The Cybersecurity Mesh Architecture

Composable, flexible, and scalable security approach for a resilient security ecosystem

Tarun Kumar

www.bpbonline.com

First Edition 2025

ISBN: 978-93-65891-218

Dedicated to

My beloved wife:

Kanchan Bhatia Kumar

and

My son ***Vihaan Kumar***

About the Author

Tarun is a seasoned professional with 25+ years of exclusive experience covering Cyber/Information Security, IT Risk Management, Data Protection, and Privacy. In various leadership roles, he has had the distinction of building cybersecurity capabilities (people, process, and technology) for organizations (with extensive experience in managing large teams).

He has been CISO with a large global automobile major. In his past roles, he has been Director of Cybersecurity with a Big 4 firm; Global CISO with a leading global Business Process Management (BPM) organization and General Manager of Global Security Services with a large global IT Services organization.

He has extensively been involved in providing Cybersecurity services to domestic (India) and international clients across industries. He brings a 360-degree experience in Cybersecurity as a provider (consulting) and consumer (CISO) of services.

He has extensive experience in establishing road maps and investments for Cybersecurity, security governance, and IT risk management practices. His proficiency covers cybersecurity strategy and roadmap, governance, risk, compliance and controls, threat and vulnerability management, operations, data privacy, and business continuity.

He has been recognized with various industry honors between 2012-2023. He brings recognized credentials of CRISC, CISM, CISA, CISSP, and ISO27001 Lead Auditor.

About the Reviewer

John Mathew is a Cybersecurity Architect with eight years of experience in the field. He specializes in Penetration Testing, Ethical Hacking, Red Teaming and Blue Teaming. John holds a Bachelor of Technology in Computer Science and Engineering and has earned notable accolades, including First place in Capture the Flag contests and certifications such as ISC Certified in Cybersecurity and EC-Council Certified Ethical Hacker.

Outside of work, he is an avid reader and enjoys playing video games. He believes that Security is a myth and Testing is inevitable, a philosophy that drives his commitment to excellence in Cybersecurity.

Acknowledgement

I want to express my deepest gratitude to my family and friends for their unwavering support and encouragement throughout this book's writing, especially my wife Kanchan and son Vihaan.

I am also grateful to BPB Publications for their guidance and expertise in bringing this book to fruition. Revising this book was a long journey, with valuable participation and collaboration of reviewers, technical experts, and editors.

I have always thought that what makes the job worthwhile are the people you work with. I am thankful for the people I have worked with – on my team, across departments, and in my ecosystem, and would like to acknowledge their valuable contributions.

I would also like to thank my mentors, stakeholders, and colleagues for their continuous support and guidance.

Finally, I would like to thank all the readers who have taken an interest in my book and for their support in making it a reality. Your encouragement has been invaluable.

Preface

We reside in a world where the field of cyber threats is enormous and ever-evolving. Every new security solution/tool seems to result in newer ways for attackers to circumvent defenses.

The one standout pluck from the book is that a robust cybersecurity posture in today's times necessitates the amalgamation of and partnership (collaboration) between the various security solutions/tools that have been deployed.

Contemporary technology stacks are extensively distributed and often difficult to manage when separated into individual Silos. Hence, partnership (collaboration), integration, and aggregation are critical features of a successful cybersecurity strategy.

The book explores the concept of **Cybersecurity Mesh Architecture** (**CSMA**). After reading through all chapters, readers will appreciate the fact that CSMA is a valuable asset to enterprises (businesses) since it is an architectural philosophy that advocates solution/tool integration and data aggregation to achieve the desired outcomes. It also provisions for security analytics, integrated threat intelligence/dashboards, and automation supported by AI to achieve a cybersecurity posture that is dynamic and capable of responding swifter than attackers.

This book is suitable for students who are studying cybersecurity as a subject in their bachelor/master programs. It is also written for technical readers with a basic understanding of cybersecurity and networking technologies and their challenges.

This book is a resource that will enable you to have more trust in your knowledge of CSMA. I hope you will find this book informative and helpful.

Chapter 1: Cybersecurity: A Dynamic Changing Paradigm – This chapter reviews the chronology of the evolution of cybersecurity, presents a detailed overview of some noteworthy cybersecurity events (2010 – to date), takes a look at some major trends that had a noteworthy impact on cybersecurity, and examines the building blocks of cybersecurity and traditional cybersecurity measures.

Chapter 2: Cybersecurity: Understanding Today's Security Challenges – This chapter covers topics such as distributed systems, examines the security challenges of distributed systems, and presents details about cybersecurity threats, attacks, and key issues in the digital age.

Chapter 3: Emerging Cybersecurity Trends – In this chapter, we will explore the cybersecurity trends of today and the future, concentrating on presenting the common themes in these trends. This chapter also allows the reader to understand the importance of cyber resilience.

Chapter 4: The Need for Cybersecurity Mesh Architecture – This chapter presents the current situation of the cybersecurity ecosystem, explains CSMA, and illustrates its layers, needs, and benefits.

Chapter 5: Fundamental Components of Cybersecurity Mesh Architecture – This chapter gives special attention to the key components of CSMA, discusses the outcome of the adoption of CSMA, a unified architecture and provides a sneak preview of CSMA products/solutions.

Chapter 6: How to Effectively Adopt Cybersecurity Mesh Architecture – This chapter reassesses the cybersecurity landscape of today, elaborates on the key aspects of CSMA adoption, provides directions on how to get started with CSMA, and discusses the key factors of consideration while adopting CSMA.

Chapter 7: Benefits of Adopting Cybersecurity Mesh Architecture – This chapter emphasizes the necessity of CSMA and the benefits of leveraging CSMA. The chapter then discusses

the characteristics of a CSMA strategy and presents a few target use cases. Furthermore, it details the features to be considered for CSMA solutions and presents the pitfalls of not leveraging CSMA.

Chapter 8: CSMA Best Practices – In this chapter, we will compare CSMA with the traditional defense-in-depth approach and re-visit the salient points and goals. We will also discuss a systematic approach to implementing CSMA and take a look at the KPIs for assessing the effectiveness of the implementation of CSMA. The chapter also covers the commandments of CSMA and discusses the challenges in implementing CSMA.

Chapter 9: Potential Outlook for CSMA Adoption – This chapter will cover three distinct use cases in different environments where CSMA works [viz., work from home, cloud, and **operational technology** (**OT**)]. The chapter will also examine the use of CSMA in the healthcare sector and take a look at the CSMA market overview, its growth factors, dynamics, and growth opportunities.

Coloured Images

Please follow the link to download the
Coloured Images of the book:

https://rebrand.ly/75e90aj

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

Cybersecurity: A Dynamic Changing Paradigm

Introduction

Not only have the domains of cybersecurity and technology advanced but also have criminals/bad actors who aim to exploit weaknesses in the system for personal gain. Likewise, cybersecurity and cybercrime have progressively developed from the 1940s to the present, and this chapter explains the evolution of cyberattacks and security solutions.

Structure

In this chapter, we will cover the following topics:

- Evolution of cybersecurity
- Notable cybersecurity events
- Notable shifts impacting cybersecurity
- Cybersecurity threats evolution
- Building blocks of cybersecurity
- Traditional cybersecurity measures

Objectives

When we are asked when cybersecurity started, an instant answer, in most cases, is when the Internet started. Essentially, in this chapter, we shall realize that the cybersecurity industry has