CHRIS HUGHES, M.S., MBA
NIKKI ROBINSON, DSc, PhD

FOREWORD BY **RON GULA**

EFFECTIVE VULNERABILITY MANAGEMENT

MANAGING RISK IN THE VULNERABLE DIGITAL ECOSYSTEM

WILEY

Effective Vulnerability Management

Effective Vulnerability Management

Managing Risk in the Vulnerable Digital Ecosystem

Chris Hughes, M.S., MBA
Nikki Robinson, DSc, PhD

WILEY

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada and the United Kingdom.

ISBNs: 9781394221202 (Paperback), 9781394221226 (ePDF), 9781394221219 (ePub)

Library of Congress Control Number: 2023948620

Cover images: Dragon: © CSA-Printstock/Getty Images
Background: © enjoynz/Getty Images
Cover design: Wiley

This book is dedicated to my wife Kathleen and our children Carolina, Calvin, Callie, and Clayton, whose unwavering support enabled me to continue to grow professionally and who continue to be my primary purpose for always striving forward.

—Chris Hughes

I dedicate this book to my husband, Brian, and my daughters, Keira and Teagan. Without your constant support and encouragement, I would never be able to pursue the things I love. You all are my world. I also dedicate this book to my Grandma Osbourn—one of the strongest women I know. I'm lucky to have had such an independent and fearless female to look up to.

—Dr. Nikki Robinson

Contents at a Glance

Contents

Foreword

When I helped found Tenable Network Security, in many ways I was trying to get ahead of all the ways that we'd seen bad actors break into networks with our Dragon Network Intrusion Detection System. With Dragon, we saw all sorts of hostile state-of-the-art nation-state attacks and exploitations of unpatched systems as well as ankle-biter hackers. In starting Tenable, my cofounders and I wanted to make cybersecurity an obtainable and defendable goal. Continuous monitoring did not exist as a concept in the early 2000s. Annual penetration tests and even quarterly vulnerability scans were the norm. We wanted to make understanding cybersecurity risks easy for individuals and organizations.

As use of the Internet and dependency on it grew, so did nation-state threat actors. Our industry responded with IT regulations and frameworks. By 2020, we had the Payment Card Industry requirement, which was a wide variety of government standards that culminated in the National Institute of Standards and Technology (NIST) Cybersecurity Framework as well as the MITRE ATT&CK framework. During that same time frame, we saw the SANS organization publish their list of the Top 20 Vulnerabilities. This quickly became hard to manage and was replaced by the SANS Top 20 Controls, which was subsumed by the Center for Internet Security (CIS). We also saw hacking move from denial-of-service attacks on websites in the early 2000s, to crippling nation-state attacks that shut down hospitals, shipyards, and grocery stores.

As awareness of the risks of IT grew, new types of tech seemed to grow faster. From 2000 to 2020, we saw the introduction of Wi-Fi networks, mobile devices, virtualization, containers, software-as-a-service (SaaS) services, elastic cloud infrastructure, and embedded devices, and now we are grappling with implementing artificial intelligence (AI).

In the last decade, we have seen an increased role of government in IT. The Trump administration banned network technologies like drones, security cameras, and network devices from China, and introduced the "defend forward" concept that is still in use by the National Security Agency (NSA). The Biden administration recently added the Office of the National Cyber Director, which quarterbacks much of the

U.S. government's cyber strategy. It's very likely there will be more regulation to come that will impact how we defend and use the Internet.

However, as of late 2023, we don't have a consistent recipe or set of rules for securing data. If you are new to vulnerability management, this may seem surprising to you. How you perform vulnerability management is extremely subjective, based on the technology, the sensitivity of the data stored within it, the sophistication of the threat actors you are protecting against, your available budget, your people, and a wide variety of political, regulatory, and legal requirements. What works for a financial institution protecting trillions of dollars of transactions per day simply won't work for protecting the U.S. President's email. Protecting a video game service with millions of users is very different than keeping ransomware actors from stealing credit cards at your favorite coffee shop. Even though we all use the Internet, we all use it differently, with different technologies and tolerances for reliability and potential data loss.

It's because of this that I am very happy to have been asked by Nikki and Chris to write this book's Foreword. No matter what type of network security background you have, this book does an excellent job of covering the various aspects of vulnerability management. It presents several different advantages and limitations of technology for measuring vulnerabilities and remediating them across a wide breadth of technologies. It also covers the different types of frameworks that can be used to make sense of assets, their vulnerability, and compliance data, which can be extremely overwhelming. Whether you are learning vulnerability management concepts for the first time or looking to run an enterprise team focused on securing the network of a major bank, this book has the proper topics covered.

—Ron Gula, President, Gula Tech Adventures and Co-Founder, Tenable Network Security

Introduction

We live in a world that is enabled in countless ways by software. Over a decade ago, Marc Andreessen quipped, "Software is eating the world," and it indeed is. From our personal leisure activities to critical infrastructure and national security, nearly everything uses software. It powers our medical devices, telecommunications networks, water treatment facilities, educational institutions, and countless other examples. This means that software is pervasive, but as software use and integration into every facet of society has grown, so have the vulnerabilities associated with our digital systems. This has manifested in tremendous levels of systemic risk that can, has, and will continue to impact our daily lives.

The World Economic Forum (WEF) stated that at the end of 2022, a total of 60 percent of global gross domestic product (GDP) was dependent on digital technologies. That said, the WEF also conducted a survey in 2023 with respondents projecting a "catastrophic" cyber incident within the next two years. The threats of vulnerability exploitation are growing each year, in combination with the ease of use of malicious tools for creating and distributing ransomware and malware.

Since the earliest days of computer systems, researchers and practitioners have been trying to address vulnerabilities in digital systems by practicing what is referred to as "vulnerability management." As defined by the National Institute of Standards and Technology (NIST), a vulnerability is "a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source."

Digital system vulnerabilities and the ability for them to be exploited were documented as early as the 1970s, with a report titled "Security Controls for Computer Systems," also known as the "Ware Report" because a RAND employee named Willis Ware chaired the committee producing it for the U.S. Department of Defense (DoD). In addition to the report touching on vulnerabilities in systems, it discusses the need to design systems with security in mind throughout the software and system development life cycle. In 2023, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) issued guidance titled, "Shifting the Balance of Cybersecurity Risk: Security-by-Design and Default

Principles," which called for technology manufacturers to shift to creating products that are secure-by-design.

Despite the calls for secure-by-design systems and the awareness for over 50 years of the vulnerabilities of digital systems and the ability to exploit them, as an industry we continue to struggle with remediating vulnerabilities in digital systems as well as ensuring that security is a core part of system design and development. As modern digital environments have only gotten more complex and software more pervasive, organizations struggle to keep up with addressing vulnerabilities, now leading to unforeseen levels of systemic risk in our digital ecosystems.

Tremendous growth has occurred in publicly disclosed and tracked vulnerabilities, with notable sources such as the NIST National Vulnerability Database (NVD) seeing Common Vulnerabilities and Exposures (CVEs) grow from merely a few hundred in the 1990s to over 190,000 in 2022. These vulnerabilities are seen across a sprawl of software, hardware, libraries, and tools (in both open source and off-the-shelf solutions). With the complexity of software and applications across organizations, the sheer volume of vulnerabilities is difficult to track and remediate.

As the list of publicly disclosed vulnerabilities has grown each year, so have organizations' backlogs of unresolved vulnerabilities as they struggle to keep pace. A 2022 survey conducted by security vendor Rezilion and the Ponemon Institute found that 66 percent of respondents cited having a backlog of more than 100,000 vulnerabilities, and that they're only able to patch less than half of those vulnerabilities. Another study published in 2022 by security vendor Qualys found that there remains a gap between organizations' mean-time-to-remediate (MTTR) vulnerabilities and malicious actors' abilities to exploit them. In our roles both in organizations and as members of society, we, as cybersecurity practitioners, simply cannot keep up with the growth of vulnerabilities associated with our digital ecosystem, nor the malicious actors who are actively exploiting them.

Contributing to the problem of the growing publication of vulnerabilities and malicious actors exploiting them is the reality that organizations can't identify the important components of the noise. Despite there being over 25,000 known vulnerabilities published in 2022, less than 1 percent of all these known vulnerabilities were exploited by malicious actors. This means that organizations are spending energy, effort, and resources on addressing vulnerabilities that never actually

get exploited by malicious actors, and are trying to make sense of and prioritize the ones that have been or are likely to be exploited.

As we will point out throughout the text, in addition to organizations struggling to keep up with patching flaws in software and systems, there are a myriad of other factors that complicate an organization's ability to address vulnerabilities. These include challenges with proper asset visibility and inventory, ensuring secure configurations are in place to prevent system exploitation by malicious actors, the pervasive use of third-party and open source code, configuration missteps, and the addition of the human factors in vulnerability management.

Malicious actors increasingly are gaining efficiency at chaining together vulnerabilities and taking advantage of the pervasiveness of software in modern society, driven by widespread efforts at digital transformation. Efforts such as DevSecOps that promise to "shift security left" have their own challenges like noisy findings by modern vulnerability scanning tools, cognitive overload on often-understaffed security teams, and worldwide shortages of cybersecurity talent.

Given the prevalence of vulnerability chaining, digital transformation, DevSecOps, and software supply chain security concerns, vulnerability management is more important now than ever. Without an updated and modern approach to handling vulnerabilities, organizations will continue to be buried in vulnerabilities with little context. Our approach addresses cloud environments, large and small development programs, and the combination of hybrid and multicloud deployments. This approach focuses on not just the technology and methodologies of vulnerability management, but also the humans and organizations involved in the activities.

So let's begin.

What Does This Book Cover?

This book covers the following topics:

Chapter 1: Asset Management This chapter addresses fundamental activities such as asset management, which includes physical and mobile asset management, as well as software asset inventory and dealing with complex cloud, hybrid, and multicloud environments. There will also be coverage of tooling to facilitate asset management.

Chapter 2: Patch Management This chapter covers the fundamentals of patch management, including both manual and automated patch management, as well as the benefits and trade-offs between the two. It discusses software patch management, including open source management, and the various roles and responsibilities for patch management between different teams within the organization.

Chapter 3: Secure Configuration While patching known vulnerabilities are a core of vulnerability management processes, there is also the need for secure configurations. This chapter discusses the role of regulations and frameworks in secure configurations, as well as resources such as the NSA and CISA Top 10 cybersecurity misconfigurations publication. It also discusses industry-leading configuration resources such as CIS Benchmarks and DISA STIGs.

Chapter 4: Continuous Vulnerability Management Vulnerability management is far from a snapshot in time or once-and-done activity. This chapter discusses the concept of continuous vulnerability management and continuous monitoring. It discusses resources such as CIS and NIST controls that tie in to continuous vulnerability management and their associated tasks and activities.

Chapter 5: Vulnerability Scoring and Software Identification A major part of vulnerability management is identifying software and properly prioritizing vulnerabilities. In this chapter we cover both, including long-standing vulnerability scoring methodologies, as well as emerging vulnerability intelligence resources to help organizations more effectively prioritize vulnerabilities such as the Exploit Prediction Scoring System (EPSS) and the CISA Known Exploited Vulnerability (KEV) catalog.

Chapter 6: Vulnerability and Exploit Database Management Vulnerabilities are captured and stored in vulnerability databases. In this chapter, we cover widely used vulnerability databases such as the NIST National Vulnerability Database (NVD), as well as emerging databases such as Open Source Vulnerabilities (OSV) and others that address gaps in databases such as NVD. We also cover the role of exploit databases and how they can be used for both good and harm, depending on the user.

Chapter 7: Vulnerability Chaining It's often said that defenders think in lists while attackers think in graphs. This is because attackers are often looking to chain vulnerabilities together to move laterally through

environments or make their way toward sensitive resources. In this chapter, we discuss the concept of vulnerability chaining, as well as provide examples and gaps in the industry when it comes to focusing on vulnerability chaining.

Chapter 8: Vulnerability Threat Intelligence This chapter covers the role of vulnerability threat intelligence and advanced techniques such as threat hunting. We also discuss integrating threat intelligence into vulnerability management programs, including not just technologies but also people and process.

Chapter 9: Cloud, DevSecOps, and Software Supply Chain Security The modern threat landscape is complex, including cloud, a push for DevSecOps, and increasing attacks on the software supply chain. In this chapter, we go deep into these topics, including multi- and hybrid cloud containers, as well as the role of open source software and the systemic risks across the software supply chain.

Chapter 10: The Human Element in Vulnerability Management Most conversations about vulnerability management focus on the technical aspects, such as software and applications. However, behind all that technology are humans, operating in complex socio-technical environments, dealing with psychological stressors and challenges such as decision and alert fatigue. This chapter covers the human element of vulnerability management, including leading research on the topic from one of the authors.

Chapter 11: Secure-By-Design At the heart of vulnerability management is an uncomfortable truth, that the process of "patch faster, fix faster" is broken. Organizations continue to struggle with mounting vulnerability backlogs and insecure products. This chapter discusses the push for secure-by-design/default software and products and some of the key players who advocated for this paradigm shift. It also discusses some of the challenges facing the need to make this fundamental change of how we operate in the digital world.

Chapter 12: Vulnerability Management Maturity Model We conclude the book with a chapter looking at how to begin down the path of creating a mature vulnerability management model. We discuss key recommendations and steps, from asset management to continuous monitoring and integrating human factors. We hope to empower

readers to modernize their vulnerability management programs and ultimately lead to decreased organizational risk.

Who Should Read This Book

As the title implies, this book is intended for people who have an interest in vulnerability management, software, and digital and cyber physical systems. It is suited for various professional roles ranging from the C-suite (CISO, CTO, CEO, etc.) to security and software practitioners and aspiring entrants looking to better understand the vulnerability management practice and evolving landscape.

How to Contact the Publisher

If you believe you have found a mistake in this book, please bring it to our attention. At John Wiley & Sons, we understand how important it is to provide our customers with accurate content, but even with our best efforts an error may occur.

In order to submit your possible errata, please email it to our Customer Service Team at `wileysupport@wiley.com` with the subject line "Possible Book Errata Submission."

How to Contact the Authors

The authors would appreciate your input and questions about this book! Email Chris Hughes at `chughes@resilientcyber.io` and Dr. Nikki Robinson at `dr.nikki.robinson@gmail.com`.

1 Asset Management

Asset management is one of the most critical components of a vulnerability management program (VMP). Of all the fundamental building blocks of a successful VMP, it's crucial to get asset management right and complete before focusing on other aspects of vulnerability management.

Asset management is the listing or inventory of all hardware and software of an environment. Each environment has a different makeup of assets, including everything from mobile devices (e.g., laptops and cell phones) to application libraries and third-party software-as-a-service (SaaS) software. Without a comprehensive asset management program, organizations are limited in building mature VMPs with secure configuration, patch management, and continuous monitoring.

Asset management has evolved quite a bit over the last 10 years, with the advent of cloud infrastructure, increased use of SaaS, exponential growth of open source software use, and incredibly large and complex development environments. Years ago, asset management could be as simple as a spreadsheet with a list of asset names, tag numbers, and potentially an asset owner or IP address. Hardware and software inventories were kept separately and possibly managed by that same IT administrator. Yet with the increased use of cloud infrastructure, whether infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), or SaaS, traditional asset management methods are simply no longer viable. Using a spreadsheet to manage complex and dynamic assets is not maintainable or feasible to keep updated information available for management.

Traditional vulnerability management components are no longer able to mature with manual or incomplete asset inventories. It's increasingly difficult to manage dynamic assets such as containers, which are meant

to come online and be torn down at will. These asset types require a dynamic asset management program—one that can be updated quickly and at scale with large-scale development projects. An asset library can no longer be solely used for managing mobile devices or hardware assets but must be capable of keeping updated information on ephemeral applications and tools.

Without a modern approach to asset management, organizations have limited visibility of the hardware and software used by employees, which can have several cascading effects. Without knowledge of a laptop, for example, there is no way to determine if it has proper monitoring software installed, if it's still in the employee's possession, if it's checking for updated patches, or if it's compliant with organizational policies. And if an organization does not have the ability to see what software is installed on what systems, they have no way of knowing the number of vulnerabilities it has, what its potential attack surface is, or what dependencies that software might have on other systems.

Other limitations of an immature asset management program are the "unknown unknowns." If there are hardware or software assets that aren't effectively managed or visible to IT operations staff, organizations do not know the scope of vulnerabilities, inherent risks, or the interconnectivity of devices and applications. These limitations make it impossible to prioritize and remediate vulnerabilities effectively. It also makes it difficult to determine if applications are at the right patch level, if the application's version is at end of life/support, and if there are outstanding vulnerabilities or missing configurations that could lead to cyberattacks like distributed denial-of-service (DDoS) attacks, malware, or ransomware.

Asset management can be performed in a variety of ways. Organizations are using IT operations software, vulnerability scanning tools, cloud inventories, and even other configuration management software like ServiceNow (`www.servicenow.com`). This type of software can not only keep track of assets, but can also tie tickets and ongoing management of those devices with a system owner. Smaller organizations might still be managing assets manually, which limits the maturity and capability of a VMP. In this chapter, we discuss the common limitations of asset management tools and processes, possible impacts of an immature asset management program, and what organizations can do to create a modern approach to asset management.

Physical and Mobile Asset Management

In traditional data centers, asset management consists of the physical components in server racks—for example, networking devices, servers, power management, and any other physical devices in the organization. However, organizations have moved to a much more digital workforce, utilizing multiple mobile devices per employee. One employee might have a tablet, laptop, and smartphone, and use primarily online applications for collaboration versus solely working on a physical desktop located in an office setting.

Many organizations are moving to hybrid work environments where employees are working between an organization's office and their home or an off-site location. This type of work environment complicates the management of these devices, given that they may or may not be connected to the organization's virtual private network (VPN) or potentially cloud assets and servers. This setup has increased the challenge of managing and tracking mobile devices.

In modern organizations, managing all these mobile devices requires an asset management solution to handle all the operating systems (OSs) and types of applications required for online collaboration. A mobile toolkit includes asset management and inventory software, as well as configuration management, usually performed by a mobile device management (MDM) solution. This tool provides a management console to catalog each mobile device and assigns policies and security configurations as determined by the organization.

Several SaaS solutions are also available as well as tools provided by the mobile carrier. For example, mobile solutions provided by Apple (e.g., iPhones and iPads) have their own asset management solution like Jamf software. Other devices or applications, however, can be managed by MDM solutions like Miradore and Citrix Endpoint Management.

Because most organizations are moving away from on-premises data centers, there are fewer servers and network devices requiring asset management. With the advent of the cloud, more organizations are migrating their physical assets to a cloud infrastructure and using more ephemeral servers like containers. Yet on-premises data centers still require an asset management solution to provide full visibility to all systems. And it's not just for security reasons—they also must manage systems and ensure they are properly online and functioning without hardware failures. All the physical assets could be providing warning