultimately lead to lack of remediating potentially damaging vulnerabilities within organizations. Vulnerability management is vital to the success of cybersecurity programs, so the sooner we work towards standardization of terminology, the sooner we can protect our organizations from common cyber threats.

About the Author

Nikki Robinson holds a Doctor of Science in Cybersecurity from Capitol Technology University. Her specialization is in vulnerability management and the challenges around it. She has over 12 years in both the IT and Security fields as a cybersecurity engineer with an IT background, which brings technical descriptions to each presentation. Dr. Robinson holds certifications in both IT and Security, including the CISSP, CEH, CNDA, MCITP, and CCAA. Her goal is to help people to solve issues around vulnerability management and lower their organization’s risk profile.

About Capitol Technology University

Since its start in 1927, Capitol Technology University has remained true to its mission – preparing students for careers in a quickly changing world. With a tradition of academic excellence and practical learning, Capitol Tech has equipped its alumni with the knowledge and skills to evolve with the advanced sophistication of technology. While innovations spur new developments and industries, the foundations taught at Capitol Tech– thinking critically, actively and creatively – remain. Capitol Tech is committed to providing students with a quality education and the relevant experience to excel in a rapidly changing world filled new technology and global commerce both now and in the future.

About ICIT

The Institute for Critical Infrastructure Technology (ICIT) is a 501c(3) cybersecurity Think Tank with a mission to cultivate a cybersecurity renaissance that will improve the resiliency of our Nation’s 16 critical infrastructure sectors, defend our democratic institutions, and empower generations of cybersecurity leaders.

References

Afifi-Sabet, K. (2021). Patch management vs vulnerability management. Retrieved from https://www.itpro.com/security/27713/the-importance-and-benefits-of-effective-patch-management#:~:text=%20Applying%20fixes%20and%20updates%20for%20security%20vulnerabilities,of%20dealing%20with%20security%20vulnerabilities%20of%20all%20guises.

Althonayan, A., and Andronache, A. (2018). Shifting from information security towards a cybersecurity paradigm. Proceedings of the 2018 10th International Conference on Information Management and Engineering. https://doi.org/10.1145/3285957.3285971

Crowdstrike (2021). Vulnerability management? Retrieved from https://www.crowdstrike.com/cybersecurity-101/vulnerability-management/

Dempsey, K., Eavy, P., and Moore, G. (2017). Automation support for security control assessments: Volume 1. https://doi.org/10/6028/NIST.IR.8011-1

Durkin, P. (2009). The Oxford Guide to Etymology. Oxford University Press. New York: New York.

FIRST (n.d.). Common Vulnerability Scoring System v3.1 User Guide. Retrieved from https://www.first.org/cvss/v3.1/user-guide

Foreman, P. (2019). Vulnerability management: 2nd edition. CRC Press: Boca Raton, FL.

Hill, M. (2022). Exploit chains explained: How and why attackers target multiple vulnerabilities. Retrieved from https://www.csoonline.com/article/3645449/exploit-chains-explained-how-and-why-attackers-target-multiple-vulnerabilities.html

Joint Task Force (2020, Sept). Security and privacy controls for information systems and organizations. https://doi.org/10.6028/NIST.SP.800-53r5

Lockheed Martin (n.d.). The cyber kill chain. Retrieved from https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html#

MITRE (n.d.). CVE. Retrieved from https://cve.mitre.org/

NISTa (n.d.). NVD. Retrieved from https://nvd.nist.gov/

NISTb (n.d.). NVD: Vulnerabilities. Retrieved from https://nvd.nist.gov/vuln

NISTc (n.d.). NVD: Understanding vulnerability detail pages. Retrieved from https://nvd.nist.gov/vuln/vulnerability-detail-pages

Nugent, P. D., and Collar, E. (2015). Where is the cybersecurity hero? Practical recommendations for making cybersecurity heroism more visible in organizations. International Journal of Computer Science and Information Security, 13(4).

Robinson, N. (2021). An exploratory study into vulnerability chaining blindness terminology and viability. Retrieved from https://www.researchgate.net/publication/359390675_An_Exploratory_Study_into_Vulnerability_Chaining_Blindness_Terminology_and_Viability

Scott, B., and Mason, R. (2022). Cyber as a second language? A challenge to cybersecurity education. Journal of the Colloquium for Information Systems Security Education, 9(1).

Souppaya, M., and Scarfone, K. (2013, July). Guide to enterprise patch management technologies. http://dx.doi.org/10.6028/NIST.SP.800-40r3