Managing the Cyber Risk

A CISO's practical guide to threat and vulnerability management

Saurabh Mudgal

www.bpbonline.com

First Edition 2025

ISBN: 978-93-65892-918

LIMITS OF LIABILITY AND DISCLAIMER OF WARRANTY

The information contained in this book is true and correct to the best of author's and publisher's knowledge. The author has made every effort to ensure the accuracy of these publications, but the publisher cannot be held responsible for any loss or damage arising from any information in this book.

All trademarks referred to in the book are acknowledged as properties of their respective owners but BPB Publications cannot guarantee the accuracy of this information.

Dedicated to

My father: ***H N Sharma***

My mom: ***Kiran Sharma***

My wife: ***Anubha Mudgal***

My son: ***Yuvaan Mudgal***

My daughter: ***Vedika Mudgal***

About the Author

Saurabh Mudgal is a seasoned cybersecurity leader with over 19 years of experience. Currently, he serves as a principal group manager for the security engineering team at Microsoft, where he plays a pivotal role in building and implementing robust security solutions. Throughout his career, Saurabh has garnered extensive knowledge across various cybersecurity domains.

A distinguished alumnus of the **Indian School of Business** (**ISB**), a top-ranked business school in India, Saurabh further honed his leadership skills by completing a specialized CTO program. This unique blend of technical expertise and business acumen positions him to effectively translate security best practices into actionable strategies.

Saurabh's passion for sharing knowledge and fostering a proactive security culture is evident in his contribution to *Managing the Cyber Risk*. This book draws upon his experience and insights to empower CISOs, security leaders, and IT professionals with the tools and strategies needed to combat ever-evolving cyber threats.

About the Reviewers

- **Bhooshan Gadkari** is an experienced cybersecurity engineer currently working at one of the top telecom companies in the world. He is currently working on securing 5G applications which carry traffic of hundreds of millions of subscribers.

  From a technology stack perspective he has worked on container-native infrastructure, virtualization deployments, IoT products and iOS/Android mobile applications. He loves the daily security hustle and takes pride in protecting the company he is working in. In his personal time he enjoys listening to podcasts and watching historical movies.

- **Hrushikesh Deshmukh** is a seasoned Cloud and DevOps Solutions Architect with a distinguished career spanning industry leaders such as Apple Inc., Amazon, Fidelity Investments, Capital One, Teradata, Comcast, T-Mobile, AT&T, Fannie Mae and others. With deep expertise in cloud migration strategies, infrastructure automation, CI/CD pipelines, containerization, and security best practices, he has been instrumental in driving cutting-edge digital transformations for global enterprises.

  Recognized as a strategic cloud leader, innovative solutions architect, and technical visionary, he brings extensive experience in operational excellence, cross-functional leadership, and customer engagement. His ability to develop effective proposals, manage stakeholder relationships, and implement scalable cloud solutions has made him a trusted expert in the field. Passionate about advancing cloud technologies, he actively contributes to the tech community through research, publications, and speaking engagements at global conferences.

Acknowledgement

I would like to express my sincere gratitude to all those who contributed to the completion of this book.

First and foremost, I extend my heartfelt appreciation to my family for their unwavering support and encouragement throughout this journey. Their love and encouragement have been a constant source of motivation.

I am immensely grateful to BPB Publications for their guidance and expertise in bringing this book to fruition. Their support and assistance were invaluable in navigating the complexities of the publishing process.

I would also like to acknowledge the reviewers, technical experts, and editors who provided valuable feedback and contributed to the refinement of this manuscript. Their insights and suggestions have significantly enhanced the quality of the book.

Last but not least, I want to express my gratitude to the readers who have shown interest in our book. Your support and encouragement have been deeply appreciated.

Thank you to everyone who has played a part in making this book a reality.

Preface

In today's rapidly growing digital world, cyber threats are continuously evolving and changing, and organizations are struggling to keep pace. *Managing the Cyber Risk* equips CISOs and security professionals with the knowledge and strategies to build a solid defense against these pervasive threats.

This comprehensive guide takes you through evolving threat patterns, from understanding attackers' motivations and tactics to emerging threats that are plaguing today's technology. You will learn to build a solid vulnerability management foundation, become a master of essential skills like risk analysis and prioritization, and apply ongoing threat detection and response strategies.

With step-by-step instructions, real-world examples, and bonus chapter resources, *Managing the Cyber Risk* allows you to deploy a vulnerability management program that is tailored to meet your organization's specific needs. You will be able to properly prioritize and remediate vulnerabilities in a way that will minimize security threats, instill a culture of security awareness within your staff, and apply innovative tools and approaches to proactive hunting and response to threats.

You will be prepared by the end of this book to face the ever-changing threat landscape and build a cyber fortress that protects your organization's most critical assets and data.

Chapter 1: Rise of Vulnerability Management - This chapter sets the stage by outlining the ever-increasing threat landscape faced by organizations. It defines key terms like vulnerability management and explains its critical role in modern cybersecurity. This chapter also delves into the cost of cybercrime and the benefits of a robust vulnerability management program. Additionally, this chapter explores advanced threat and vulnerability management strategies, such as continuous threat detection and response, deception technologies, and DevSecOps integration.

Chapter 2: Understanding Threats - This chapter delves into the world of cyber attackers, exploring their motivations (financial gain, espionage, disruption) and the different types of actors (state-sponsored, cybercriminals, hacktivists). It also explains common attack vectors that attackers exploit to gain access to systems (phishing, social engineering, and SQL injection). We will dissect social engineering tactics, common attack vectors like phishing emails and malicious attachments, and vulnerabilities in software and hardware.

By understanding these techniques, we can build stronger defenses and safeguard our digital domain from intruders

Chapter 3: The Modern Threat Landscape - This chapter explores the constantly evolving threat landscape, focusing on emerging threats like AI-powered attacks and supply chain compromises. It also addresses the unique security challenges associated with cloud computing and the growing attack surface presented by the **Internet of Things** (**IoT**). Through detailed analysis and case studies, the chapter offers actionable insights and strategies to mitigate these threats, highlighting best practices for securing cloud deployments and IoT infrastructures.

Chapter 4: The Cost of Cybercrime - This chapter quantifies the significant financial impact of cybercrime, including incident response costs, ransom payments, and lost revenue. It explores the consequences of data breaches, covering regulatory fines, customer churn, and reputational damage. Readers will be able to define mitigation strategies for such pervasive threats.

Chapter 5: Foundations of Vulnerability Management - This chapter lays the groundwork for a successful vulnerability management program. It covers essential asset discovery and inventory techniques using tools like CMDB and vulnerability scanners. It also explains asset classification based on criticality and sensitivity and introduces risk-based prioritization frameworks like CVSS. By the end of this chapter, readers will have a deep understanding of foundational practices in effective vulnerability management.

Chapter 6: Vulnerability Scanning and Assessment Techniques - This chapter dives into the tools and techniques used to identify vulnerabilities in your systems. It covers automated vulnerability scanning tools like Nessus and OpenVAS, penetration testing methodologies (white-box, black-box), and the importance of integrating threat intelligence feeds (STIX/TAXII) for a more comprehensive approach. All these techniques, when combined, present a comprehensive way of doing vulnerability management.

Chapter 7: Vulnerability Risk Analysis - This chapter delves into vulnerability risk analysis, a crucial step in prioritizing remediation efforts. It explains the exploitability (likelihood of successful attack) and severity (potential impact) of vulnerabilities. It also introduces the **Common Vulnerability Scoring System** (**CVSS**) and the importance of considering business impact during risk analysis. By the end of this chapter, readers will learn how to assess and mitigate risks to maintain a strong security posture.

Chapter 8: Patch Management Prioritization and Remediation - This chapter focuses on prioritizing and remediating identified vulnerabilities. It covers patch management strategies and tools (Microsoft CM and Intune), alternative risk mitigation techniques like

workarounds and network segmentation, and strategies for allocating resources effectively for vulnerability remediation.

Chapter 9: Security Awareness Training and Employee Education - This chapter emphasizes the critical role of a security-aware workforce in mitigating cyber threats. It discusses effective security awareness training methods like phishing simulations and social engineering awareness programs and explores tools and platforms for delivering ongoing security education.

Chapter 10: Planning Incident Response and Disaster Recovery - This chapter prepares organizations for the inevitable security incident. It outlines the key components of an incident response plan (IR framework, roles, and responsibilities) and explores disaster recovery planning for data backup and restoration, ensuring business continuity. It also highlights the importance of regularly testing IR plans and updating them through simulation exercises.

Chapter 11: Role of Security Champions and Security Operations Center - This chapter explores the critical roles of security champions and the **security operations center** (**SOC**) in maintaining a strong security posture. It explains how security champions promote security awareness within departments and collaborate with SOCs, which utilize tools like SIEM and threat intelligence platforms for continuous monitoring and threat detection.

Chapter 12: Measuring Program Effectiveness - This chapter explores the importance of measuring the effectiveness of your vulnerability management program. It introduces key metrics like **mean time to patch** (**MTTP**) and the number of vulnerabilities identified. It also explores methods for calculating the program's return on investment (ROI) and creating compelling reports for leadership.

Chapter 13: Continuous Threat Detection and Response - This chapter delves into advanced detection and response techniques like **endpoint detection and response** (**EDR**) tools, **network traffic analysis** (**NTA**), and threat hunting methodologies. It explains how these methods work together in a **Continuous Threat Detection and Response (CTDR)** framework for proactive threat management.

Chapter 14: Deception Technologies and Threat Hunting - This chapter explores advanced threat hunting techniques like deception technologies, including honeypots and honeynets. It explains how these tools can lure attackers and provide valuable insights into their **tactics, techniques, and procedures** (**TTPs**). By the end of this chapter, readers will learn how to integrate findings from threat hunting into a robust security strategy.

Chapter 15: Integrating Vulnerability Management with DevSecOps Pipelines - This chapter explores the importance of integrating vulnerability management into the **software development lifecycle** (**SDLC**) using DevSecOps methodologies. It covers security code scanning tools (SAST, DAST) and strategies for embedding vulnerability management throughout the development process to identify and fix vulnerabilities early.

Chapter 16: Emerging Technology and Future of Vulnerability Management - This chapter explores the impact of emerging technologies on the threat landscape and vulnerability management practices. It discusses the potential of **artificial intelligence** (**AI**) for threat detection and response, the implications of blockchain for secure data storage, and the challenges and opportunities presented by quantum computing for cybersecurity.

Chapter 17: The CISO's Toolkit - This chapter equips CISOs with practical resources to implement the strategies outlined in the book. It provides a collection of essential templates, checklists, and reference materials to streamline program development and execution. This chapter offers a valuable starting point for CISOs to build and maintain a robust threat and vulnerability management program. By providing these resources, the book goes beyond theory and empowers CISOs to take immediate action and strengthen their organization's security posture.

Code Bundle and Coloured Images

Please follow the link to download the
Code Bundle and the ***Coloured Images*** of the book:

https://rebrand.ly/45e128

The code bundle for the book is also hosted on GitHub at
https://github.com/bpbpublications/Managing-the-Cyber-Risk.
In case there's an update to the code, it will be updated on the existing GitHub repository.

We have code bundles from our rich catalogue of books and videos available at **https://github.com/bpbpublications**. Check them out!

Errata

We take immense pride in our work at BPB Publications and follow best practices to ensure the accuracy of our content to provide with an indulging reading experience to our subscribers. Our readers are our mirrors, and we use their inputs to reflect and improve upon human errors, if any, that may have occurred during the publishing processes involved. To let us maintain the quality and help us reach out to any readers who might be having difficulties due to any unforeseen errors, please write to us at :

errata@bpbonline.com

Your support, suggestions and feedbacks are highly appreciated by the BPB Publications' Family.

Piracy

If you come across any illegal copies of our works in any form on the internet, we would be grateful if you would provide us with the location address or website name. Please contact us at **business@bpbonline.com** with a link to the material.

If you are interested in becoming an author

If there is a topic that you have expertise in, and you are interested in either writing or contributing to a book, please visit **www.bpbonline.com**. We have worked with thousands of developers and tech professionals, just like you, to help them share their insights with the global tech community. You can make a general application, apply for a specific hot topic that we are recruiting an author for, or submit your own idea.

Reviews

Please leave a review. Once you have read and used this book, why not leave a review on the site that you purchased it from? Potential readers can then see and use your unbiased opinion to make purchase decisions. We at BPB can understand what you think about our products, and our authors can see your feedback on their book. Thank you!

For more information about BPB, please visit **www.bpbonline.com**.

Join our book's Discord space

Join the book's Discord Workspace for Latest updates, Offers, Tech happenings around the world, New Release and Sessions with the Authors:

https://discord.bpbonline.com

Table of Contents

Chapter 1
Rise of Vulnerability Management

Introduction

In an era where digital transformation drives business innovation, the risk of cyber threats has never been higher. This chapter provides a foundational understanding of the increasing threat landscape that organizations face today. We will explore various types of security threats, look into alarming cybercrime statistics, and discuss the substantial costs associated with cybercrime. A key focus of this chapter is the concept of vulnerability management—its principles, critical importance, and the substantial benefits it brings to an organization's cybersecurity posture. By the end of this chapter, readers will have a solid grasp of the essential components of vulnerability management and its role in mitigating modern cyber threats.

Structure

The chapter will cover the following sections:

- Case study, Target corporation data breach (2013)
- Security threats
- Cybercrime landscape statistics
- Cost of cybercrime

- Vulnerability management strategy
- Benefits of a robust vulnerability management program

Objectives

This chapter aims to equip readers with a comprehensive understanding of the current threat landscape and the importance of vulnerability management. Readers will learn about different types of security threats, gain insights from recent cybercrime statistics, and understand the financial implications of cyberattacks. The chapter will also introduce the core principles of vulnerability management and highlight the benefits of implementing a robust vulnerability management program.

Case study, [1]Target corporation data breach (2013)

The details of the case study are as follows:

- **Target**: A major retail corporation in the United States known for its wide variety of merchandise and affordable prices.
- **Attack type**: **Point-of-sale** (**POS**) system malware injection
- **Vulnerability exploited**: Unpatched vulnerabilities in Target's POS systems.
- **Attackers**: A group of cybercriminals, possibly linked to Eastern Europe.
- **Impact**:
    - Over 40 million customer credit and debit card details were stolen.
    - Additional personal information, like names and addresses, of millions of customers was potentially compromised.
    - Financial losses exceeding $200 million.
    - Damaged reputation and loss of customer trust.
- **Timeline**:
    - Attackers infiltrated the target's network as early as July 2013, exploiting vulnerabilities in a third-party **Heating, Ventilation, and Air Conditioning** (**HVAC**) vendor's web application.
    - Malicious code was injected into the target's POS systems, allowing attackers to steal customer data during transactions at physical stores between November and December 2013.

1. *Source: Target Corporation Data Breach: https://redriver.com/security/target-data-breach#:~:text=What%20Happened%20During%20the%20Target,was%20one%20of%20the%20largest.

- The breach was not discovered until late December 2013, when fraudulent activity on the stolen cards was flagged.

- **Lessons learnt**:
  - **Importance of vulnerability management**: The attack highlighted the critical need for organizations to proactively identify and patch vulnerabilities in their systems, especially those connected to sensitive data.
  - **Third-party risk management**: The target's reliance on a vulnerable third-party vendor's software demonstrates the importance of thorough security assessments for vendors whose systems integrate with a company's infrastructure.
  - **Security awareness training**: Educating employees about cyber threats and best practices for handling customer data can help prevent future attacks.

Target's data breach serves as a cautionary tale for organizations of all sizes. It emphasizes the importance of robust cybersecurity measures, including vulnerability management, third-party risk assessment, and employee security awareness training.

Cybercrime has become prominent, inflicting an estimated $6 trillion in global damages in 2021 alone[2]. This staggering figure underscores the urgency for organizations to prioritize cybersecurity measures.

The following figure highlights the annual increase in the number of reported **Common Vulnerabilities and Exposures** (**CVEs**). CVEs are publicly disclosed cybersecurity vulnerabilities that are cataloged in a standardized format. The rising trend in the number of CVEs underscores the growing complexity and volume of security threats that organizations face.

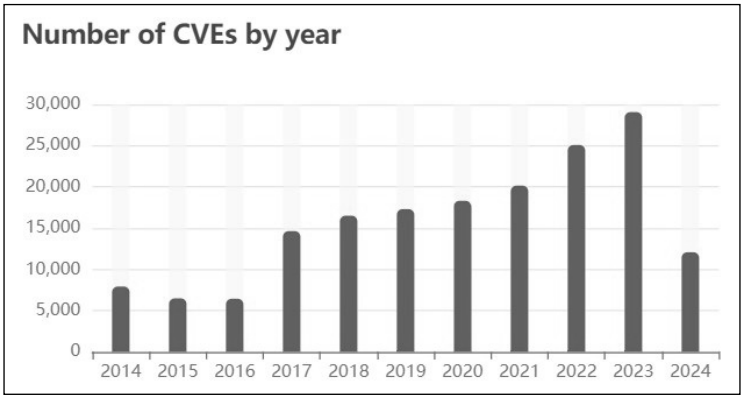

***Figure 1.1**:[3] Number of CVEs by year*

2. (Source: Cybersecurity Ventures)
3. https://www.cvedetails.com/

Security threats

The digital realm is fraught with various security threats that can compromise the integrity, confidentiality, and availability of information systems. Here, we outline some of the prevalent threats.

Malware

Malware, short for malicious software, is designed to infiltrate, damage, or disable computers and networks. It encompasses various forms, including viruses, worms, trojans, and spyware.

The types of malware are as follows:

- **Viruses**: Malicious programs that attach themselves to clean files and spread to other clean files. They can delete files, reformat the hard disk, or cause other damage.
- **Worms**: Malware that replicates itself to spread to other computers, often exploiting vulnerabilities in network software.
- **Trojans**: Disguised as legitimate software, trojans trick users into loading and executing them on their systems.
- **Spyware**: Software that secretly monitors user activity without their knowledge.
- **Adware**: Advertising-supported software designed to deliver ads automatically.
- **Ransomware**: Malware that locks or encrypts a victim's data and demands payment for the decryption key.

Real-world example

Stuxnet, a highly sophisticated worm, targeted industrial control systems and is believed to have been responsible for causing significant damage to Iran's nuclear program. It highlighted the potential for malware to impact physical infrastructure and national security.

Ransomware

Ransomware is a type of malware that encrypts a victim's files and demands a ransom payment for the decryption key. It has become one of the most lucrative and devastating forms of cybercrime.

Case study, WannaCry ransomware attack

The details are as follows:

- **Background:** The WannaCry ransomware attack, which occurred in May of 2017, is considered one of the most widespread and disruptive cybersecurity attacks of late. It is ransomware that greatly affects computers running Microsoft Windows, encrypting files, and demanding payments via Bitcoin. The speed at which it spread and the amount of damage caused really drove home how horrific cyber vulnerabilities could be on a global scale.
- **Key facts about the attack:** WannaCry used an exploited weakness in the Windows operating system SMB protocol, revealed by the NSA and then subsequently leaked by a group of hackers operating under the name The Shadow Brokers. While the makers of Windows had already issued a patch two months earlier for that exact vulnerability, called **MS17-010**, many organizations simply had not applied it.
- **Impact:** WannaCry spread to over 230,000 computers running in more than 150 countries within one day. This ransomware caused disruptions across industries such as healthcare, telecommunications, and logistics. For instance, the UK's NHS witnessed massive disruptions, which even forced postponements in surgical operations and patient care. The estimated financial impact of WannaCry was billions in terms of operational downtime costs, recovery expenditure, and security enhancements.
- **Analysis:** The WannaCry incident has again driven home the point of timely patch management and network segmentation as critical defense mechanisms against malware on a mass scale. The impact was high on organizations that had older systems or were lax with patching. Third, the incident brought to light the need for Incident Response and backup strategies since many organizations were left without access to data or backups.
- **Lessons learned:**
    - **Patch management**: Updates of software are fundamental to mitigating risks. The organizations that were able to apply the patch MS17-010 just in time did not fall prey to WannaCry.
    - **Network segmentation**: Segmentation of network segments may prevent malware from spreading all over an organizational organization.
    - **Regular backups**: A well-designed backup helps an organization to restore the data without giving ransom in order to retrieve it.
    - **Security awareness training**: Employee training on the concepts of phishing and malicious links can help reduce the chances of malware execution.