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

LIMITS OF LIABILITY AND DISCLAIMER OF WARRANTY

The information contained in this book is true to correct and the best of author's and publisher's knowledge. The author has made every effort to ensure the accuracy of these publications, but 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.

www.bpbonline.com

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 revisit 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.

Did you know that BPB offers eBook versions of every book published, with PDF and ePub files available? You can upgrade to the eBook version at www.bpbonline.com and as a print book customer, you are entitled to a discount on the eBook copy. Get in touch with us at :

business@bpbonline.com for more details.

At **www.bpbonline.com**, you can also read a collection of free technical articles, sign up for a range of free newsletters, and receive exclusive discounts and offers on BPB books and eBooks.

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

1. Cybersecurity: A Dynamic Changing Paradigm....................1

Introduction..1

Structure...1

Objectives..1

Evolution of cybersecurity...2

Time before networking...2

Time of phone phreaks...3

Time of early hacking..3

Time of ARPANET and the Creeper and Reaper.................4

Decade of commercial antivirus..5

The first DoS attack...5

Connected world...6

The time of email..6

Cybersecurity threat canvas expansion.........................6

The Anonymous..7

Operation Aurora...8

Stuxnet...8

General Data Protection Regulation..............................8

The X hack..8

The SolarWinds attack..9

Remote and hybrid work..9

Use of artificial intelligence in cybersecurity..................9

Notable cybersecurity events... 11

Events in 2013..11

Events in 2014..11

Events in 2015 and 2016...12

Events in 2017..12

Events in 2018..13

Events in 2019......14

Events in 2020......14

2021-2023 and beyond......14

Notable shifts impacting cybersecurity 15

Cybersecurity threats evolution......17

Building blocks of cybersecurity 18

Traditional cybersecurity measures 19

Conclusion 20

Points to remember......21

Key terms 21

References 23

2. Cybersecurity: Understanding Today's Security Challenges..25

Introduction 25

Structure 26

Objectives 26

Distributed systems 26

Relatively easy to permeate......27

Security challenges of distributed systems 27

Lack visibility......27

Difficult to manage 29

Digital age: Cybersecurity threats......29

Sources of cyber threats......30

Digital age: Cybersecurity attacks......31

Malware attacks......31

Ransomware attacks......33

Cryptojacking attacks......34

Supply chain attacks......35

Social engineering attacks 36

Phishing attacks 36

Generative artificial intelligence phishing attacks......38

Internet of Things attacks......38

Smart medical devices and Electronic Medical Records vulnerabilities..................................39
Privacy concerns of connected cars 39
Cloud attacks 40
State-sponsored attacks..40
Insider attacks..41
Man-in-the-middle attack...41
Denial-of-Service attack..42
Injection attacks..43
Digital age: Cybersecurity key issues 44
Budgets issue 44
The skills gap issue 45
Artificial intelligence issues..45
Conclusion 46
Points to remember..47
Key terms 47
References 48

3. Emerging Cybersecurity Trends..49
Introduction 49
Structure 49
Objectives 50
Cybersecurity trends 50
Trend 1: Tenacious data breaches..50
Trend 2: Upsurging ransomware..51
Trend 3: Smarter social engineering attacks.......................51
Trend 4: Imminent cloud security threats 51
Trend 5: Threat emanating due to mobile devices...............52
Trend 6: Evolving IoT threats..53
Trend 7: Growing power of AI..53
Trend 8: Intensifying cyber warfare by rogue nations........53
Trend 9: Improving MFA..54

Trend 10: Enhanced automation..54

Trend 11: Rise of data privacy...55

Trend 12: Risks of distributive workforce 55

Trend 13: Rise in insider threats..56

Trend 14: Widening IT skills gap 56

Trend 15: Rising threats of Deepfakes 56

Trend 16: More supply chain attacks..................................57

Trend 17: Continued prominence of regulations 57

Trend 18: Emphasis on incident response and recovery.....58

Trend 19: Cyber resilience..58

Trend 20: A board room agenda...58

Cybersecurity future trends 58

Future trend 1: Zero trust 59

Future trend 2: Cryptography resistant to quantum computing..60

Future trend 3: 5G network security.................................60

Future trend 4: Stronger authentication measures 60

Future trend 5: Human-centric security............................60

Future trend 6: cyber insurance 61

Future trend 7: AI-assisted security testing.......................61

Future trend 8: AI-driven cybercrime 62

Future trend 9: Smart cities and critical infrastructure security..62

Future trend 10: Ethical hacking and bug bounty programs 62

Common themes in trends 62

Understanding cyber resilience 64

Importance of cyber resilience 64

Building blocks of cyber resilience 65

Conclusion 67

Points to remember...67

Key terms 68

4. The Need for Cybersecurity Mesh Architecture................69

Introduction..69

Structure..70

Objectives..70

The current situation of cybersecurity ecosystem 70

CSMA explained 71

Illustrating the layers of CSMA 71

The need for CSMA 72

Challenge 1: Data deluge...73

Challenge 2: Data analysis 74

Challenge 3: Real-time security monitoring.....................75

Challenge 4: Attackers think holistically..........................76

Challenge 5: Disjointed perimeter 77

Challenge 6: Adoption of multi-cloud strategy 78

Benefits of CSMA...78

Enhancement of visibility 79

Reduction in complexity..81

Enhanced sharing of intelligence.....................................81

Enhanced automation 82

Consolidation of security products 83

Security analytics 84

Conclusion 85

Points to remember...86

Key terms 87

5. Fundamental Components of Cybersecurity Mesh Architecture 89

Introduction..89

Structure..89

Objectives..89

A re-look at CSMA...90

CSMA working relationship with zero trust.....................91

CSMA's scalability relative to other architectures 92

Working of CSMA..92

Key components of CSMA...92

Integrated data..93

Distributed identity fabric..94

Comprehensive security intelligence 94

Automated operations..95

Centralized operations...95

Consolidated dashboards...96

CSMA's most important component 96

The unified architecture of CSMA 96

Extensive 97

Integrated...97

Accelerated through automation 98

Major products/solutions of CSMA 98

Conclusion 102

Points to remember...103

Key terms 104

6. How to Effectively Adopt Cybersecurity Mesh Architecture 107

Introduction 107

Structure 107

Objectives 108

Performance..108

Problem with past solutions 108

Answer lies in the unified architecture............................110

Cybersecurity landscape of today 110

Attack surface expansion 111

Adoption of cloud..112

Key aspects for CSMA adoption....................................... 113

Integration 113

Comprehensiveness *114*

Automation *114*

Getting started with CSMA 115

Assess current tools and identify gaps *116*

Build the key components *116*

Evaluate compatible tools *117*

Consider befitting vendor(s) *118*

Seek consolidation *118*

Review and revise *119*

Key factors to consider while adopting CSMA 119

Conclusion 122

Points to remember 123

Key terms 123

7. Benefits of Adopting Cybersecurity Mesh Architecture....125

Introduction 125

Structure 126

Objectives 126

What is the necessity of CSMA 127

Benefits of leveraging CSMA 127

Enhanced agility and flexibility *128*

Enhanced security intelligence *128*

Enhanced incident response *129*

Efficient compliance *131*

Enhanced savings *131*

Characteristics of a CSMA strategy 131

Target use cases 133

Security operations *133*

Vulnerability management *133*

Compliance management *134*

Features to be considered for CSMA solutions 134

API Graph *134*

Data normalization and correlation 134
Natural language processing..135
Generative AI for context enhancement............................135
Pitfalls of not leveraging CSMA 135
Increased security overheads..136
Increased security risk 137
Inefficient security incident management 138
Restricted decision-making..139
Conclusion 141
Points to remember...141
Key terms 142

8. CSMA Best Practices 143
Introduction 143
Structure 143
Objectives 144
CSMA vs. defense-in-depth approach 144
Salient points and goals of CSMA....................................147
CSMA needs to be vendor-agnostic..................................149
Systematic approach to implementing CSMA.................150
CSMA standouts (in comparison to other architectures).152
CSMA key performance indicators 153
The ten commandments of CSMA 154
Challenges in implementing CSMA.................................158
Conclusion 159
Points to remember...159
Key terms 160

9. Potential Outlook for CSMA Adoption 161
Introduction 161
Structure 161
Objectives 162

Work-from-home environment..162

Zero-trust network access...162

Endpoint detection and response.....................................163

Home network security...164

OT security environment..166

CSMA in the healthcare industry 167

Summarizing CSMA in healthcare 170

CSMA...170

Global market overview and growth factors.....................171

Market dynamics..172

Driver: Management of evolving threat landscape.....172

Threat: Shortage of skilled expertise...........................172

Opportunity: Growing adoption of multi-cloud.........173

Conclusion 174

Points to remember...174

Key terms 177

Multiple choice questions..178

Answer key 180

Index...183-189

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