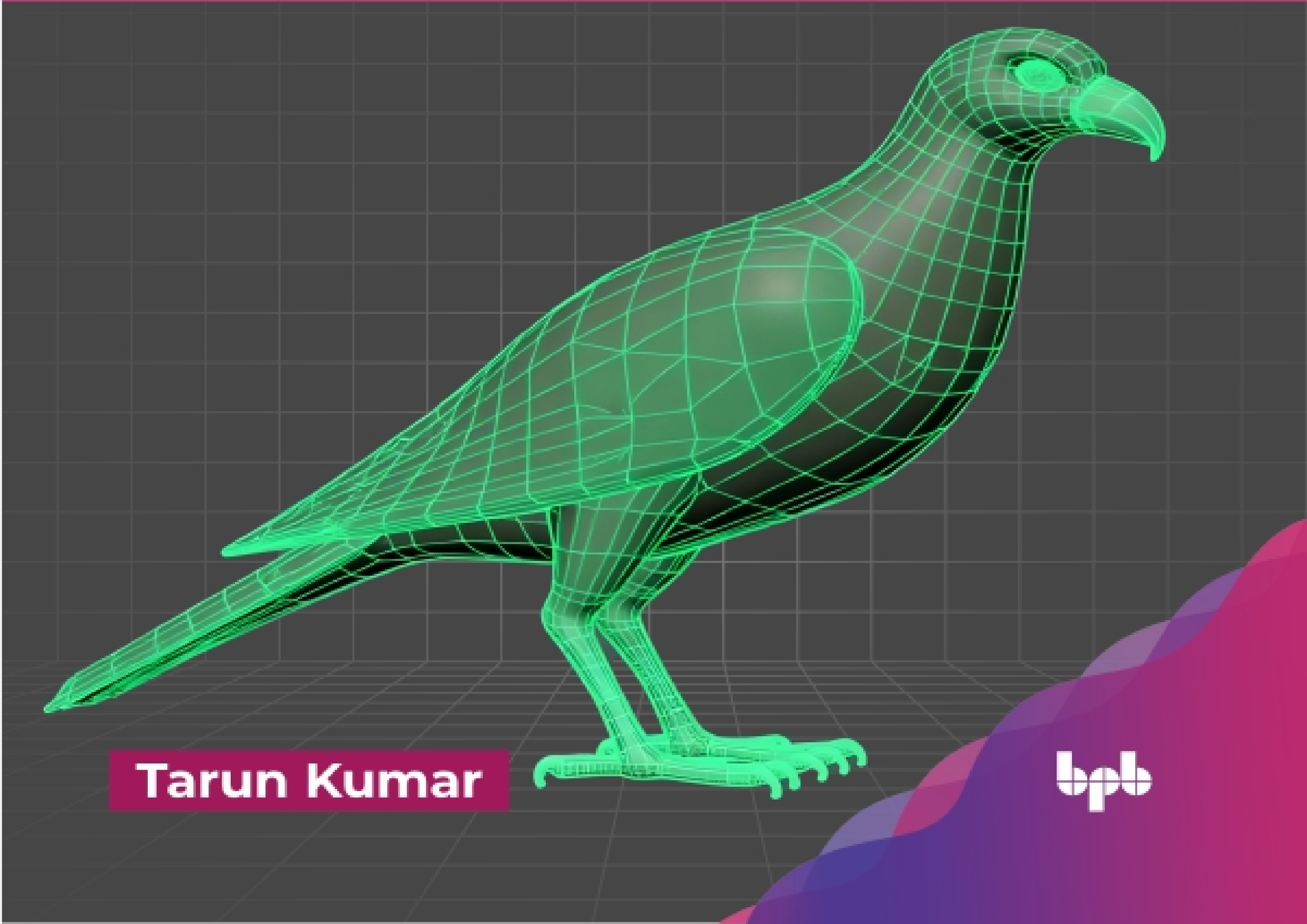
Pocket Guide

The Cybersecurity Mesh Architecture

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



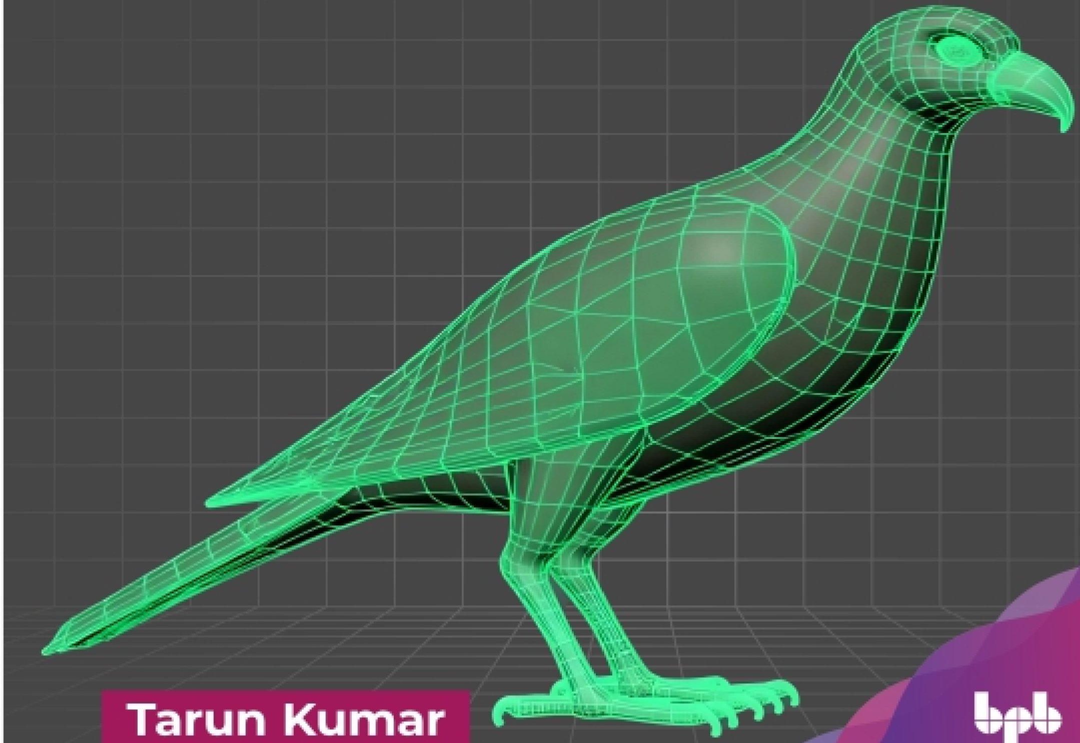
Tarun Kumar

bpb

Pocket Guide

The Cybersecurity Mesh Architecture

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



Tarun Kumar

bpb

The Cybersecurity Mesh Architecture

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

Tarun Kumar

www.bpbonline.com

First Edition 2025

Copyright © BPB Publications, India

ISBN: 978-93-65891-218

All Rights Reserved. No part of this publication may be reproduced, distributed or transmitted in any form or by any means or stored in a database or retrieval system, without the prior written permission of the publisher with the exception to the program listings which may be entered, stored and executed in a computer system, but they can not be reproduced by the means of publication, photocopy, recording, or by any electronic and mechanical means.

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.

To View Complete
BPB Publications Catalogue
Scan the QR Code:

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 Cyber Security 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.

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

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 been growing since the 1940s. Even when networks did not exist, theorists were getting prepared for the risks that may emerge with the advancement of technology.

In this chapter, we will explore the history and evolution of cybersecurity—from the age of the first computer threats to the rise of risks due to the advent of artificial intelligence and cloud computing.

Evolution of cybersecurity

The evolution of cybersecurity has been hand in glove with the developments in communication technology. Thereafter, its evolution has been influenced by developments in geopolitical tensions and major global events.

For the sake of discussion, let us keep our focus on developments in technology. Over the years, we have progressed from telegraphs to smartphones. With this, the types of cyberattacks have transformed from Morris Worm (refer to *The first DoS attack* section) to Stuxnet (refer to *Stuxnet* section for details), to Snake ransomware. Also, to secure data and communication, we have dealt with simple ciphers to sophisticated algorithms.

There have been umpteen incidents in our history that have influenced the developments in cybersecurity. However, it is not feasible to describe all of them. While we look back in history, some crucial junctures need to be given their due importance and thus cannot go unnoticed.

Let us take the time capsule and go back to the 1940s.

Time before networking

1943 saw the arrival of the first digital computer. Interestingly, electronic machines existed which, were not networked. Moreover, only a small group of people had access, and many did not know how to operate them. Hence, cyberattacks were challenging to execute because the threat was virtually non-existent.

It is very intriguing to note that the theory regarding computer viruses first came to the fore in the late 1940s. This was when the computer pioneer, *John von Neumann,* first raised the prospect of computer programs reproducing themselves.

Time of phone phreaks

In the 1950s, telephone use came into being, and a new phrase, **phone phreaks**, was coined. Phone phreaking became prevalent in the late 1950s. The phrase refers to various practices used by *Phreaks* or those interested in the functioning of phones and tampering with their protocols. This allowed telecom experts to operate remotely on the network and place free calls, thus avoiding paying long-distance charges. The initial purpose of hacking was not *information gathering*, which it is now.

Though phone phreaking practice gradually disappeared in the 1980s (after creating havoc for almost three decades), phone providers (who can be compared to today's enterprises) were powerless to halt the phreaks (who can be compared to today's cyber attackers).

Time of early hacking

The 1960s saw the arrival of massive mainframes that were kept in controlled environments. Even for programmers, access was restricted because these computer devices were a high expense.

The majority of the development of the phrase **hacking** took place during this decade. It was again not the motive of *information gathering* by which the hacking took place, rather it was driven by the motive of breaking into high-tech machines to alter their functionality.

In this decade, the idea of hacking shifted to computers. We would rather term it **early hacking**. As discussed, the motive of hacking was not big business; the motive of these early hacking incidents was to gain access to systems. Hacking was not performed for political or economic gains, it was primarily to ascertain if messing up with computers was possible. It not only remained a new concept, newer, faster, and more innovative, hacking techniques also started to emerge during this decade.

In 1967, IBM invited some students to see the newly made computer system. The students were provided training on various system components of the computer system so that IBM could gather information about the system's weaknesses.

As a result, the idea and concept of implementing *defensive security measures* to prevent hacking came into effect. We can state that IBM allowed the students to perform **ethical hacking** (rather, this could be the first time ethical hacking was performed in the industry).

Nowadays, we all know that ethical hacking has become a highly sought-after profession (skill). On reflection, big strides in cybersecurity developments took place in this decade. The years to follow saw an increase in computer use. The size of computers not only decreased (became compact), but due to their affordability, enterprises/businesses started to use them to store data.

Another entrant to the scene was **passwords** which were used to access and secure computers.

Time of ARPANET and the Creeper and Reaper

The actual start (and need) of cybersecurity was seen in the 1970s. The **Advanced Research Projects Agency Network** (**ARPANET**), also known as **Early Internet**, came up during this time. In fact, ARPANET (the connectivity) network was built before the Internet was created. '*I'm the Creeper; catch me if you can!*' was printed using a program developed by an ARPANET developer using PCs connected to the network. For the first time, this program switched from one machine (mainframe computers) to another by itself. The Creeper, therefore, is viewed as the world's first Computer Worm (code that could be transported between machines), although it was not destructive in nature.

A program called **Reaper** was created by another ARPANET researcher which was designed to move through ARPANET deleting copies of Creeper worm. The Reaper is known as the first **anti-virus**.

Decade of commercial antivirus

The two terms: **Trojan horse** (when early malware specimens emerged) and **computer virus** made a formal announcement during this time.

We all remember this time of the Cold War between the United States and the Soviet Union, which led to an increase in the threat of cyber espionage. In 1985, the Trusted Computer System Evaluation Criteria, also referred to as **The Orange Book**, was published by the US Department of Defense, that guided on:

- Assessing the grade of trust to be placed in software that processes classified/sensitive information.

- The security measures needed by manufacturers to be built into their commercial products.

This is the decade when the history of **computer crime** took shape. Consequently, cybersecurity started to be taken more seriously. Savvy users quickly learned to monitor the command.com file size, having noticed that an increase in size was the first sign of potential infection. Although there are claims for the innovator of the first antivirus product, 1987 is widely regarded as the birth year of **commercial antivirus** because:

- The first antivirus was released by German inventors (*Andreas Luneng* and *Kai Figge*).
- Version 1.0 of NOD antivirus was created by 3 Czechoslovakians
- First VirusScan was released by McAfee (now Intel Security)
- Anti4us and Flushot Plus (commercial antivirus programs) were released.

The first DoS attack

The first DoS attack took place due to an unintentional error in a computer worm (Morris worm) code. This code was intended to gauge the size of the Internet. The error caused the worm to replicate continually to the point that the ARPANET was clogged, and 10% of all the systems that were connected crashed. *Robert T. Morris*, the person who created the Morris worm, was the first person to be charged under the Computer Fraud and Abuse Act.

Connected world

This decade gave us the growth and development of the Internet (beyond proportions). The cybersecurity domain expanded along with it. Many significant developments in computer security took place in this decade, such as:

- Fears of **polymorphic viruses** emerged since it was difficult to detect. 1990 witnessed a code that altered itself while spreading through computing systems.

- In 1995, the **Secure Sockets Layer** (**SSL**) protocol was developed by Netscape as a way to keep people secure online data and securely use Internet transactions and browse. Later, it would act as the foundation for **HyperText Transfer Protocol Secure** (**HTTPS**).

The time of email

Towards the end of the 1990s, email was revolutionizing communication and was growing in leaps and bounds. However, it also opened up a new entry avenue for viruses.

1999 witnessed the release of the Melissa virus. The virus found its way into the user's computer through MS Word and then emailed copies of itself to the first 50 email addresses in Microsoft Outlook. The damage costed around $80 million to fix.

Cybersecurity threat canvas expansion

The 2000s witnessed further growth of the Internet. The majority of homes and enterprises (businesses) now had computers and this presented new opportunities for cybercriminals. This was the time when infections on websites and instant messaging systems were on the rise. This decade also led to an increase in hacks of credit cards (credit card data leaks).

With the proliferation of the Internet across homes and offices globally, there were more devices and software vulnerabilities for cybercriminals to exploit than before. As more data were being kept digitally, there was more to steal:

- In 2001, a new technique to infect computer systems appeared where there was no need for users to download files to get their systems infected (they were simply required to visit an infected website). Bad actors could replace clean pages with infected ones or *hide* malware on legitimate web pages.
- Also, worms designed to propagate via **Internet Chat Relay** (**IRC**) channel had arrived and instant messaging services also began to get attacked.
- The term **zero day** attack was coined during this time and this was the time of these attacks were making news. Zero day attack would mean

exploiting *holes* in security for new applications and software (with an attack taking place when hackers exploit the flaw before being addressed by the developers).

- The development of zero-day attacks led to antivirus becoming less effective.
- Another innovation in this decade was **operating system** (**OS**) security – Cybersecurity, that is built into the OS, providing an additional layer of protection. This includes performing regular OS patch updates, installing updated antivirus and software, firewalls, and secure accounts with user management.
- Smartphones also proliferated, and this required antivirus software to be developed for Android and Windows mobiles.

The Anonymous

2003 saw the debut of Anonymous, a popular hacktivist group. The objective of carrying out attacks by the group is to expose high-profile targets and garner attention regarding its political views.

Operation Aurora

Until now, no one had thought that Cyber operations could be used as a tool to carry out industrial espionage at a large scale. Operation Aurora, a series of cyberattacks brought this to the fore. The attack was sponsored by the Chinese Government and targeted the intellectual property of many U.S. private-sector companies, including Google, Yahoo, and Adobe.

Stuxnet

Multiple Windows zero-day vulnerabilities were exploited by Stuxnet (a sophisticated computer worm). It is alleged to have been created by a secret U.S.-Israeli program to target and destroy centrifuges at the uranium enrichment facility in Iran, causing extensive damage to its nuclear program.

Cybercriminals had newer opportunities to exploit owing to the increase in connectedness and ongoing digitization.

General Data Protection Regulation

The **General Data Protection Regulation** (**GDPR**) is a compliance regulation that provides citizens of the **European Union** (**EU**) greater control over their personal data. Under this directive, organizations are responsible for safeguarding the personal data and privacy of EU citizens. The GDPR applies not only to all the organizations within the EU but also to organizations outside of the EU that offer goods/services to customers/businesses in the EU. It was approved by the European Parliament in April 2016 and came into force on May 25, 2018.

The X hack

This year witnessed dramatic cybersecurity incidents that involved X (formerly Twitter) accounts of prominent users getting hacked.

A new category of the breach was coined with this, viz., **Insider Threat**. Whether it is the actions of a negligent employee/or malicious insider, it went on to showcase that humans are the weakest link in the cybersecurity chain.

The SolarWinds attack

The above-mentioned X hack was quite dramatic, however a more ill-famed hack related to supply chain was unfolded in 2020. This was the exploit of SolarWinds which caused aftershocks globally (the full consequences of the attack are still largely unknown).

The SolarWinds *Supply Chain Attack* is a global hack, as threat actors turned the SolarWinds' Orion software into a weapon gaining access to several government systems and thousands of private systems around the world. The cybercriminals were able to corrupt one of the servers which provided access to patches and updates for SolarWinds Orion software.

Remote and hybrid work

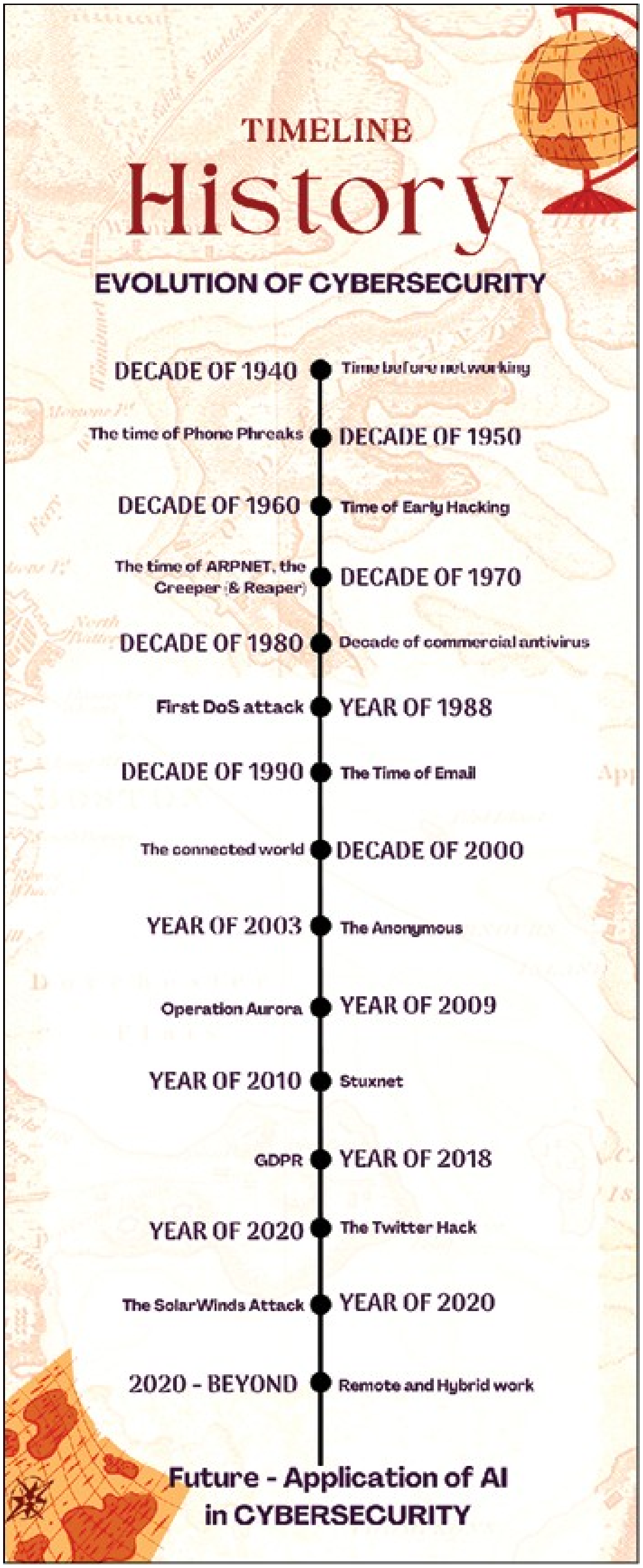
The times of the COVID-19 pandemic witnessed remote work model being adopted by most enterprises (businesses), not by design, but in the wake of the circumstances. Though this transition was not easy for many organizations, we are still witnessing hybrid work scenarios in place even after the pandemic has ended. We have seen a rise in the use of work tools to enable smooth team work remotely. With this, the security aspect has rapidly evolved well and is expected to continue in the future. Techniques such as **multi-factor authentication** (**MFA**), better encryption techniques, principles of zero trust, etc. are becoming commonplace.

Use of artificial intelligence in cybersecurity

The aspect of real-time detection of threats and automated incident response is improving continuously, thanks to the efficient **machine learning** (**ML**) algorithms and integration of AI (rather seamless) in cybersecurity. Cyber-attacks can be detected in early stages (can also be pre-empted in cases) since threat correlation engines are becoming more refined (therefore more effective). These are in effect becoming pivotal defence mechanisms for enterprises (businesses).

As we look at these milestones in cybersecurity, it becomes apparent that the threat landscape is constantly evolving. Cyberattacks are not only a concern for enterprises (businesses) and governments but also a fear for every individual who is on the Internet. All entities are equally susceptible.

The following figure displays the evolution of cybersecurity along with a timeline view:



TIMELINE

History

EVOLUTION OF CYBERSECURITY

DECADE OF 1940 — Time before networking

The time of Phone Phreaks — DECADE OF 1950

DECADE OF 1960 — Time of Early Hacking

The time of ARPNET, the Creeper (& Reaper) — DECADE OF 1970

DECADE OF 1980 — Decade of commercial antivirus

First DoS attack — YEAR OF 1988

DECADE OF 1990 — The Time of Email

The connected world — DECADE OF 2000

YEAR OF 2003 — The Anonymous

Operation Aurora — YEAR OF 2009

YEAR OF 2010 — Stuxnet

GDPR — YEAR OF 2018

YEAR OF 2020 — The Twitter Hack

The SolarWinds Attack — YEAR OF 2020

2020 - BEYOND — Remote and Hybrid work

Future - Application of AI in CYBERSECURITY

***Figure 1.1:** Timeline view of evolution of cybersecurity*

Notable cybersecurity events

The story of the evolution of cybersecurity will be incomplete without a brief mention of some of the notable and unique cybersecurity incidents/breaches that took place between 2013 and most recently impacting the national security of countries and costing enterprises (businesses) millions.

Events in 2013

Some of the noteworthy events of 2013 are listed as follows:

- **Singaporean government:** Anonymous (a hacktivist group) launched cyberattacks on the Singaporean government. These were a series of assaults in revenge for Singapore's censorship laws for the Internet.
- **Israeli government:** Hacktivists targeted the Israeli government touting the campaign as #OpIsrael (which was tied with Holocaust Remembrance Day). This became an annual synchronized cyberattack (using many methods such as DDoS).
- **NSA:** *Edward Snowden*, a former CIA employee (US Government), copied and leaked classified information from the National Security Agency. The leaked documents were passed on to The Guardian, who made them public.
- **Target:** Security lapse at Target (US retailer) resulted in the exposure of the personal information of 70 million consumers (in addition to the credit card information of tens of millions of shoppers).

Events in 2014

Some of the noteworthy events of 2014 are listed below:

- **Home Depot:** Credit card information of customers of the Home Dept (US Retailer) was exposed due to specially crafted malware. The hackers first breached the Home Depot’s network using credentials that were stolen from a service vendor and then installed the malware on the retailer's machines (self-checkout): Quantum – 56 million.

- **Sony Pictures Entertainment:** Confidential data of executives (salaries, employee details, plans for future films, and some film scripts) was leaked by a hacker group (Guardians of Peace). The investigation concluded government of North Korea was behind the attack.

Globally, it is reported that the number of data breaches in 2014 was about 50% more as compared to 2013.

Events in 2015 and 2016

Some of the noteworthy events of 2015 and 2016 are listed below:

- **Experian data breach:** User records at Experian (a global data analytics and consumer credit reporting company) were compromised. This was due to a human mistake in a customer verification process: Quantum – 15 million.
- **Snapchat data leak:** An unnamed hacker/organization had posted the phone numbers and usernames of Snapchat users online for free: Quantum ~4.6 million.
- **Democratic National Committee (DNC) data breach**
    - The DNC computer network was breached by Cozy Bear and Fancy Bear (part of Russian intelligence agencies).
    - This case is often covered as cybercrime in politics as it was alleged to be carried out by Russia in support of Donald Trump (during the U.S. Presidential election of 2016).

Events in 2017

Some of the noteworthy events of 2017 are listed below:

- **Equifax breach:** A data breach at Equifax (the American credit reporting agency) exposed the personal details of about 145+ million people.
- **The Shadow Brokers leaks:** A hacker group (named The Shadow Brokers) leaked EternalBlue, a hacking tool used by the National

Security Agency. EnterrnalBlue is an exploit that utilizes vulnerabilities in the Server Message Block protocol of Windows.

- **WannaCry ransomworm attack:** World's first and most infamous ransomworm targeted Windows computer systems (globally) infecting 200,000+ computers in one day.
- **NotPetya ransomware attack:** Petya and NotPetya are malware that encrypt data. In June 2017, NotPetya was used to perpetrate a cyberattack globally. WannaCry and NotPetya used the EternalBlue exploit to affect unpatched computers.
- **Bad Rabbit ransomware attack:** Bad Rabbit ransomware spreads through drive-by attacks. It appeared as an update for Adobe Flash (masquerading) that tricked users into downloading it. It asked for $280 in Bitcoin (providing a 40-hour deadline).

Events in 2018

Some of the noteworthy events of 2018 are listed as follows:

- **Privacy concerns at Facebook:** Access tokens (that were stolen) were used to expose the accounts of millions of individuals on Facebook. This was ultimately made public by the company.
- **Marriott cyberattack:** Marriott's reservation system was compromised. The data breach went unnoticed for 4 years (probably took place in 2014, however, was hidden), and impacted 500 million guests of the hotel.
- **British Airways cyberattack:** Hundreds of thousands of records (personal data of customers and employees) were breached.
- **California Consumer Privacy Act (CCPA) signed into law:** Due to the increase in complexity and sophistication of cyber threats, CCPA was signed into law in 2018 and it went into effect in 2020. It included an array of privacy rights for consumers and obligations for businesses concerning the collection and sale of personal information.

Events in 2019

Some of the noteworthy events of 2019 are listed as follows:

- **Singapore’s health sectors’ breaches:** 30+ breaches took place in Singapore’s healthcare sector in 2019 alone. The number increased to 80+ in 2020.
- **Attacks on the New Zealand stock market:** New Zealand’s stock market came to a grinding halt due to multiple DDoS attacks.

Events in 2020

This was the year of COVID-19 and proved challenging for cybersecurity professionals. The year witnessed cybercriminals continued illegal activities. Some of the important data breaches of 2020 are listed below:

- Personal information of MGM Resorts Hotels guests was leaked on a hacking forum: Quantum – 10+ million.
- Facebook profiles were available on the dark web for sale: Quantum – 250+ million.
- Zoom accounts were available on the dark web for sale: Quantum - 500k+.
- Cognizant Technology Solutions was subjected to a ransomware attack (perpetrated by the Maze group).

2021-2023 and beyond

These years continued to see many cyberattacks. These cyberattacks can be categorized as data breaches, ransomware, and data extortion attacks and they have had a broad impact on enterprises (businesses) during this time and are expected to continue in the future. Amongst these categories of cyberattacks, the most prevalent risk to any enterprise’s data security is ransomware. Unfortunately, over these years, the world has witnessed its use and ransomware attacks have been on the rise.

According to *Verizon's Report,* 2023, external threat actors are responsible for the vast majority (83%) of breaches, and financial gain accounts for almost all (95%) breaches.

The positive development is in the form of cybersecurity markets that have been expanding fast as well. According to Statista (Global Statistics portal for Market Data, Market Research and Market Studies), the size of the cybersecurity market worldwide by 2026 is anticipated to increase to $345.4 billion.

Notable shifts impacting cybersecurity

So far, we have seen the historical timeline of the evolution of cybersecurity and some of the major cybersecurity incidents and breaches that have taken place over decades. Let us now discuss the major shifts that have changed cybersecurity over decades:

- **Personal information or Personally Identifiable Information (PII)**
    - Has become ubiquitous as a result of social media (which occupies a major portion of our time).
    - Has become the most precious product in the current marketplace.
    - Is available in vast amounts and has reshaped the way hacktivists operate (in the earlier days, attackers could have attacked network infrastructure and developed ways to get around firewalls, however, it took time for them to realize that personal information could be an obvious target).
    - Is freely available on the web, hence attackers are increasingly using phishing strategies for data skimming.

There is a dire need to take reasonable measures to protect personal data, like never before.

People realized, for the first time, how easily personal data can be shared and spread without their consent.

- **WannaCry ransomware (2017 event)**: The first ransomware, the biggest and most wide-ranging:
    - Infected over two hundred thousand computers across 150+ countries, holding computers hostage and demanding Bitcoin payments to return them to their owners.

WannaCry showcased a new age of data risk that urged users to sit up and take notice like never before. The attack proved that data breaches were no longer restricted to large enterprises (businesses); they could also invade and damage personal computers.

- **Multi-factor authentication**
    - Due to numerous massive data breaches (high-profile cyberattacks), the use of MFA has been widespread.

MFA protects data and it is now almost mandatory (become the default) for all websites to implement the same.

We have covered a brief history of cybersecurity (1940-Present). We then looked at some notable cybersecurity events from 2010 to date) and then delved into what we believe were the major shifts that had a remarkable impact on cybersecurity.

In summary, these times have witnessed a sea change concerning technological advancements and their impact on cybersecurity. Cybercriminals have continuously been bestowed with new opportunities to exploit due to the increase in connectedness and the ongoing digitization in most aspects of life. It is also evident that cyberattacks and Cybersecurity measures have become sophisticated with time passing.

Here is another dimension to take cognizance of. With the world as connected as it is, let us not forget that Cybersecurity is not only about protecting computer systems but also about protecting people. People have weaknesses, and, like computers, these vulnerabilities can be taken advantage of. *Emotional manipulation* and *social engineering* are being used by hackers to gain access to otherwise secure systems.

Discussion would be incomplete, if we do not mention that in Cybersecurity, we must learn from our past mistakes, and apply the lessons learned to prevent attacks in the future. This is where professionals such as security researchers and ethical hackers come into the picture. The collective effort of Cybersecurity professionals should be to discover and fix vulnerabilities before they are exploited and help make us and our computers safe.

Cybersecurity threats evolution

Cybersecurity threats have been advancing from time immemorial. This section presents a unique perspective of how the threat landscape of cyber threats has evolved periodically (say shifted constantly) over time. Up until this point, we have seen the following five **Life Stages** (**LS**) of cybersecurity threats:

- **LS 1: Virus**

  Refer to section *Decade of Commercial Antivirus – The 1980s* of this chapter, where we discussed how virus attacks against standalone computers prompted the creation of the first antivirus.

- **LS 2: Network**

  Refer to section *Connected World – The 1990s*, the decade that gave us The Internet (growth and development). When cyberattacks started coming in through the Internet, a Firewall was designed to detect and stop them.

- **LS 3: Applications**

  Due to the widespread exploitation of vulnerabilities inside application software, security measures such as the implementation of **Intrusion Prevention Systems** (**IPS**) gathered pace.

- **LS 4: Payload**

  From the 1980s when the world saw the early emergence of malware specimens till the advent of Petya and NotPetya (the encrypting malware), malware became more targeted. It was able to circumvent signature-based defenses, and solutions such as *Anti-bot* and *Sandboxing* became necessary to detect these threats. Therefore, we refer to this advanced threat as **payload malware**.

- **LS 5: Multi-vector**

> Most recent cyberattacks are large-scale and employ multi-vector techniques. The growth in sophistication of cyberattack techniques has rendered the previous forms of Cybersecurity measures (solutions) less effective over time. Cybersecurity solutions for LS 5 threats are required to protect against the present cyber threat landscape adequately. All we need now is advanced threat protection solutions.

Building blocks of cybersecurity

After all that we have discussed and learned in this chapter, cybersecurity revolves around data. The focal facets to be considered are - how is data stored, who has access, what type of access, and how data is transferred.

The most integral aspect is to ensure that the integrity of data is maintained at all times, failing which will render data useless. Protecting the integrity of data should on the forefront of any comprehensive security system. Equally crucial is to harden the security ecosystem with proper access controls. Access to sensitive information should be controlled by applying appropriate access permissions (preventing unauthorized access). Access controls also play an important role in monitoring and logging an entire IT ecosystem.

Identity and Access Management (**IAM**) needs to be mentioned which allows enterprises (businesses) to organize teams in a security-centric way. Due to changes in roles, personnel, and business needs and goals over time, data access is a moving target. Data access permissions should reflect these dynamic changes.

Finally, availability, of not just data but of services and tools, is critical to the day-to-day functioning of an enterprise. All network-based threats, DDoS, and Malware attacks need to be remediated, or else they have the potential to shut down entire IT systems.

Traditional cybersecurity measures

As the threat landscape has evolved, the cybersecurity measures have advanced as well, however as point solutions (i.e., specific to threats, targeting single elements of the security landscape). It would be reasonable to state that cybersecurity measures have been siloed. This method of securing IT systems involves pinpointing a problem area, such as the need for a Firewall, and using a single solution to fill the one defense gap. This creates a silo.

We mentioned IAM solutions above that cover access controls (permissions), authorization, and authentication. However, IAM is just a one-part solution in any comprehensive security ecosystem. Similarly, network security tools, like perimeter defense solutions, traffic flow monitoring, intrusion detection, and DDoS protection, cover another section of an enterprise' (business') security needs. Likewise, encryption, web application security, threat intelligence, data loss prevention solutions, etc. are some other types of security solutions that are part of a holistic cybersecurity ecosystem.

Considering that the ecosystem has become too complex, cybersecurity silos are not effective. The advent of a hybrid work environment (home workers, on-premises resources) and technologies such as the Cloud (edge devices) have added to a complex web of security risks. Siloed treatment, therefore, leads to a lack of visibility and control.

A major issue with using a siloed approach is that attackers can avoid detection. For example, an attacker might use a trusted platform, like a penetration tool to install malware or create a communication channel between a trusted server and a malicious server. Next, the attacker exfiltrates data using the communication channel to the malicious server. Assuming the trusted server regularly sends data to external servers, this kind of data transfer will not seem unusual. What is missed is the fact that penetration testing may set up communication channels for the duration of a test but not keep the channel open for long periods. By using siloed security information systems, we are not able to see connections between events that would look suspicious and prompt further investigation.

Response times in siloed security systems are too slow. These systems are difficult to scale and do not talk to each other, leading to a lack of precision required for remediation and detection. The possibility of human error is also much higher than when using an integrated security solution. Human error can also result from alert fatigue, which in turn can lead to serious lapses in threat preparedness.

Conclusion

It is evident that with the evolution of technology, the domain of cybersecurity has evolved and so have criminals and *bad actors* whose endeavor is to exploit weaknesses in the system to prove a point for personal gains. It is also important to note that the threat actors have continued to thrive against the backdrop of macroeconomic and geopolitical uncertainties. They have incessantly used all the tools and intelligent resources available at their disposal to make their way past corporate defenses.

We have covered a brief history of cybersecurity (1940-Present). We then looked at some notable cybersecurity events from 2010 to date) and then delved into what we believe were the major shifts that had a remarkable impact on cybersecurity. In summary, these times have witnessed a sea change concerning technological advancements and their impact on cybersecurity. Cybercriminals have continuously been bestowed with new opportunities to exploit due to the increase in connectedness and the ongoing digitization in most aspects of life. It is also evident that cyberattacks and cybersecurity measures have become sophisticated with time passing.

Discussion would be incomplete, if we do not mention that in Cybersecurity, we must learn from our past mistakes, and apply the lessons learned to prevent attacks in the future. This is where professionals such as security researchers and ethical hackers come into the picture. The collective effort of Cybersecurity professionals should be to discover and fix vulnerabilities before they are exploited and help make us and our computers safe.

The need of the hour is for each siloed system to be a part of the larger security picture. Network security tools, IAM solutions, Endpoint security, etc. should all be visible and manageable from a centralized place. Since, modern threats have ways of countering or avoiding single-point security controls, a comprehensive view of the enterprises' (business') security environment is a must to detect today's attacks.

In the next chapter, we will understand today's cybersecurity challenges.

Points to remember

- Cyber-attacks take pace daily and are evolving in sophistication constantly
- Milestone cybersecurity events have played a major role in what cybersecurity is today
- Everyone is susceptible to cyber-attacks
- Cyber-attacks perpetrate from insiders as well (in addition from outside)
- It is imperative to stay alert and keep up with important industry trends to keep attacks at bay
- Cyber-attacks will continue to rise in future with their impact becoming more consequence

Key terms

- **Phone phreaks:** Various practices used by *Phreaks* or those who have interest in the functioning of phones and tampering with their protocols.
- **Advanced Research Projects Agency Network:** Referred to as Early Internet (network that was built before Internet was created).
- **Creeper:** World's first computer worm (a code that could be transported between machines).
- **Reaper:** World's first anti-virus.
- **Trojan horse:** Type of malware that downloads onto a computer disguised as a legitimate program.
- **The orange book:** Trusted computer system evaluation criteria published by the US Department of Defense.
- **Denial of service:** Type of cyber-attack wherein a malicious actor renders a device unavailable by interrupting the normal functioning of the device.
- **Polymorphic virus:** Code that alters itself while spreading through computing systems.

- **Secure sockets layer:** It is a protocol to keep people secure online data and securely use Internet transactions.
- **Hyper text transfer secure:** Is the secure version of HTTP (protocol that enables transfer of data between web browser and website. HTTPS encrypts the data transfer.
- **Internet chat relay:** This is a chat system based on text for instant messaging.
- **Zero day attack:** Attack exploiting holes in security for new applications and software (exploiting the flaw before they are addressed by the developers)
- **General data protection regulation:** A compliance regulation that provides citizens of the EU greater control over their personal data.
- **Insider threat:** Cybersecurity threats that begin with authorized users viz., employees/ contractors/business partners.
- **Supply chain attack:** Cyberattack against enterprises (businesses) suppliers.
- **Multi factor authentication:** Authentication method, a core aspect of a strong identity and access management framework. It mandates a user to provide two or more verification factors to gain access to a computing resource.
- **Distributed denial of service:** Type of DoS attack that involves multiple connected online devices.
- **California consumer privacy act:** A data privacy law in California, US to protect the data and privacy rights of residents.
- **Personally identifiable information:** Any data that could potentially identify a specific individual.
- **Identity and access management:** A framework that aims to control user access to critical information within enterprises (businesses).
- **Artificial intelligence:** The ability of a computer or robot (computer-operated) to perform tasks commonly associated with human beings.
- **Machine learning:** The field of AI that focuses on using data and algorithms to behave the way humans learn.

References

1. https://cybermagazine.com/cyber-security/history-cybersecurity
2. https://www.digitalguardian.com/blog/biggest-moments-cybersecurity-history-past-10-years

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

CHAPTER 2
Cybersecurity: Understanding Today's Security Challenges

Introduction

Through *Chapter 1*, *Cybersecurity: A Dynamic Changing Paradigm*, we realize that the modern cybersecurity threat is complex, diverse, and dynamic. Since time immemorial, we have seen new threats emerge every year. While attackers continuously seek new ways to bypass defenses, cybersecurity professionals are finding newer ways to secure sensitive data. It would be fair to state that people on both sides of the equation (attackers and defenders) are smart and determined.

One of the most significant developments in the cyber world, especially in the last decade, is the expansion of the attack surface. Each end-point (employees working from the office or home) or perimeter device (edge devices, hybrid cloud systems) in an enterprise (business) is a potential entrance (unauthorized) into its internal systems. What exacerbates the issue is their growing numbers.

Let us now concentrate on the systems in an enterprise (business) that are widely distributed in nature and on how their disparateness impacts Cybersecurity. The modern-day infrastructure is not only disparate but also increasing in breadth, which presents new and unique challenges to cybersecurity operations.

Structure

In this chapter, we will cover the following topics:

- Distributed systems

- Security challenges of distributed systems
- Digital age: Cybersecurity threats
- Digital age: Cybersecurity key issues

Objectives

This chapter looks at how disparately distributed systems operate in today's enterprises (businesses) and their impact on cybersecurity. It will also explore varied cybersecurity challenges (threats, attack vectors, and issues).

Distributed systems

Since there is never a one-size-fits-all solution, all large enterprises (businesses) have highly distributed IT systems and face the consequences. Each enterprise (business) has definite organizational and operational needs that must be met, unique ecosystems that must be hardened, and limited resources available to commit to **Security Operations** (**SecOps**).

Consider this common scenario through which enterprises (businesses) distribute their systems: multiple campuses | Branch offices | Multiple public clouds | Edge computing | IoT devices, etc. Many larger enterprises (businesses) will have this distribution or may combine some of these aspects. Now, think about the administrative complexities of managing these resources.

For instance, say your business operations are spread across several offices. Each office's devices, network, and on-premises computing resources will need to be secured. The enterprise (business) would likely be using cloud technologies in day-to-day operations given its advantages in doing so. Additionally, for each office, communications between public clouds and on-premises devices/applications would need to be secured. Consequently, the volume of data will increase, leading to an increase in log data to sift through. There will also be a dire need for the right-set visibility of data across the enterprise (business). This is how inherently the ecosystem of distributed systems works.

Relatively easy to permeate

In distributed systems, various sub-systems (e.g., network communication/user or device authentication) need to communicate with one another. Both networks and authentication events need to be monitored. Moreover, edge computing, remote offices, and other external devices need access to company networks and systems. This means opening the door for legitimate communication.

Authentication presents a similar problem. Each user or device attempting to access the network has to be treated as a potential security incident. Given the rise in phishing attacks, user devices are particularly vulnerable to becoming carriers of malicious code. Legitimate users can be hijacked by attacker code, not only from phishing threats but also from compromised web applications that inject malicious code into user devices.

Public cloud is one of the biggest security concerns nowadays. Public cloud adoption leads to an increase in configuration and management overhead, new authentication challenges, and increased network monitoring requirements.

Security challenges of distributed systems

The main problems with distributed ecosystems that make it difficult to be hardened at all times are that they are *relatively easy to permeate*, *lack visibility*, and are *difficult to manage*, given their dispersed nature.

Let us take these problems one at a time.

Lack visibility

The ecosystem of any distributed system comprises many applications, servers, and services. This makes the ecosystem difficult to monitor. On one hand, there are many individual elements to monitor, and on the other hand, there is log overload and complexity of communication that make it difficult to see what is transpiring.

Traffic and activity monitoring thus becomes the main pain point as they maneuver through the web of interconnected systems to find a threat's source. Though modern security solutions such as **Security Information and Event Management** (**SIEM**) make it easy to monitor data, analyzing this data is another story. The problem is simply the volume of data generated with SIEM and other solutions. Owing to the overwhelming amount of monitoring data, there is every chance of potential security events (probably breaches) getting lost and unusual usage patterns getting overlooked. Security professionals also suffer from burnout trying to sort through the deluge of information.

The real problem is the visibility of events, not the number of alerts. Data integration is a huge challenge in siloed security solutions (since a large volume of logs and monitoring information comes from different tools/separated regions of the ecosystem), leading to delays in properly integrating that data.

Cybersecurity professionals do not have the luxury of time if a threat event materializes. Any enterprise' (business's) effectiveness in responding to an attack (its readiness) is assessed through a metric referred to as **Mean Time To Detect** (**MTTD**). MTTD is the average time taken to detect a security incident or failure from the time it takes place in a system. The longer a bad actor has access to internal systems, the more damage they can do and the more money and time it will cost an enterprise (business).

Another important metric in this context is **Mean Time To Remediate** (**MTTR**). MTTR is the amount of time taken by an enterprise (business) to neutralize an identified threat or failure within their network environment. Threat remediation is the process used by enterprises (businesses) to identify and resolve threats to their network environment. A threat is a malicious intrusion/infiltration into a system to steal information (that negatively affects operations and/or damages hardware or software).

MTTD and MTTR are vital metrics to consider when assessing the effectiveness of any enterprise's (business's) security systems. With maturity in the cybersecurity posture, these metrics should follow a downward trend as time progresses.

Visibility is not a matter of knowing that an attack is occurring, what matters is whether we have a proper understanding of the threat and whether we have the required context. If, due to a vulnerable port in the infrastructure, a network security alert is noticed, merely closing that port might not be the whole solution. It is important to understand why that specific network was compromised. Comprehensive visibility is required for the cybersecurity staff to understand why the network was compromised (was the device infected with malicious code?). In summary, modern IT ecosystems are large and interconnected, so comprehensive visibility is the key.

Difficult to manage

Distributed systems require well-defined policies to function properly (policy consistency is difficult to maintain across siloed systems). In security Silos, there are different tools/ solutions/resources with different policy control requirements and needs. The policy controls may need to change over time depending on operational requirements and the changing threat landscape. In these scenarios, it is a must to stay agile and adapt to new security threats. Essentially, every day sees new threats emerging and changing attack patterns, prompting security teams to change strategies to meet these new attacks.

Inconsistent application of policies is likely to produce redundant/false alerts, leading to adverse impacts. Also, in siloed security systems, any fixes (not well thought through) to complex problems are likely to create new vulnerabilities.

Digital age: Cybersecurity threats

Actions performed by individuals with wrongful intentions to steal data, cause harm, or disrupt computing systems are treated as **cybersecurity threats**. Threat categories cover malware (ransomware), social engineering, **man-in-the-middle** (**MitM**) attacks, **denial of service** (**DoS**), injection attacks, etc. These threats can come from various sources, such as hostile nation-states, terrorist groups, individual hackers, and trusted employees/contractors, who take advantage of their privileges to perform malicious acts.

Sources of cyber threats

Listed are some of the several common sources of cyber threats against enterprises (businesses):

- **Nation states**: These are hostile countries working to interfere with communications (disrupt other nations) and gain secrets. They are politically/economically motivated to launch cyber-attacks against companies and institutions.

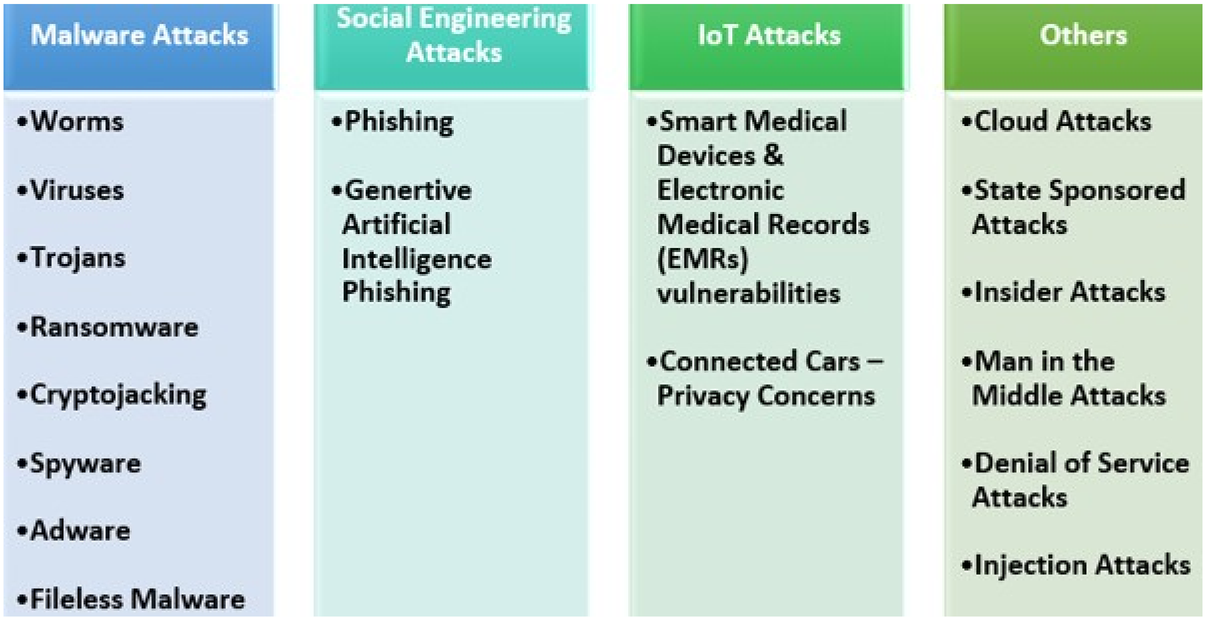
- **Terrorist organizations**: These are terrorists that perpetrate cyber-attacks to harm/destroy critical infrastructure, threaten national security and disrupt economies.
- **Criminal groups**: These are a group of hackers who are well organized to break into computer systems for economic benefit. Phishing, malware, spamming, and spyware are some techniques used for extortion, theft of private information, and online scams.
- **Hackers**: These people are usually motivated by personal gain, financial gain, political activity, or even revenge and use various attack techniques.
- **Malicious insiders**: This is an employee with legitimate access to company resources who abuse their privileges to steal information or damage computing systems for economic or personal gain. Insiders can be employees, contractors, suppliers, or partners of the target organization. They can also, in some cases, be outsiders who may have compromised a privileged account and are impersonating its owner.

Digital age: Cybersecurity attacks

So far with what has been discussed in this chapter, technology is taking over the business. This is because technology has a huge influence on business decision-making and reducing manual work.

Millions of people’s personal information can be exposed as a result of a single security breach. These circumstances can lead to adverse business financial impact and loss of client confidence. Therefore, it is critical to have cybersecurity to safeguard both persons and enterprises (businesses) from spammers and online criminals.

With this backdrop, let us look into some of the challenges facing enterprises (businesses) in the digital age. The following figure lists various attacks, which are subsequently discussed further:



Malware Attacks	Social Engineering Attacks	IoT Attacks	Others
•Worms •Viruses •Trojans •Ransomware •Cryptojacking •Spyware •Adware •Fileless Malware	•Phishing •Genertive Artificial Intelligence Phishing	•Smart Medical Devices & Electronic Medical Records (EMRs) vulnerabilities •Connected Cars – Privacy Concerns	•Cloud Attacks •State Sponsored Attacks •Insider Attacks •Man in the Middle Attacks •Denial of Service Attacks •Injection Attacks

Figure 2.1: *Digital age cybersecurity attacks*

Malware attacks

Malware, also known as **malicious software**, is the most common type of cyberattack and covers viruses, worms, trojans, spyware, and ransomware. Malware perpetrates a system via a link on an untrusted website/email/an unwanted software download. It has a typical way of operation, firstly it gets deployed on the target system, then starts collecting sensitive data, manipulates the system, and may destroy data/or shut down the system altogether.

Here are some of the main types of malware attacks:

- **Viruses**: This is a piece of code that injects itself into an application and on application run, executes the code.
- **Worms**: This is a piece of malware that exploits software vulnerabilities and gains access to computer systems through backdoors. The worms (malware) are behind most of the **Distributed Denial of Service** (**DDoS**) attacks.
- **Trojans**: This is software (malicious code) that looks to be a harmless program and hides itself in apps/games/email attachments. When a user (gullible) downloads the trojan, it gains control of the user's device.

- **Ransomware**: It is a type of malware in which the data on a victim's computer is locked, and payment (monetary ransom) is demanded before the data is unlocked (using a decryption key). There is no guarantee that paying the ransom will lead to the restoration of full access/functionality.
- **Cryptojacking**: This is a type of attack where software is deployed on a user's computer, thereby using its computing resources to generate cryptocurrency (without the user's knowledge).
- **Spyware**: This is an attack where a threat actor gains access to a user's (gullible) sensitive information (via desktop browsers/applications and mobile phones).
- **Adware**: Adware is related to Spyware but it does not install software on users' computers and is not used generally for malicious purposes. However, it can be used without the users' consent and tracks users' browsing activity to determine behavior patterns and interests thereby allowing advertisers to send the user targeted advertising.
- **Fileless malware**: This is an innovative type of malware wherein no software is installed on users' computers and is stealthy in nature. Malicious functions are enabled through editing native files such as WMI and PowerShell. These attacks are difficult to detect, and the computer system believes the compromised file is legitimate. These attacks cannot be detected by traditional antiviruses.

Ransomware attacks

Ransomware is a type of malware in which the data on a victim's computer is locked, and payment (monetary ransom) is demanded before the data is unlocked. After successful payment, access rights are returned to the victim. These attacks are perpetrated by cybercriminals or nation-state-sponsored groups.

The earliest ransomware attacks simply demanded a ransom in exchange for the encryption key needed to regain access to the affected data or use of the infected device. By making regular or continuous data backups, an organization could limit costs from these ransomware attacks and often avoid paying the ransom demand.

However, in recent years, ransomware attacks have evolved to include double-extortion and triple-extortion attacks that raise the stakes considerably—even for victims who rigorously maintain data backups or pay the initial ransom demand. Double-extortion attacks add the threat of stealing the victim's data and leaking it online; on top of that, triple-extortion attacks threaten to use the stolen data to attack the victim's customers or business partners.

These attacks result in a crisis-level operational impact on critical infrastructure and commercial enterprises (businesses), while criminals threaten to publicly release or destroy data if prompt payment is not made. In the past decade, ransomware attacks have evolved from a consumer-level nuisance of fake antivirus products to sophisticated malware with advanced encryption capabilities that now primarily target public and private-sector enterprises (businesses).

Also, ransomware is now one of cybercrime's most profitable and popular business models. It has proven effective and profitable for enterprises. Enterprises (businesses) need a powerful recovery strategy against ransomware attacks. This involves proper planning to recover corporate and customer data and applications.

Take a look at this, cybercriminals do not necessarily need to develop their own ransomware. Some ransomware developers share their malware code with cybercriminals via **Ransomware-as-a-Service** (**RaaS**) arrangements. The cybercriminal, or *affiliate*, uses the code to carry out an attack, and then splits the ransom payment with the developer. It is a mutually beneficial relationship: affiliates can profit from extortion without having to develop their own malware, and developers can increase their profits without launching additional cyberattacks.

One of the best countermeasures against ransomware attacks is **Disaster Recovery as a Service** (**DRaaS**) solution. DRaaS is a cloud computing service model that allows an organization to back up its data and IT infrastructure in a third-party cloud computing environment and provide all the DR orchestration, all through a SaaS solution, to regain access and functionality to IT infrastructure after a disaster (e.g., ransomware Attack). With DRaaS solutions, enterprises (businesses) can automatically back up files, easily identify which backup is clean, and launch a fail-over with the press of a button when malicious attacks corrupt our data.

See how things evolve. Many had touted 2020 as the *Year of Ransomware*. Then came 2021, 2022, and 2023 (and the trend continues).

Listed below are two reports about ransomware attacks:

- Verizon's report found that ransomware was involved in 24% of all breaches.
- Sophos' *The State of Ransomware 2023* found that 66% of organizations experienced a ransomware attack in the past year.

Ransomware threats cannot be ignored, especially as attackers are evolving their tactics.

Cryptojacking attacks

Cryptocurrency has become popular today. Cybercriminals hijack home or work computers to mine for cryptocurrency (like Bitcoin). Mining requires lots of computer processing power. Hence, hackers can make money by stealthily piggybacking on someone's computing resources. For enterprises (businesses), cryptojacked systems can cause serious performance issues and costly downtime.

Supply chain attacks

Supply chain attacks rose to prominence in late 2020, grew through 2021-23, and are likely to continue to be a major threat in 2024. SolarWinds (refer to section *The Solar Winds Attack* from *Chapter 1*, *Cybersecurity: A Dynamic Changing Paradigm*) hack reported in December 2020 led this trend. It involved nation-state actors exploiting an IT performance monitoring system and gaining access to more than 30,000 SolarWinds customers and partners. Threat actors compromised SolarWinds' development environment and inserted backdoor code into its Orion network monitoring product. The discovery of the Sunburst malware kicked off an extended investigation that uncovered the details of the SolarWinds hack, multiple malware variants, and an attack campaign that impacted various public and private sector organizations.

Another high-visibility supply chain exploit in 2021 was the Kaseya Attack, which leveraged the relationships between **Managed Service Providers**

(**MSPs**) and customers to distribute ransomware using MSPs' remote monitoring and management software.

In this light, recount the Log4j zero-day vulnerability exploitation (Log4j is a widely-used Apache logging library). The zero-day vulnerability in the Java-based Apache Log4j library allowed an attacker who could control the contents of log messages or their parameters to achieve remote code execution. This flaw was widely exploited with about 40,000 attempted attacks detected within two hours of it becoming public and over 830,000 attempts within the first three days. While enterprises (businesses) could quickly update the library version they used, the libraries used by their suppliers and partners - and in turn their suppliers and partners, and their suppliers and partners, and so on - needed to be updated to avoid being vulnerable to attack.

The high-profile supply chain attacks have demonstrated that it is a viable and potentially profitable attack vector for cyber threat actors. Going into the future, cyber threat actors are likely to expand their use of supply chain attacks to amplify the reach and impact of their attacks. Organizations must be mindful of the third-party vendors and suppliers they work with. Trust is an inherent value here, but organizations should also do their due diligence in vetting third parties.

Social engineering attacks

Not only are the hackers continually evolving their tactics in the use of technology, but they are also now using weaknesses in psychology to their advantage. Social engineers are hackers who exploit weaknesses in human psychology. Hackers use phone calls and social media to trick people into offering them access to sensitive information.

Let us examine Phishing, the most common type of social engineering attack.

Phishing attacks

A Phishing attack is a type of social engineering attack that targets users' login details and credit card information (this user information benefits the malicious actors). These attacks involve malicious actors to trick employees into revealing sensitive information in many forms. Those forms include email phishing and the more sophisticated and targeted spear phishing, **Business Email Compromise** (**BEC**), whaling, and vishing attacks.

Here are some of the main types of phishing attacks:

- Spear-phishing is a type of phishing attack that targets specific individuals or organizations, typically through malicious emails.
- BEC is a form of phishing attack where a criminal attempt to trick a senior executive (or budget holder) into transferring funds or revealing sensitive information.
- Whaling is a highly targeted phishing attack aimed at senior executives- masquerading as a legitimate email.
- Vishing is short for *voice phishing*, which involves defrauding people over the phone, enticing them to divulge sensitive information.

Phishing attacks are a never-ending challenge faced by organizations of all shapes and sizes, and no company nor employee is immune to attack. According to Verizon's 2023 Report, 18% of all breaches involved were phishing.

Let us simplify this for the readers. If you are a Gmail (Google email service) user, you might come across a spam folder consisting of emails the platform recognizes as a threat to your data security. These spam emails consist of thousands of phishing attacks that your mailing partner recognizes and warns you about the potential cyber threat that it carries. Yet, some communications still make it to your inbox, where you might fall into a trap. Officially, Google released a statement of how it blocks over 100 million phishing emails every day. It further emphasized how most of the communications were trying to impersonate government officials, authorities, agencies, or websites to sound more reliable to mail recipients.

The following are some notable phishing attacks:

- Facebook and Google were scammed out of more than $100 million after attackers impersonated a legitimate partner of the businesses between 2013 and 2015. The phishing scams involved contracts and invoices for funds due.

- Sony Pictures was hacked in 2014 after company executives received phishing emails from a group named Guardians of Peace. The attackers reportedly stole more than 100 TB of data.
- Austrian aircraft supplier FACC was defrauded of $54 million in 2016 after an employee was phished by an attacker, purporting to be the company CEO, who requested a wire transfer to a bank account controlled by the attackers.

Generative artificial intelligence phishing attacks

The year 2023 witnessed the advent of **Generative AI** (**GenAI**) platforms, such as ChatGPT. Along with this came a string of security challenges, especially when it comes to phishing.

GenAI can improve grammar and spelling to help attackers craft more convincing social engineering and phishing scams. However, it can also gather information about people and companies from social media and other websites to conduct targeted spear phishing and BEC campaigns.

A major AI phishing concern is deepfakes. This type of AI creates fake yet convincing audio, image, and video content to fool people into believing their legitimacy. Deepfakes can lead to misinformation campaigns, blackmail, reputational damage, election interference, fraud, and more.

Internet of Things attacks

Internet of Things (**IoT**) is a system of interrelated physical devices which can be accessible through the Internet. The connected physical devices have a **unique identifier** (**UID**) and have the ability to transfer data over a network without any requirements of human-to-human or human-to-computer interaction. The firmware and software that is running on IoT devices make consumers and businesses highly susceptible to cyber-attacks.

Let us view some statistics. In 2024, the number of connected devices is predicted to increase to more than 14.4 billion. IoT Analytics [5] (a leading global provider of market insights and strategic business intelligence for IoT, AI, Cloud, Edge, and Industry 4.0) claims that by 2025, there will be more than 27 billion gadgets online simultaneously.

The IoT sector is the primary target for hackers accessing users' sensitive data. To access your device containing your sensitive information, hackers use devices (IoT gadgets) that surround you, such as wearable smartwatches, baby monitors, smart fridges, smart lights, smart watches, webcams, household appliances, medical devices, automobiles, and even home security systems.

With the expansion of IoT gadgets, it is pivotal to guarantee their security. These gadgets are vulnerable because they often have default setups, lack firmware refreshes, and suffer from inadequate encryption. To avoid unauthorized access and potential breaches, IoT devices must have robust authentication, encryption, and monitoring mechanisms.

Smart medical devices and Electronic Medical Records vulnerabilities

The healthcare industry realizes the benefits of developments in smart medical devices. With this, patient medical records have now moved online. This has led to concerns about cybersecurity threats, privacy, and safety.

As more devices are connected to hospitals and medical facilities, hackers exploit vulnerabilities in their security defenses. This is rendering patient data and information (sensitive information) increasingly vulnerable. The possibility of remote compromise of a device directly connected to a patient always exists. An attacker could theoretically increase or decrease dosages, send electrical signals to a patient, or disable vital sign monitoring.

Privacy concerns of connected cars

As technology evolves, the connected car is becoming more and more ubiquitous. Connected car provides access to various infotainment services, such as music, radio, movies, news updates, and text/WhatsApp notifications. These cars support navigation systems through third-party apps, ensuring real-time traffic updates and route guidance for efficient navigation to destinations.

For hackers, this evolution in automobile manufacturing and design means yet another opportunity to exploit vulnerabilities in insecure systems, steal sensitive data, and harm drivers. In addition to safety concerns, connected cars pose serious privacy concerns.

Cloud attacks

Cloud computing is an innovative modern-day technology that revolutionized the physical world of data storage. Cloud computing has led to improvements in IT efficiency, and provided flexibility and scalability to enterprises (businesses). Due to these advantages, enterprises (businesses) from large to **Micro, Small, and Medium Enterprises** (**MSMEs**) utilize cloud services for storing their data (that includes Corporate and user-sensitive information). On the one hand, its adoption promises a reduction in cost and increased efficiency; on the other, it opens possibilities for data security breaches.

In cloud computing, enterprises (businesses) must understand the *Cloud shared responsibility model*. The model is a working framework followed by **Cloud Service Providers** (**CSP**) that details the responsibility over an entire cloud environment, from infrastructure to hardware, data, identities, workloads, network, settings, and more. Responsibility is divided between the CSP and the customers. Many organizations cannot delineate where CSP responsibilities end and their responsibilities begin, opening them to numerous vulnerabilities.

The exploitation surface for cyber criminals has widened due to using cloud computing services, and enterprises' (businesses') need to address this. The main reasons for compromised data security/that present an opportunity for cyber criminals to exploit are the lack of encryption, multi-factor authentication, improper configuration, insecure APIs, poor access control, shared tenancy, and supply chain vulnerabilities.

State-sponsored attacks

Hackers are eyeing to make a profit by stealing individual and corporate data. Now, nation states are using their cyber skills to infiltrate other governments and perform attacks on their critical infrastructure. Cybercrime, which has been a major threat to the private sector and for individuals so far, has now become a menace for the governments and nations. As we move into the future, state-sponsored attacks are expected to increase, with attacks particularly on critical infrastructure.

Insider attacks

All cybersecurity challenges in enterprises (businesses) do not come alone from the outside; they come from within as well. Insider threats are threats initiated by authorized users (who could be employees, contractors, or business partners) who advertently or inadvertently misuse their legitimate access or have their accounts hijacked by cybercriminals.

While it is the external threats that get noticed (become headlines), insider threats, whether malicious or the result of negligence—can be costly and dangerous for enterprises (businesses). For example, confidential data may be leaked by employees (which can prove extremely detrimental as the data can be used by its competitors. As a result, it can bring significant losses to the company’s finances and reputation.

Look at these reports that indicate that data breaches due to insider threats are costlier than data breaches due to external threats:

- **IBM’s 2023 report**: average cost of a data breach ($4.90 million due to insider threat versus $4.45 million due to external threat).
- **Verizon’s 2023 report**: average compromises due to external threat of ~200 million records versus 1 billion records or more due to insider threat.

Man-in-the-middle attack

This attack involves intercepting the communication between two endpoints, such as a user and an application. The attacker can eavesdrop on the communication, steal sensitive data, and impersonate each party participating in the communication.

Some examples of MitM attacks include:

- **Wi-Fi eavesdropping**: Here, an attacker sets up a Wi-Fi connection (seemingly looking authentic) that people at large may connect to. The fake Wi-Fi allows the attacker to monitor the activity of connected users and intercept sensitive data (login credentials, etc.).
- **Email hijacking**: Here, a legitimate email address of an organization (say that of a Bank) is spoofed by the attacker. Users are tricked (by following instructions they believe have come from the bank, while it is not true) into giving up sensitive information/transferring money to the attacker.

- **Domain name server spoofing**: In this, a **domain name server** (**DNS**) is spoofed, which directs a user to a fake website (seemingly looking authentic). Attack uses this technique to steal the user's credentials.
- **Internet Protocol spoofing**: Here, an attacker spoofs an **Internet Protocol** (**IP**) address (which connects users to a specific website) to pose as a website (which in real is fake).
- **HTTPS spoofing**: The secure version of HTTP is referred to as HTTPS, but this can also trick the browser into thinking that a malicious website is safe. The attacker uses *HTTPS* in the URL to conceal the malicious nature of the website.

Denial-of-Service attack

This attack overloads the target system with a large volume of traffic, hindering the ability of the system to function normally. An attack involving multiple devices is known as a **DDoS attack**.

DoS attack techniques include:

- **HTTP flood DDoS**: In this attack, HTTP requests (seemingly looking authentic) are used to overwhelm an application or web server. The target system is forced to allocate as many resources as possible for each request.
- **SYN flood DDoS**: This attack uses a **transmission control protocol** (**TCP**) connection. TCP connection requires an **synchronize** (**SYN**) request to be sent to the host with a response from the host with SYN-ACK acknowledging the request, and finally a response back from the requester with an ACK. It is possible to mess up with server resources, by sending SYN requests but not responding with the SYN-ACKs. This sequence is exploited by attackers.
- **User datagram protocol flood DDoS**: In this attack, **user datagram protocol** (**UDP**) is used to flood a host with UDP packets sent to random ports. This host then searches for applications on the affected ports and since the packets are not legitimate, the host responds with "Destination Unreachable". This leads to the use of the resources of the host.

- **ICMP flood**: In this attack, inward and outward-bound bandwidth are consumed, as the target is overwhelmed with a barrage of ICMP Echo Request packets. The system is unable to keep pace with the rate of requests, eventually slowing down.
- **Network time protocol amplification**: This attack uses **network time protocol** (**NTP**) servers that are publicly accessible wherein open NTP servers are used to send high volumes of UDP traffic to a targeted server.

Injection attacks

Injection attacks exploit various vulnerabilities to directly insert malicious input into the code of a web application. Successful attacks may expose sensitive information, execute a DoS attack, or compromise the entire system.

Here are some of the main vectors for injection attacks:

- **Structured Query Language injection**: In this attack, an **Structured Query Language** (**SQL**) query is entered into a web form or comment field to exfiltrate data. Since databases in Web applications are based on SQL, they are vulnerable to SQL injection. Also, there are also NoSQL attacks that are targeted against those databases that do not use a relational data structure.
- **Code injection**: In this attack, malicious code is injected into a vulnerable web application. The code is executed by the web server as if it were a legitimate part of the application.
- **OS command injection**: In this attack, command injection vulnerability can be exploited to input commands for the OS to execute, which the attack to exfiltrate OS data or take over the system.
- **Lightweight directory access protocol injection**: In this attack, characters are inputted to alter unsanitized **lightweight directory access protocol** (**LDAP**) queries, making the system vulnerable. Since LDAP servers may store user accounts and credentials for an organization, these kinds of attacks can be severe.

- **XML injection**: In this attack, vulnerabilities in legacy XML parsers are exploited. The attack is perpetrated using specially-made XML documents (which can be used to traverse paths and remotely execute code.
- **Cross-Site Scripting**: In this attack, malicious code (using JavaScript) perpetrates a target browser. The browser executes the code, redirecting users to a malicious website or stealing users' session cookies to hijack the session.

Digital age: Cybersecurity key issues

In addition to the above-mentioned cybersecurity challenges being faced by enterprises (businesses) in the form of Cyber Attacks, other issues need to be addressed by the industry at large. A few of them are given below.

Budgets issue

Cybersecurity is seen as a cost center by enterprises (businesses) because it is difficult to calculate its **return on investment** (**ROI**). With time, as its importance has increased, it has been relatively safe from the perspective of budget and staff cuts. However, it is not immune from them. **Chief information security officers** (**CISOs**) and security teams can face budget cuts and reductions in spending (we saw this happen during COVID-19).

High-interest rates environment (as it is now), high inflation, recession fears, and geopolitical uncertainty are all extraneous factors and will continue to plague the IT industry (in response to which enterprises (businesses) resort to budgets and staff cuts. In such circumstances, they must plan carefully to maintain the security posture of their enterprise (business) without burning themselves out. It is not easy to get more done with less.

The skills gap issue

Skills shortage is not new to the world of the cybersecurity industry. We have been hearing this consistently for many years that the industry needs more security staff than are available to hire. There is a demand-supply issue. Budget cuts and layoffs make things worse, as this means the same amount of work is expected to be completed by fewer staff members.

According to the *ISC2 Cybersecurity Workforce Study*, the industry needs an additional four million security professionals to safeguard enterprises (businesses) against growing threats. Hiring employees with the right skills and employee retention is a stiff challenge. That is the reality even before considering potential budget cuts and layoffs.

Artificial intelligence issues

We have discussed that attackers can use AI to drive sophisticated phishing/other types of attacks. Enterprises (businesses) organizations are facing many concerns related to the usage of AI:

- Users might inadvertently or maliciously input sensitive data, such as source code, copyrighted material, or confidential business data, into an AI-powered chatbot, which could lead to data exposure.
- Attackers can poison AI models with inaccurate data to fool the models into believing attack behaviors are not malicious.
- Using personally identifiable information or sensitive data to train large language models can result in data leakage, create data privacy concerns, or lead to data breaches. Copyright infringement, fraud, and breach of contract are many legal issues that are a possibility.
- AI tools, like any other tool or software, might have vulnerabilities that attackers can exploit.
- Be aware of any nonpermitted, non-company-controlled AI use by employees, known as **shadow AI**. Security policies or acceptable use policies should outline the challenges of shadow AI and prohibit it as needed. Monitor systems for shadow AI use, and assess and remediate any risks.

Conclusion

We now realize that cybersecurity risks are everywhere, hence cybersecurity has become a dominant concern for all enterprises (businesses), whether large, medium, or small. What is suggested here, is for enterprises (businesses) to adopt and rigorously follow an industry-accepted cybersecurity framework (e.g., NIST), conduct regular assessments, and train their employees consistently to make them security conscious. This is paramount in creating a secure digital environment.

Enterprises (businesses) should implement modern technologies such as **endpoint detection and response** (**EDR**), adopt strong password management, and conduct cloud security assessments to counter attacks such as malware, ransomware, and phishing. Cybersecurity strategies have to continually evolve and adapt to the changes in our digital frontier as the threat attack surface expands. Cybersecurity should not be a mere tick mark in the box. Financial and reputation implications on enterprises (businesses) due to a cyberattack are immense, hence cybersecurity should be an integral part of business strategy.

In the next chapter, we shall discuss the emerging cybersecurity trends in details and understand their common themes. We shall also introduce the subject of cyber resilience, its building blocks, and its importance for enterprises (businesses).

Points to remember

- Distributed ecosystems have their challenges viz., they are relatively easy to permeate, lack visibility, and are difficult to manage owing to their dispersed nature.
- Be aware of various types of cybersecurity challenges (threats/attacks/issues) being faced by your enterprise (businesses) today.
- It is imperative to be up-to-date on the latest cybersecurity threats/attacks/issues to safeguard your enterprise (business).
- The biggest challenge in cybersecurity today is the evolving nature of cyber threats.
- Cybercriminals are continuously formulating new methods and strategies to exploit vulnerabilities in networks and systems.
- The first step to address cybersecurity risks is to create a plan (based on an industry-accepted framework.

Key terms

- **Security information and event management**: A solution that helps enterprises (businesses) to detect, analyze, and respond to security threats before they can have adverse impact on its operations.

- **Mean time to detect**: A measure of how long it takes to discover a potential security incident.
- **Mean time to respond**: The time it takes to control and remediate a threat once it has been discovered.
- **Internet of Things**: A network of interconnected devices that connect and exchange data with other IoT devices and the cloud.
- **Data privacy**: Element of data protection that addresses the proper storage, access, retention, security, etc. of sensitive data.
- **Disaster recovery as a service**: A cloud computing service that offers an enterprise (business) an offsite disaster recovery capability in a third-party cloud.
- **Internet control message protocol**: A protocol that devices within a network use to communicate problems with data transmission.

References

1. **https://www.techtarget.com/searchsecurity/feature/Ransomware-trends-statistics-and-facts**
2. **https://www.cnbc.com/2019/03/27/phishing-email-scam-stole-100-million-from-facebook-and-google.html**
3. **https://www.chegg.com/homework-help/questions-and-answers/case-study-sony-pictures-entertainment-hack-problem-november-24-2014-hacker-group-called-g-q45826501**
4. **https://www.computerweekly.com/news/4500271523/54m-cyber-fraud-hits-aircraft-supplier-share-price**

5. **https://www.techtarget.com/iotagenda/opinion/IoT-trends-to-keep-an-eye-on**

6. **https://www.ibm.com/topics/insider-threats**

7. **https://www.nextdlp.com/resources/blog/seven-takeaways-from-2023-verizon-data-breach-investigations-report**

CHAPTER 3
Emerging Cybersecurity Trends

Introduction

In the previous chapters, we looked at the chronology of the evolution of cybersecurity, explored noteworthy cybersecurity events and their impact on this domain, and also examined the building blocks of cybersecurity.

Further, we understood distributed systems, their workings, and challenges. We then detailed cybersecurity threats, attacks, and key issues and further discussed how to secure digital boundaries.

In this chapter, we will explore some prominent cybersecurity trends (and their characteristics) that are present and emerging due to the change in the threat landscape owing to our ever-increasing reliance on digital technology for conducting business.

Structure

In this chapter, we will cover the following topics:

- Cybersecurity trends
- Cyber security future trends
- Common themes in trends
- Understanding cyber resilience

Objectives

Cybersecurity has become a vital objective for enterprises (businesses) to protect data from online threats and unauthorized intrusions. Cybersecurity trends have evolved with technological advances, and data breaches, ransomware attacks, and cyber hacks have increasingly become commonplace.

Cybersecurity trends

With the increase in reliance on digital technology for communication, commerce, and critical infrastructure, the threat landscape has evolved in complexity and sophistication. In this section, we will explore some of the prominent (20 nos.) cybersecurity trends and the challenges they pose to individuals, enterprises (businesses), and governments.

Figure 3.1 depicts the first five (1-5) cybersecurity trends (with trends 6-20 to follow in continuation):

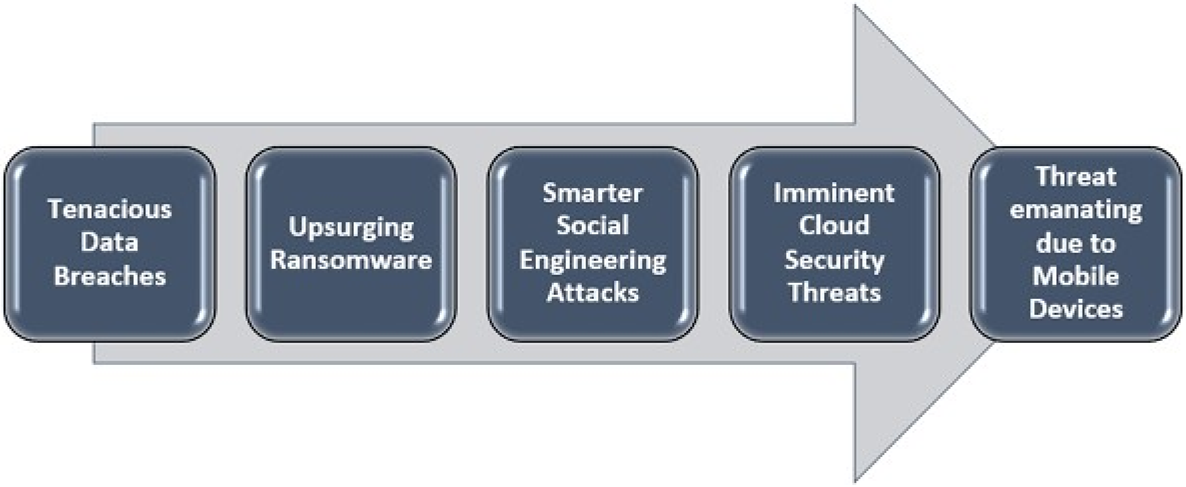

Tenacious Data Breaches
Upsurging Ransomware
Smarter Social Engineering Attacks
Imminent Cloud Security Threats
Threat emanating due to Mobile Devices

Figure 3.1: *Cybersecurity trends 1-5*

Trend 1: Tenacious data breaches

Data breaches have taken the world by storm and are unlikely to abate. They affect both individuals and enterprises (businesses) and present themselves as a paramount concern. In *Chapter 1*, *Cybersecurity: A Dynamic Changing Paradigm*, we covered regulatory frameworks such as GDPR and CCPA. The risk of data breaches can be mitigated through rigorously complying with these regulations and implementing security measures proactively.

Trend 2: Upsurging ransomware

We have touched upon this threat in the preceding chapters. There possibly are 120+ varieties of ransomware out there and the lure of monetary rewards is behind its successful rise (the trend of remote working during the COVID-19 pandemic added to the woes).

Attackers are expected to perpetrate more targeted ransomware attacks on vulnerable enterprises (businesses) using sophisticated phishing techniques and the power of **artificial intelligence** (**AI**) and **machine learning** (**ML**). Enterprises (businesses) must remain cautious and implement strategies proactively to mitigate the risks of a ransomware attack.

Trend 3: Smarter social engineering attacks

Social engineering attacks (refer to *Chapter 2*, *Cybersecurity: Understanding Today's Security Challenges,* for examples like spear phishing, BEC, whaling, vishing, etc.) continue to target sensitive user information through illegal means such as phishing by exploiting human weaknesses. Hence, these attacks will remain a significant threat to individuals and enterprises (businesses). A combination of employee awareness is effective in countering the associated risks through training and implementing security measures proactively.

Trend 4: Imminent cloud security threats

Due to various benefits ranging from scalability, to cost savings to efficiency, enterprises (businesses) are embracing cloud services. With sensitive data stored in the cloud, it has become a key target for attackers. In *Chapter 2*, *Cybersecurity: Understanding Today's Security Challenges,* we discussed that the responsibility of data security in and of the cloud is of the customer and **cloud service provider** (**CSP**) respectively. Cloud is becoming vulnerable due to insecure interfaces, misconfigurations, errors by end users, etc on account of customer and/or CSP.

As the reliance on the cloud increases, enterprises (businesses) must implement stringent security measures (protocols) and the rigor of continuous monitoring to mitigate risks and protect sensitive data stored in the cloud. Security measures can include regular patching, encryption, authentication, etc.

Cloud-related vulnerabilities will continue to be one of the biggest trends impacting the cybersecurity industry.

Trend 5: Threat emanating due to mobile devices

Mobile devices have become rewarding targets for attackers due to their proliferation. We have witnessed a noteworthy increase in malware and targeted attacks on mobile banking (since mobile devices are used for carrying out financial transactions). Mobile device security has become an integral point in the cybersecurity ecosystem and we are expected to see a rise in mobile device-specific viruses and malware.

Figure 3.2 depicts the next five (6-10) cybersecurity trends (with trends 11-20 to follow in continuation):

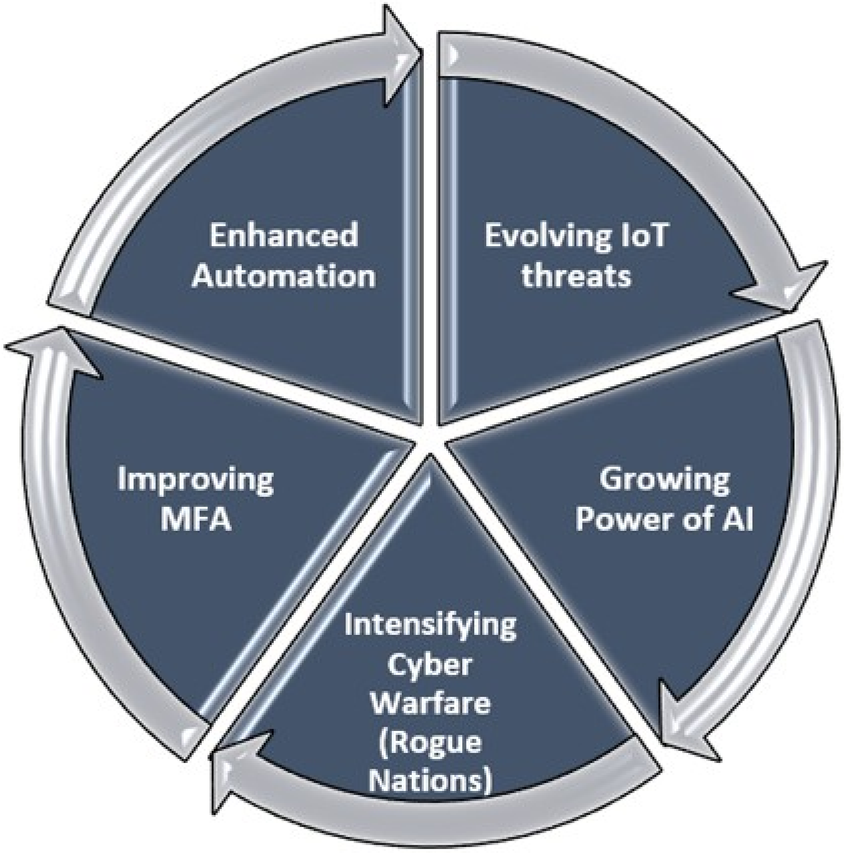


***Figure 3.2**: Cybersecurity trends 6-10*

Trend 6: Evolving IoT threats

Internet of Things (**IoT**) and IoT attacks were introduced and discussed in Chapter 2, *Cybersecurity: Understanding Today's Security Challenges*. The number of IoT devices continues to grow, creating greater opportunities for perpetrating cybercrime. It is important to note that an IoT device has very little processing and storage capacity compared to a laptop/smartphone. Because of this, it is not easy to deploy firewalls/ antivirus/other security applications to protect them. Consequently, enterprises (businesses) need to prioritize the security of their IoT devices. This can be ensured through regularly updating the IoT devices and implementing robust security measures.

IoT devices are more exposed to external threats in the era of 5G networks. There is an urgency for 5G manufacturers to reduce the risk of data breaches and network attacks by developing secure hardware and software solutions.

Trend 7: Growing power of AI

AI is used to enhance various aspects of cybersecurity. AI enables the development of mechanized cybersecurity systems (by using ML algorithms) that can do tasks, such as robust threat detection, **natural processing language** (**NLP**), and face detection. Please note that attackers can take advantage of using these technologies to perpetrate attacks (automate attacks, do data poisoning, etc.) to circumvent security protocols. Though the usage of AI in cybersecurity is a work in progress, it is widely expected that threat detection and threat hunting abilities will gain importance in sophistication through the application of AI and ML.

Trend 8: Intensifying cyber warfare by rogue nations

Escalation of tensions between two powerful nation-states fuels cyber-warfare, which is state-sponsored (this nation-state is then known as a **rogue nation**). The target in the situation remains to be the critical infrastructure of the other nation. Events such as national elections are increasingly becoming targets of such attacks. We expect an increase in data breaches and acts of cyber terrorism in 2024.

Trend 9: Improving MFA

Usage of **multi-factor authentication** (**MFA**) is becoming a default as it renders an extra layer of security (improves the security posture) and mandates users to provide authentication before accessing accounts/systems. Despite MFA enhancing security, attackers will keep finding ways to bypass it. Therefore, the world is moving away from using phone-based MFA towards application-based authenticators (such as Google Authenticator) and security keys, which are more secure. Enterprises (businesses) will need to continue this journey of adopting MFA on priority and shield themselves against cyber threats.

Trend 10: Enhanced automation

Management of the ever-growing volume of data (increasing workloads) and steadying security processes require more and more automation to be embraced. Also, timely and efficient responses to cyber threats can be enabled through automation. The workplaces are already seeing (and continue to see) the integration of security measures into development processes, which promises to create more secure software solutions.

Figure 3.3 depicts the next five (11-15) cybersecurity trends (with trends 16-20 to follow in continuation):

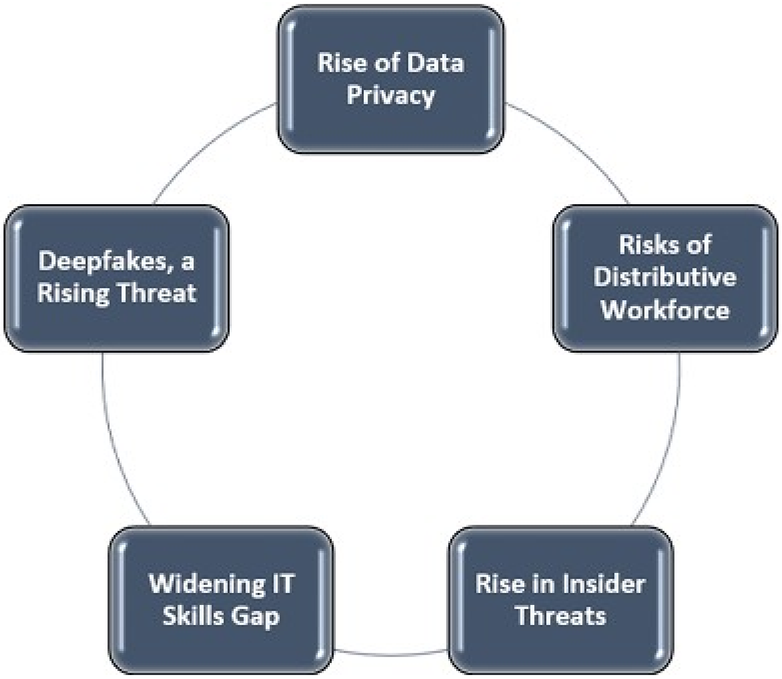


Figure 3.3*: Cybersecurity trends 11-15*

Trend 11: Rise of data privacy

Data privacy is a prominent data security trend on the rise that affects many aspects of an enterprise (business). The world has witnessed millions of **personally identifiable information** (**PII**) records getting exposed over the years which has led to the introduction of data protection laws worldwide viz., **General Data Protection Regulation** (**GDPR**), **California Consumer Privacy Act** (**CCPA**), etc. which indicates that data privacy will continue to be prioritized.

Non-compliance with such regulations will lead to fines (penalties), loss of customer trust, and bad publicity. Due to these implications, enterprises (businesses) will, going forward, recruit data privacy officers and emphasize critical controls such as role-based access control, MFA, encryption (transit and rest), segmentation of the network, etc. to continually improve their data privacy posture.

Trend 12: Risks of distributive workforce

COVID-19 had a profound impact on enterprises (businesses) by forcing them to shift their workforces to performing work remotely, which happened quite fast. It is expected that a hybrid work environment is likely to prevail post-pandemic. Therefore, a challenge for enterprises (businesses) will be to safeguard their workforce, which will work in a distributed environment.

Trend 13: Rise in insider threats

Insider threats will remain a growing challenge for enterprises (businesses). Security can be compromised inadvertently or maliciously by employees or trusted individuals. Enterprises (businesses) are expected to increase their focus on enhancing employee behavior monitoring and detection capabilities to proactively identify insider threats. Emphasis will be on employee awareness and regular training.

Trend 14: Widening IT skills gap

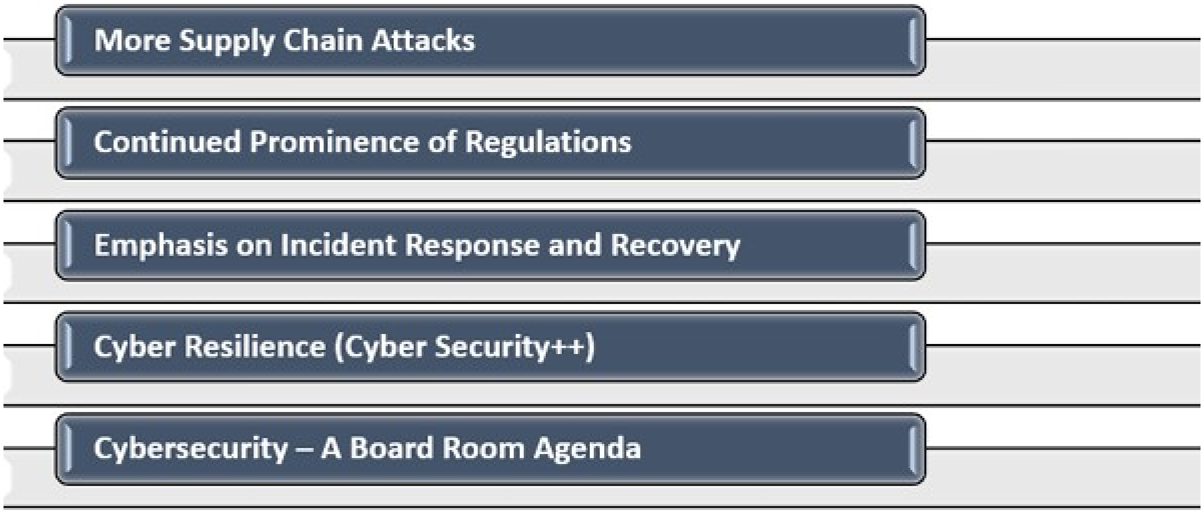
The demand for skilled cybersecurity professionals is expected to further rise. Consequently, the gap between demand and supply (talent available) will grow. This gap will present a challenge for enterprises (businesses) to seek competent experts to manage their Cybersecurity requirements. Enterprises (businesses) will invest in programs (training) to upskill the existing workforce and attract new talent. The shortage of cybersecurity will remain an unrelenting issue.

Trend 15: Rising threats of Deepfakes

Deepfake technology has started to create havoc and is expected to remain a deep concern. It involves manipulating audio and video to create realistic but fake content. This can be used to perpetrate social engineering attacks, spread disinformation through impersonation, etc. Enterprises (businesses) will invest in deepfake detection tools, employees' education, and awareness to protect data integrity and reputation.

Businesses of all sizes, corporate entities, organizations, and even governments have embraced computerized systems to streamline daily operations. Consequently, ensuring cybersecurity has emerged as a paramount objective to protect data from many online threats and unauthorized intrusions. As technology evolves, so do cybersecurity trends, with data breaches, ransomware attacks, and hacks becoming increasingly commonplace. Elevate your expertise by enrolling in security courses led by industry experts, empowering you with the knowledge and skills needed for comprehensive data protection.

Figure 3.4 depicts the next five (16-20) cybersecurity trends:



More Supply Chain Attacks

Continued Prominence of Regulations

Emphasis on Incident Response and Recovery

Cyber Resilience (Cyber Security++)

Cybersecurity – A Board Room Agenda

Figure 3.4: *Cybersecurity trends 16-20*

Trend 16: More supply chain attacks

Attacks targeting supply chains of enterprises (businesses) to compromise their services and products are expected to be on the upswing. Events like SolarWinds have demonstrated the devastating impact it can have on enterprises (businesses) and their customers. This will increasingly focus on enhancing their visibility into the supply chain and implementing robust cybersecurity measures to reduce the risk of compromise.

Trend 17: Continued prominence of regulations

Cyberattacks are a threat to national security and can thwart economic growth, and governments and enterprises (businesses) are aware of this. Regulations have emerged to address the growing cybersecurity issues and the impact data breaches have on social and even political fronts. Compliance with regulations (global data privacy laws) such as GDPR, CCPA, etc., centered around consumer data privacy, the need for aspects such as consent management, etc. will become more significant. These regulations will continue to evolve, urge enterprises (businesses) to adopt more stringent data protection measures and this subject will be on top of the agenda of legislators.

Trend 18: Emphasis on incident response and recovery

The development and testing of incident response and recovery plans will be a focus for enterprises (businesses). The capacity to detect and respond to cyber incidents and recover from them will be critical to minimizing the impact of breaches.

Trend 19: Cyber resilience

Cybersecurity and cyber resilience are not the same. Cybersecurity focuses on preventing attacks, while cyber resiliency is a measure designed to ensure the continuity of business operations after an enterprise (business) undergoes a successful data breach. The priority in the future will be to develop the ability to efficiently recover and salvage data loss and business downtime.

Trend 20: A board room agenda

With time passing, Cybersecurity has been featured among the top business risks being faced by enterprises (businesses). Consequently, cybersecurity remains a challenging area of oversight for corporate leaders and many boards regularly discuss this subject. It is widely expected that in the future there will be at least one member on the board with expertise in this domain.

Cyber security future trends

In this section, we will explore some of the prominent (10 nos.) future (emerging) cybersecurity trends and the challenges they pose to individuals, enterprises (businesses), and governments.

Figure 3.5 depicts the first five (1-5) future cybersecurity trends (with trends 6-10 to follow in continuation):

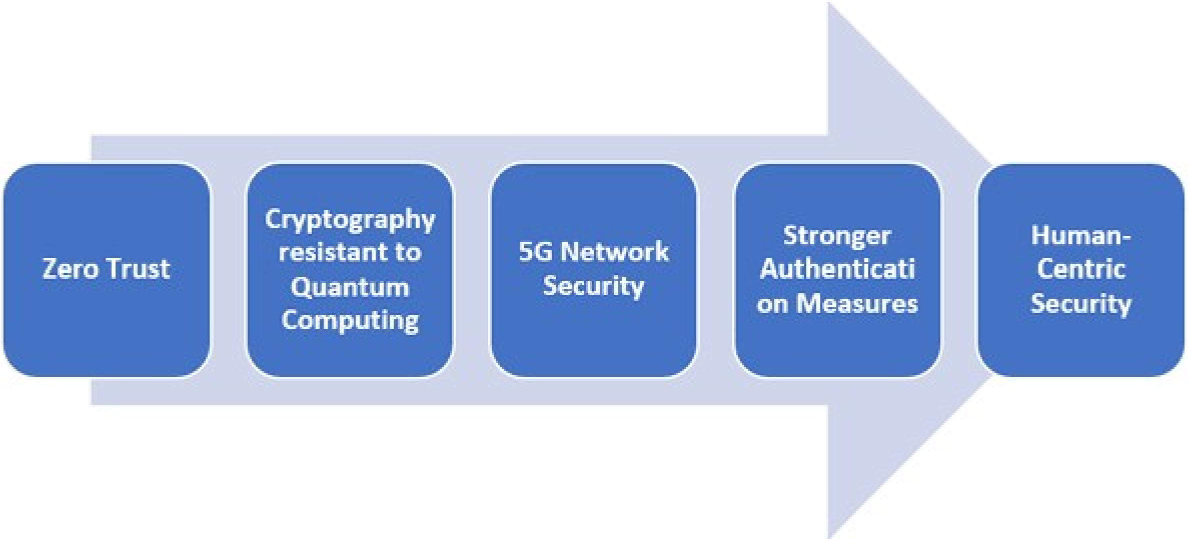

Zero Trust
Cryptography resistant to Quantum Computing
5G Network Security
Stronger Authenticati on Measures
Human-Centric Security

***Figure 3.5**: Cybersecurity future trends 1-5*

Future trend 1: Zero trust

Enterprises (businesses) have always worked with an assumption that someone inside the corporate perimeter is to be trusted (implicit trust) and anyone from outside should be suspected. This has led to data breaches (since attackers can do lateral movement throughout the network if they can breach the perimeter).

This is where a zero trust model comes to the rescue. It provides user access to information based on their identities and roles, regardless of their location (home/office/anywhere). In this model, authentication and authorization occur continuously rather than just once at the perimeter. Unwarranted lateral movement by an attacker can be avoided between applications, systems, and services through zero trust.

It would not be complete if we do not refer to microsegmentation, a core principle of zero trust. Microsegmentation enables the bucketing of network resources in isolated zones. This helps contain threats and prevents lateral within the network. Also, the application of granular role-based access (adaptive policies) is possible.

Adoption of what is known as **Zero Trust Architecture** (**ZTA**) will increase as enterprises (businesses) realize the shortcomings of perimeter-based security models for securing sensitive data. ZTA works on two main principles: continuous monitoring (verification) and *never trust, always verify*.

Figure 3.6 depicts a phased approach (iterative) for adopting a journey to implement zero trust:

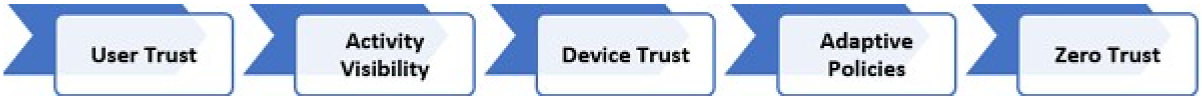


Figure 3.6*: Phases to Zero Trust*

Future trend 2: Cryptography resistant to quantum computing

The world of technology will witness advancement in quantum computing technology. With this, the development of cryptography that is resistant to quantum computing will be vital. Enterprises (businesses) will need to use cryptographic algorithms that can resist quantum attacks.

Future trend 3: 5G network security

In the years ahead, we will see rollouts of 5G networks in different countries. With this, the emphasis on the security of 5G networks will increase. Faster speed and lower latency of these networks will present new security challenges, which will make IoT devices vulnerable in particular.

Future trend 4: Stronger authentication measures

Stronger authentication measures are likely to evolve in the future viz., facial recognition and fingerprint scanning. Behavioral analytics or liveness detection are being talked about now-a-days. These measures can be used to prevent spoofing. The usage of such technologies will become more widespread to protect sensitive information.

Future trend 5: Human-centric security

User-centric security awareness and training programs will be expanded to reduce the risk of social engineering attacks. Behavioral analytics and user-focused security tools will help identify unusual user behavior and potential insider threats.

Figure 3.7 depicts the next five (6-10) future cybersecurity trends:

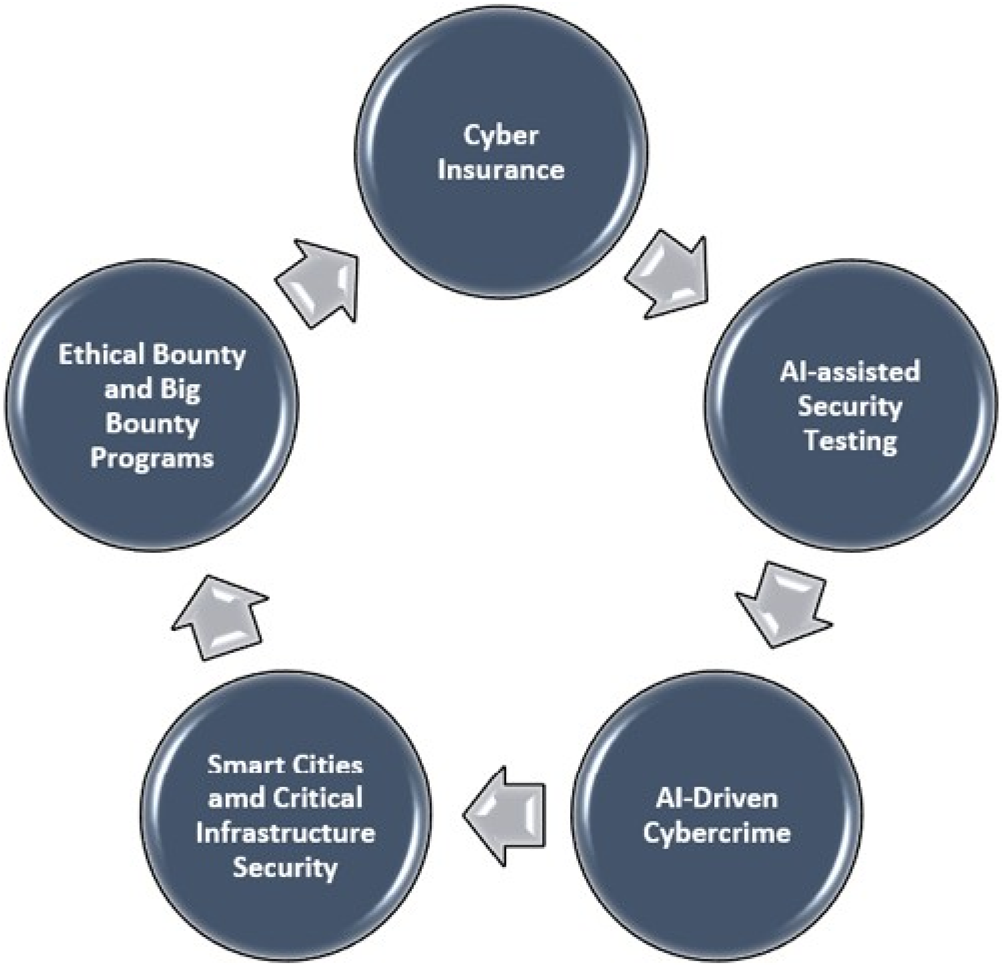

Cyber Insurance
AI-assisted Security Testing
AI-Driven Cybercrime
Smart Cities amd Critical Infrastructure Security
Ethical Bounty and Big Bounty Programs

Figure 3.7*: Cybersecurity future trends 6-10*

Future trend 6: cyber insurance

We will witness cyber insurance policies getting customized to specific risks and compliance requirements and the world will see a spurt (growth) of cyber insurance policies as the need for protection against cyber incidents from a financial perspective will increasingly be recognized.

Future trend 7: AI-assisted security testing

As the power of usage of AI increases in threat hunting and threat detection domains, AI will be used to power the conduct of penetration testing and vulnerability assessments. These activities are likely to become more sophisticated in detecting weaknesses in systems/applications and enable addressing security weaknesses on a proactive basis.

Future trend 8: AI-driven cybercrime

We have discussed the usage of AI in cybersecurity. This view is from the other side of the coin. Cyber attackers will also progressively employ AI and ML to them more sophisticated (enhanced), bypass security measures, and make them more challenging to detect.

Future trend 9: Smart cities and critical infrastructure security

The future will see the advent of smart cities and the expansion of digitization of critical infrastructure. In these scenarios, systems will get more interconnected, and security measures to protect them will become critical. Governments/enterprises (businesses) will have to prioritize the protection of critical infrastructure such as power grids, transportation systems, etc.

Future trend 10: Ethical hacking and bug bounty programs

Enterprises (businesses) utilize programs like ethical hacking, and bug bounty programs (crowdsourced) to detect system vulnerabilities (this is through their security testing capabilities). The trend is gaining traction among enterprises (businesses) that seek a cost-effective and efficient way to identify and mitigate security vulnerabilities.

Enterprises (businesses) can leverage the collective expertise of a global community of ethical hackers to unearth vulnerabilities that traditional security testing methods may not be able to find. This is giving an impetus to the bug bounty platforms and aiding in the expansion of crowdsourced security testing across industries.

Common themes in trends

So far, we have explored the cybersecurity trends (present and future). Mentioned are some of the common themes amongst these trends:

- **Sophistication**: The increase in the sophistication of cyberattacks is one of the most distinguished trends in the digital threat landscape. Attackers are constantly developing newer tactics, techniques, and strategies to exploit (breach) security systems, disrupt critical services, or steal sensitive data. There are many factors behind this viz., powerful hacking tools at the disposal of attackers, the spread of cybercrime forums, and the upsurge of hacking groups that are state nation-state-sponsored.
- **Attack vectors**: We have discussed malware, DDoS attacks, ransomware, etc. which are the various attack vectors being deployed for carrying out attacks. Attackers don't use just one, a combination of various methods to perpetrate attacks to achieve their objective. For example, a ransomware attack may commence with a phishing email and eventually lead to the deployment of malware that encrypts data.
- **Target**: None is spared. Large enterprises (businesses), governments, and individuals were the early targets of the attackers. The cyber threats equally loom large on medium and small businesses, healthcare and manufacturing entities, educational institutions, etc. Attackers crave to disrupt/steal sensitive information, which is leading to this diversification of targets and is expected to continue as digitization further permeates our digital world.

The need of the hour for enterprises (businesses) to combat cybersecurity attacks is international cooperation on cybersecurity matters and cyber resilience. Both the subjects are briefly descrived as follows:

- **International collaboration**: There is a growing need for governments around the world, law enforcement agencies, and cybersecurity enterprises (businesses) to share threat intelligence to enable effective tracking down of cyber criminals and their infrastructure. This can lead to mitigating threats at a global level. Since digital threats are global in nature, international collaboration has become paramount.
- **Cyber-resilient architecture**: In our increasingly interconnected world, the importance of cyber resilience cannot be overstated. Cyber resilience goes beyond mere cybersecurity; it is about preparing for, responding to, and recovering from cyber threats in a way that minimizes damage and ensures business continuity.

Understanding cyber resilience

As discussed earlier in this chapter (refer to *Trend 19: Cyber resilience*), cyber resilience is the aptitude of an enterprise (business) to effectively recover after a cyber-attack. This requires anticipating and preparing for the attack through detective, preventative and other proactive cybersecurity measures, and timely and efficient providing incident response. The prudence of cyber resilience acknowledges that breaches will take place. It enables enterprises (businesses) to proactively prepare for the same by emphasizing the importance of salvaging the business impact and ensuring a swift recovery.

Importance of cyber resilience

A successful cyberattack can be devastating enough and cause huge financial losses or even shut down an enterprise (business) permanently. Cyber resilience therefore is vital to identify, assess, manage, mitigate, and recover from malicious attacks.

Refer to *Figure 3.8* which reflects the importance of cyber resilience:

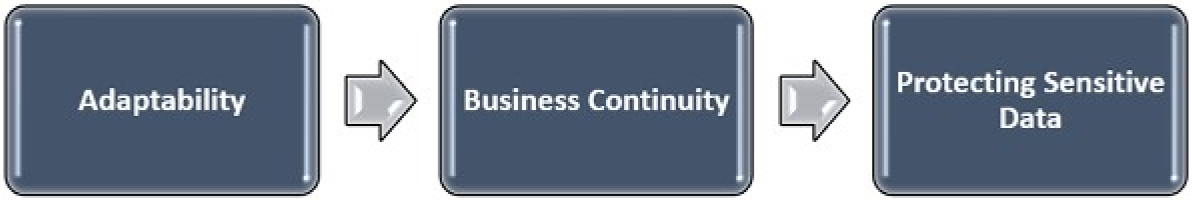


***Figure 3.8**: Importance of cyber resilience*

A comprehensive cyber resiliency strategy helps protect critical systems, applications, and data and also enables swift recovery and business continuity. Adaptability, business continuity, and protection of sensitive summarize the importance of cyber resilience:

- **Adaptability**: Cyber resilience prepares enterprises (businesses) to adjust to constantly evolving cyber threats (of sophisticated and varied nature), thereby making sure that the defenses remain effective over time.
- **Business continuity**: The downsides of a cyberattack are immense. It can interrupt business operations, inflict reputational damages, and lead to financial losses for enterprises (businesses). Cyber resilience ensures that vital business functions/services continue operating even after a cyber incident.
- **Protecting sensitive data**: Cyber resilience not only focuses on the prevention of data breaches but also the implementation of security measures to recover data in a timely and secure manner in case of a data breach. This aspect is paramount for any enterprise (business).

Building blocks of cyber resilience

Cyber resilience is not monolithic in nature. It consists of multiple structured steps along with multiple iterations.

Refer to *Figure 3.9*, which depicts the building blocks of cyber resilience:

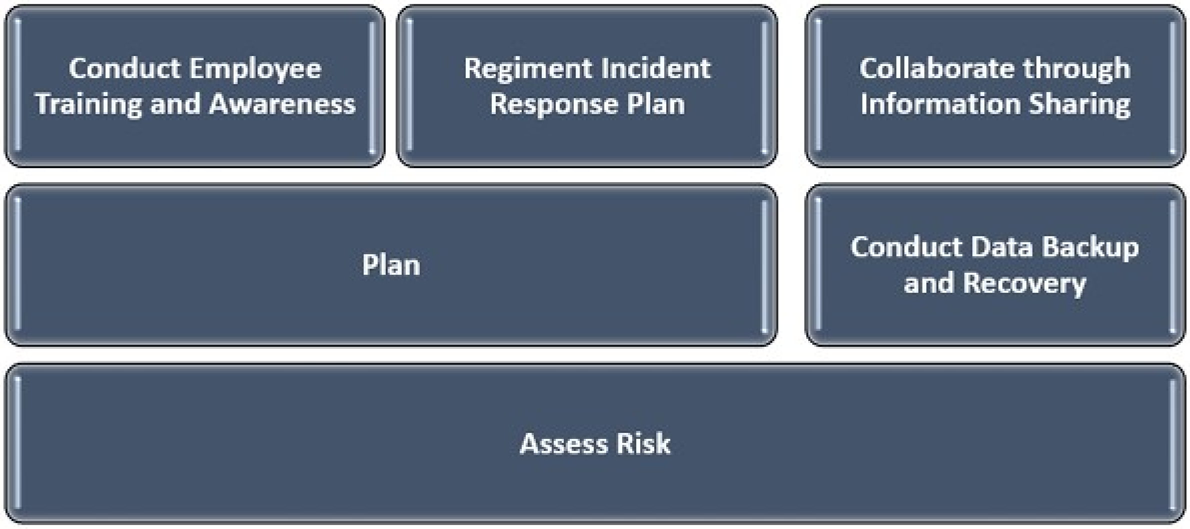

Conduct Employee Training and Awareness
Regiment Incident Response Plan
Collaborate through Information Sharing
Plan
Conduct Data Backup and Recovery
Assess Risk

Figure 3.9: *Building blocks of cyber resilience*

Following are the steps an enterprise (business) can take to build and improve its cyber resilience.

1. **Assess risk**: The first step is to identify and understand potential cyber risks. An important step in this regard is to carry out a comprehensive risk assessment to identify vulnerabilities and potential attack vectors.
2. **Plan**: The next step after identification is to develop a holistic cybersecurity plan that covers strategies for prevention, detection, response, and recovery.
3. **Conduct employee training and awareness**: This step is equally important. Employees need to be regularly trained on cybersecurity best practices (how to recognize phishing attempts, use strong passwords, etc.). Cybersecurity awareness should become second nature within the enterprise (business) as it directly addresses the employees who are the first line of defense against cyber threats.
4. **Regiment incident response plan**: The need for developing a comprehensive incident response plan needs to be overemphasized. The response plan should entail detailed steps (clear communication guidelines, roles, and

responsibilities, how to isolate and mitigate the business impact) to be undertaken in the event of a cyber incident.

5. **Conduct data backup and recovery**: Conduct regular backups of business-critical data and make sure that the data is secure and accessible in time of need (reliable). This will expedite recovery in situations involving a ransomware attack or data breach.

6. **Collaborate through information sharing**: This aspect has been discussed in this chapter (refer to the section on *International collaboration*). Industry peers and government agencies globally must collaborate and share best practices and threat intelligence. The cyber resilience of the digital ecosystem can be strengthened through this approach.

Conclusion

Cyber resiliency in today's digital world has become a necessity. It is therefore important that enterprises (businesses) adopt an approach that is proactive and adaptive which will enable them to maneuver through the changing threat landscape. Cyber resilience is an ongoing process that requires 3Cs (commitment, collaboration, and continuous improvement) to stay ahead of the curve.

In the next chapter, we will understand **Cyber Security Mesh Architecture** (**CSMA**), examine its need CSMA, and detail the benefits of its adoption.

Points to remember

- Enterprises (businesses) globally are facing numerous cybersecurity threats and attacks that can be expected to increase in volume and complexity over time
- Attackers are continuously seeking newer methods to target and cause harm to individuals/enterprises (businesses)
- Cybersecurity issues continue to evolve due to the above-mentioned reason

- Cybersecurity responses (also detective and preventive measures) need to evolve in capability to counter the growing threats and to stay ahead of the game
- Be aware of cybersecurity trends and their importance
- Understanding these trends can provide key insights into the changing threat landscape of cybersecurity
- Cyber resilience is the capability of an enterprise (business) to enable business resiliency by thorough preparedness to respond to and recover from cyber threats
- An enterprise (business) that is cyber-resilient can address known and unknown threats, events, and challenges better than others

Key terms

- **Cloud service provider**: Providers of cloud platforms, infrastructure, and services.
- **Deepfakes**: A type of AI used to create (by using deep generative methods) image, audio, and video hoaxes that appear convincing
- **Zero Trust**: A combination of concepts and ideas that fundamentally shift focus from a location-centric model to a data-centric approach for modular security controls (between users, systems, data, and assets that change over time)
- **Cyber resilience**: The ability of an enterprise (business) to limit the impact of security incidents by deploying and optimizing appropriate security tools and processes

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

CHAPTER 4
The Need for Cybersecurity Mesh Architecture

Introduction

So far, we have learned how cybersecurity has evolved dynamically over time, we then concentrated on the cyberattacks and challenges being faced by enterprises (businesses), and explored prominent cybersecurity trends emerging due to the change in the threat landscape.

Let us now take a solutions-oriented approach and discuss cyber risk management. Simplistically, it is about assessing what could potentially go wrong and then deciding on the best approaches/solutions to prevent/minimize it. In today's world, both the government and private sectors must manage any cybersecurity threat.

Let us remember the impact COVID had on enterprises (businesses). It has pressed enterprises (businesses) to what we refer to as an edgeless digital infrastructure that changes constantly expanding its attack surface. What have the enterprises (businesses) done in these situations? They have employed new technologies across their infrastructure.

We now have distinct environments to take care of viz., work-from-home, on-premise office infrastructure (traditional), and multi-cloud data centers. Not only has the complexity of safeguarding this attack surface increased (through tools) but also the management of these tools has added to the complexity (which is often done by different teams).

It is reasonable enough to state that the cybersecurity industry is at a tipping point.

Structure

In this chapter, we will cover the following topics:

- The current situation of cybersecurity ecosystem
- CSMA explained
- Illustrating the layers of CSMA
- The need for CSMA
- Benefits of CSMA

Objectives

In this chapter, we will introduce CSMA and examine its needs and benefits for enterprises (businesses). We shall also understand the various challenges that the cybersecurity architectures of today are facing.

The current situation of cybersecurity ecosystem

The cybersecurity tools/platforms/services of today, which we call the **next generation set**, need to work together coherently to manage the complex environment and dynamically changing (and growing) threat landscape.

According to a *Global Data Breach Report 2022* by a leading organization, an average enterprise (business) runs 45+ security tools (point tools covering those that monitor applications, network, cloud operations, etc. Many of these tools were not established with contemporary use cases in mind. Existing approaches to cybersecurity are not adequate to address issues of dynamic and complex environments where the sophistication of threat actors is increasing relentlessly.

With this backdrop, *Gartner* released a document titled *Gartner Top Strategic Technology Trends for 2022*. One of the many trends (e.g., Generative AI, Hyper automation, Cloud-native platforms, Data fabric, etc.) mentioned in this document was *Cybersecurity Mesh Architecture*.

Cybersecurity Mesh Architecture (**CSMA**) is a new approach to cybersecurity coined by Gartner. In this chapter, we will discuss the circumstances that have brought CSMA platforms to the fore, how these platforms work, and describe the benefits of using CSMA.

CSMA explained

CSMA is a contemporary scalable (say flexible) approach to cybersecurity architecture that allows the distributed enterprise (business) to deploy and extend security controls where needed most. Each tool running in a silo is not helpful, and CSMA enables various tools to run and interoperate via common identity, centralized policy management, automation, orchestration, security analytics, and intelligence.

There is another way of perceiving CSMA. It is an architecture that provides the base for computers and people to connect securely across various locations over hybrid and multi-cloud environments, channels, and varied applications while protecting all digital assets of the enterprise (business). While doing this, the architecture enables a security posture that is far more consistent and supports the increased agility of the enterprise (business).

Note: CSMA is not prescriptive; rather, it is a framework that is interoperable and enables disparate cybersecurity services to work together.

Illustrating the layers of CSMA

Please refer to the following *Figure 4.1*, wherein you can see that CSMA buckets existing cybersecurity tools into various layers, where each layer can interact with the ones above and below it. This leads to forming a mesh of functionality that allows distributed systems to communicate with one another (and is far more beneficial). This is fed into centralized dashboards and controls that streamline security operations.

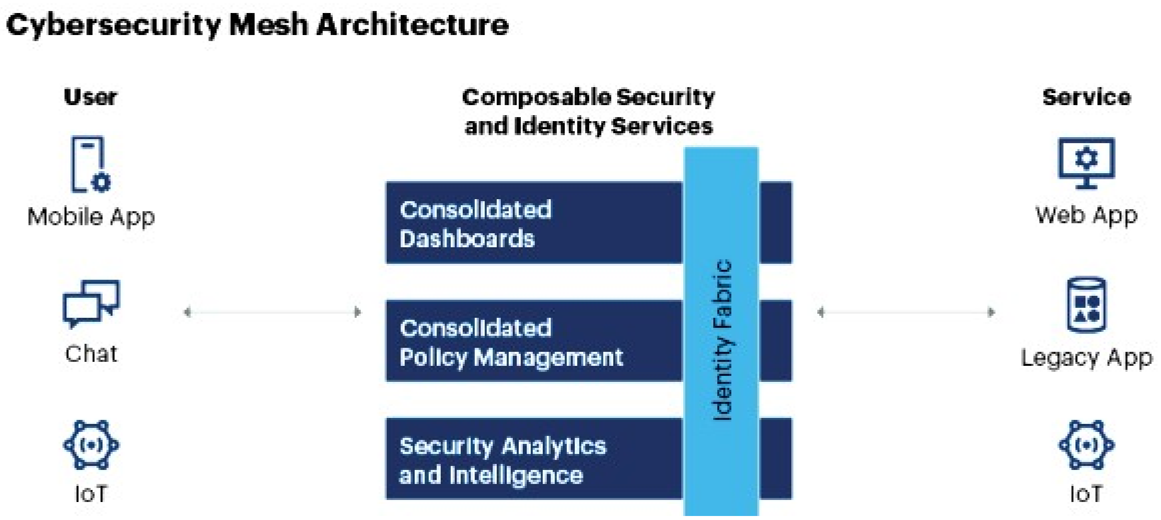

Cybersecurity Mesh Architecture
User
Mobile App
Chat
IoT
Composable Security and Identity Services
Consolidated Dashboards
Consolidated Policy Management
Security Analytics and Intelligence
Identity Fabric
Service
Web App
Legacy App
IoT

***Figure 4.1**: Cybersecurity Mesh Architecture*
***Source**: Gartner*

The need for CSMA

We have seen that historically, enterprises (businesses) have taken an approach to selecting appropriate (according to the need) solutions such as Firewalls, **Network Access Control** (**NAC**), **Intrusion Prevention System/Intrusion Detection System** (**IPS/IDS**), **Security Information and Event Management** (**SIEM**), **Endpoint Detection and Response** (**EDR**), and more, which have been of great assistance to security operations teams.

These advanced tools were architected to work independently and have limited interoperability with each other, which leads to ineffective data and alert management. In short, these tools act as vital components to the bigger cybersecurity puzzle.

The following figure lists the various challenges plaguing today's cybersecurity architectures:

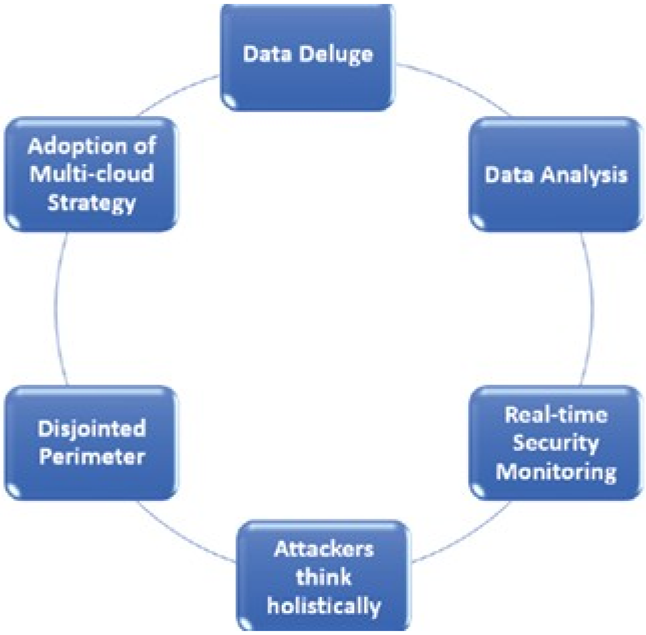

Data Deluge
Data Analysis
Real-time Security Monitoring
Attackers think holistically
Disjointed Perimeter
Adoption of Multi-cloud Strategy

Figure 4.2: *Challenges facing today's cybersecurity architectures*

Challenge 1: Data deluge

All enterprise (business) processes depend on fast and accurate data collection and processing, and so does cybersecurity. A potential concern for security teams is data deluge (refer to *Figure 4.3*, which illustrates a data deluge scenario wherein more data is generated than can be successfully/efficiently managed). Downsides of data deluge include overlooking events due to alert fatigue (due to overwhelming data), missing vital events, or insufficient time to process and leverage the data generated by security tools.

Figure 4.3: *Data deluge illustration*

Let us examine SIEM solutions. SIEM is a powerful tool used for detection purposes on a 24x7 basis thereby producing huge amounts of event data. Unless there is an infrastructure that can support real-time integration (and aggregation) of data, all this data may not be able to provide meaningful inferences.

In a way, these tools create a lot of noise, which increases over time (e.g., from new endpoints and edge devices, cloud computing resources, etc.) as there is no option for enterprises (businesses) to scale down data collection. It is not easy for the security teams to be effective in these circumstances.

Challenge 2: Data analysis

In the above issue, we realize that sifting through the sheer volumes of data created by cybersecurity tools is an issue. This data is also required to be analyzed so that meaningful inferences can be drawn (refer to *Figure 4.4* depicting the process of inspecting, cleansing, transforming, and modeling data to discover useful information). To make this happen, data has to be integrated from disparate and multiple sources. This is not an easy task by any means.

Figure 4.4: *Data analysis illustration*

Let us take an example. We often see that network and application logs are tracked separately. Anomalous data may come to the attention of a security analyst in network logs, and he/she may not know its consequences. If unusual activities are going on at the application level, they will not show up at the network level. To decipher what transpires, the security analyst must analyze the application logs from another cybersecurity tool.

This activity of correlation between network and application logs can be difficult, rather slow, and prone to errors. The analysis is even more difficult due to the volumes of data to be processed without appropriate tools. Moreover, analysis needs to consider aggregating data across various dimensions such as log severity level, time, resource type, and many more. Query tools that work on integrated data sets are required to address this challenge.

Challenge 3: Real-time security monitoring

In Chapter 1, *Cybersecurity: A Dynamic Changing Paradigm,* we mentioned two aspects viz., **Mean Time To Detect** (**MTTD**) and **Mean Time To Remediate** (**MTTR**), which are the ways to assess the overall cybersecurity posture (performance) of an enterprise (business). It is paramount for cybersecurity teams to find the source of an attack and thwart the intrusion attempt before it can cause serious damage. For this to happen, detection has to be swift, in real-time, and most importantly cybersecurity teams must have access to the tools that can assist them in taking action promptly and efficiently.

Refer to *Figure 4.5*, showcasing real-time monitoring which is the delivery of continuously updated data about systems, processes or events.

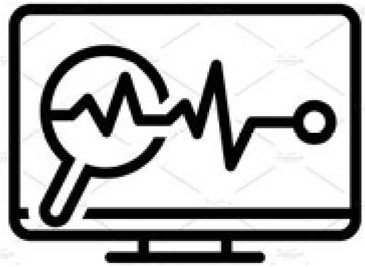


***Figure 4.5**: Real-time security monitoring illustration*

Attackers work at the speed of a machine. If they breach the defenses of an enterprise (business) and inject malicious code into a system, they can inflict huge damage. Human teams can ill-afford to respond to these situations manually to block such attacks. The first preference is always to block these kinds of attacks completely, and the second best is to detect the events proactively and provide quick incident response.

Incident response depends on the incident type. An IP address can be blocked if malicious code is detected in the traffic from that IP address. A process can be terminated if it runs on a database server and data is being exfiltrated in large amounts.

The actual response is not this simple. The process requires collecting data regarding the attack and may involve monitoring the attack process to understand its method. Overall, it is important to note that the incident response has to be real-time (as much as possible) regardless of the action taken (block or allow it to continue and monitor).

Challenge 4: Attackers think holistically

Malicious actors are motivated by the lure of lucrative potential revenues; hence, they resort to acts like Ransomware and other cybersecurity attacks. Cybersecurity attacks, especially Ransomware, lead to interruptions in the physical world when they target critical infrastructures. Refer to *Chapter 1*, *Cybersecurity: A Dynamic Changing Paradigm*, for details on various

Ransomware attacks. *Figure 4.6* shows an attacker behind a camouflage, ready to perpetrate an unauthorized action against computer infrastructure to compromise it:

***Figure 4.6**: Attacker illustration*

Countering such attacks requires a cybersecurity posture that can eliminate inefficiencies and silos not only from an organizational standpoint but also from within technology. This is precisely because hackers do not think in silos. The limiting factor is that enterprises (businesses) often work in silos, and so do various cybersecurity tools. The tools operate within their specific views without or with bare minimum interoperability with the other tools.

We have heard of lateral movement. In this, hackers use a weakness in a system to exploit an adjacent area and can, move laterally within the environment. This requires creating connections between security controls through security analytics and security intelligence using domain-specific information.

Challenge 5: Disjointed perimeter

Modern-day enterprises (businesses) do not have data and many applications in their data centers (on promise). They are increasingly using cloud-based applications that users access from anywhere. *Figure 4.7* depicts a broken perimeter:

Figure 4.7: *Disjointed perimeter illustration*

In traditional circumstances, there would have been an on-premise data center that would define the network perimeter security to control access. The need of the hour is for context and identity to become the control surface in a distributed environment where assets connect from anywhere.

Challenge 6: Adoption of multi-cloud strategy

According to various studies, enterprises (businesses) are moving towards a multi-cloud setup since they take services from more than one **Cloud Service Provider** (**CSP**). Since every CSP has a different set of policies, creating a consistent security posture across multiple CSPs is not easy. What adds to the challenge are the various services that are domiciled in the on-premise environment.

Figure 4.8 illustrates a multi-cloud environment wherein an enterprise (business) uses services from more than one public cloud provider at the same time:

Figure 4.8: *Multi-cloud strategy illustration*

Having understood the various challenges being faced by today's enterprises (businesses), let us examine the benefits that CSMA presents to address these challenges.

Benefits of CSMA

It is not adequate to meet today's demands that are rapidly changing with the existing approaches related to identity and cybersecurity architectures. Existing approaches are quite disjointed. Therefore, the growing digital landscape which is complex requires a new approach to cybersecurity architecture. This is where the CSMA kicks in.

The basic objective of CSMA is to provide a common ground and a united security framework to secure assets (on-premises and /or in the cloud). CSMA enables point (stand-alone) cybersecurity solutions to work in an integrated manner (also standardized) and bring about an improvement in the overall security posture of the enterprise (business).

CSMA's further objective is to reduce the time required to collect and organize security data, which can lend the enterprise (business) more time to plan and respond to threats. Enterprises (businesses) need a platform that performs this, which can be advantageous to IT/security operations. That is just a baseline of what CSMA can assist with. Cybersecurity meshes can go the extra mile by increasing visibility in the cybersecurity ecosystem, reducing complexity in operations, and enhancing the sharing of security intelligence across the enterprise (business).

Figure 4.9 illustrates a list of the various benefits of adopting CSMA:

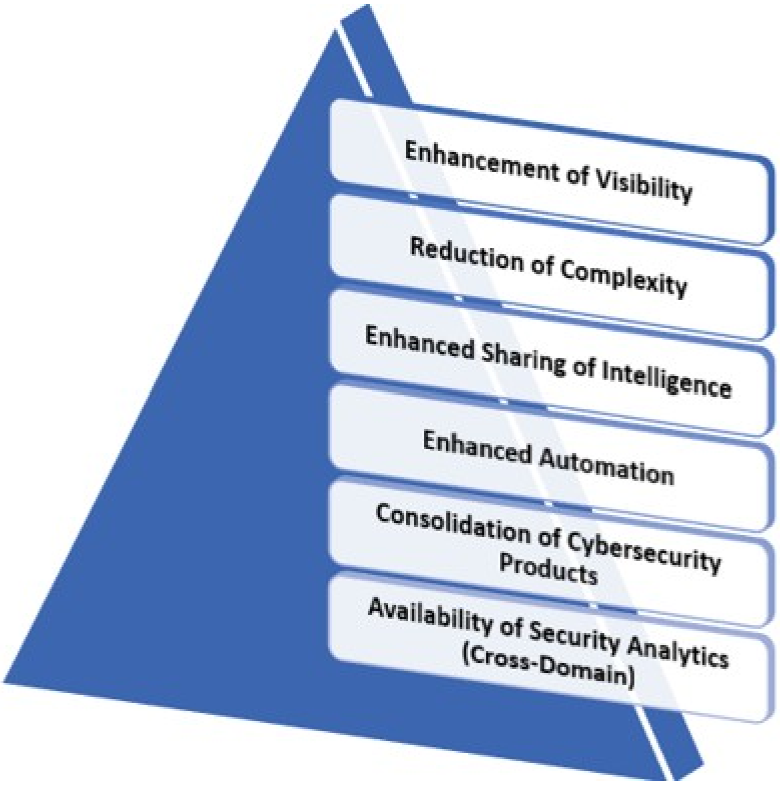

Enhancement of Visibility
Reduction of Complexity
Enhanced Sharing of Intelligence
Enhanced Automation
Consolidation of Cybersecurity Products
Availability of Security Analytics (Cross-Domain)

Figure 4.9: *Benefits of adopting CSMA*

Enhancement of visibility

As discussed in *Chapter 2*, *Cybersecurity: Understanding Today's Security Challenges,* visibility is construed as being able to see and understand various components of a cybersecurity infrastructure in a distributed ecosystem. Also, in line with what is mentioned in the preceding paragraph, CSMA follows an approach that is centered around the integration of systems, thereby leading to increased visibility predominantly through aggregation of security data and centralization of detection information. The seamless aggregation permits the cybersecurity teams to distinguish patterns easily in their data, which is the key.

Figure 4.10 portrays an eye to showcase how clearly various components of a cybersecurity ecosystem can be seen:

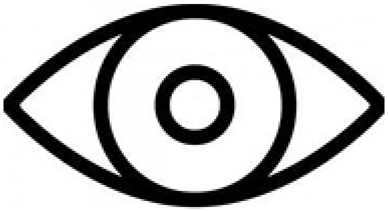


Figure 4.10: *Visibility illustration*

CSMA gathers the output from various systems (e.g., by way of integrating existing collected data and those from threat detection tools such as Firewalls, access management/ identity, EDR, etc.) and further carries out processing/analysis. This eventually leads to the end goal of CSMA, which is to assist cybersecurity teams in gaining meaningful threat intelligence (inferences).

CSMA also helps in the identification of patterns in security data that are aggregated and can determine some of the attacks that may be well-hidden. CSMA works to minimize the limitations of a distributed system where security data is generated across various devices/tools, making it difficult to correlate events. Let us learn this through an example. A cybersecurity analyst observes an increase in usage of a computing resource on a server in the cloud and would seem normal contextually. When seen in combination with an IAM incident and event on the network, there could be a real cloud security issue/event.

Let us reiterate what we have learned. Gaining visibility of data from separate cybersecurity solutions is not adequate rather a cybersecurity infrastructure (CSMA) is needed which enables cybersecurity teams to better understand the connections between various components in the ecosystem.

Reduction in complexity

In the case of cybersecurity, increased data aggregation usually goes hand-in-hand with a reduction in overall complexity. Siloed security resources are difficult to manage, as each section of an enterprise' (business') security ecosystem will have different operational upkeep needs, and this kind of structure can separate experts who should be communicating with one another.

Figure 4.11 provides an expression of the state of being intricate or complicated (aka maze):

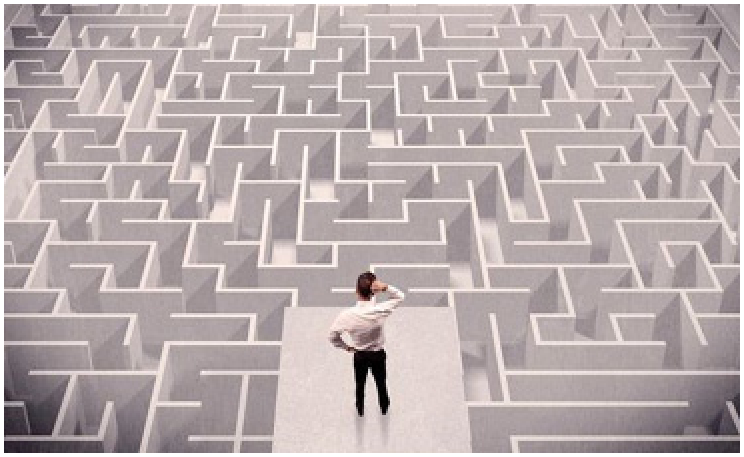


***Figure 4.11:** Complexity illustration*

CSMA reduces complexity by integrating siloed security systems into a centrally observable and controllable operations dashboard. This operational change lets SecOps staff respond to security incidents more quickly and efficiently.

When suspicious activity is detected and communicated to staff through the mesh architecture in an aggregated and integrated way, they are then able to prioritize events more accurately. More information, and more centralized controls, enable staff to exercise their security expertise by streamlining security data collection and analysis.

Enhanced sharing of intelligence

Another important characteristic of CSMA is that it enables threat intelligence and the sharing of intelligence across the cybersecurity ecosystem. We have discussed previously that cybersecurity tools/platforms/devices in siloed forms create a problem and lead to wasting time and energy of the cybersecurity teams.

Figure 4.12 illustrates intelligence sharing which is the ability to exchange intelligence, information, data, or knowledge:

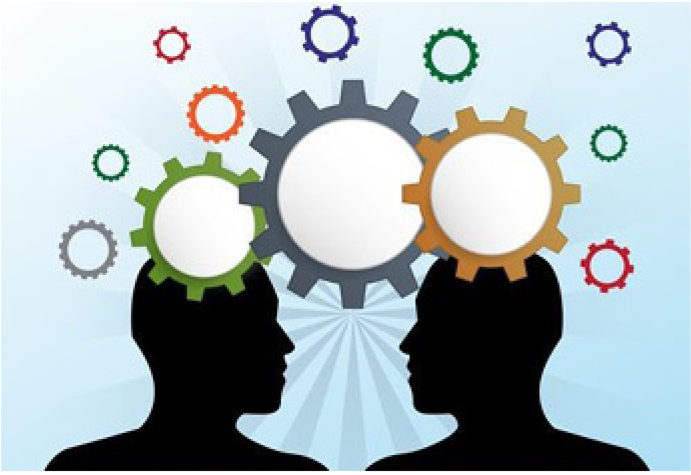


***Figure 4.12:** Sharing of intelligence illustration*

If implemented well, CSMA can enable an integrated view of the cybersecurity ecosystem and permits seamless communication amongst various resources across the enterprise (business) covering cybersecurity experts by eliminating silos. This further leads to an increase in the productivity of cybersecurity teams.

CSMA enables the sharing of intelligence amongst cybersecurity tools (on-premises/cloud). CSMA rationalizes the collection of security data feeding this aggregated data for enriching threat intelligence. Not only this, a comprehensive CSMA will cover data (aggregated) analytics, the application of machine learning, scoring of risk, and advanced analysis tools. Overall, CSMA will add intelligence for policy enhancements and aid in visualizations, orchestration, etc.

Enhanced automation

Attackers are known to be getting advanced with time and they are well-synchronized. They always attempt to work in a stealthy manner such that their attack goes unnoticed (rather than make it difficult to detect). We are increasingly observing the use of attacks using AI. This makes it difficult to respond to such attacks in time despite cybersecurity professionals working overtime (shall we say, against time).

Figure 4.13 illustrates automation, the method of making a device, a process, or a system operate by itself:

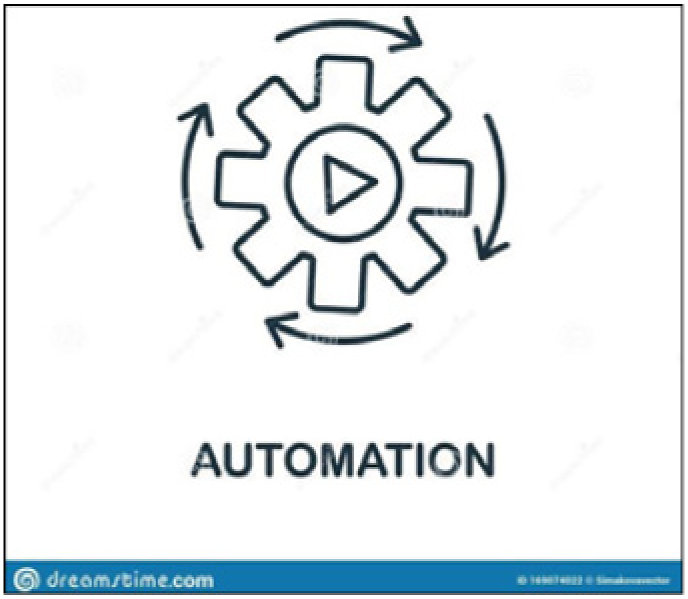


Figure 4.13: *Automation illustration*

The need of the hour for these professionals is AI-based automation which can work across the cybersecurity ecosystem to adequately address the risks posed by weaponization of AI.

Consolidation of security products

Of the many key priorities of cybersecurity, leaders are to consolidate spending on security products/solutions and reduce complications in their usage and management. According to a global report, enterprises (businesses) on average use 45+ (refer to section *Is the current situation sustainable?* of this chapter) cybersecurity products/solutions (Refer to and technologies, which further means multiple vendors.

Figure 4.14 depicts consolidation, which is the action of combining several things into a single more effective or coherent whole:

Figure 4.14: *Consolidation illustration*

In these circumstances, enterprises (businesses) need to have integrated dashboards and management of interfaces centrally. In reality, no single vendor offers all best-in-class cybersecurity controls (there is always one better than the other). Therefore, often that enterprises (businesses) often have to resort to using products/solutions from many vendors (also open-source solutions at times). Consolidation into a smaller set of cybersecurity vendors is a difficult task to achieve.

Supporting layers of CSMA are built through integrations. These integrations can be brought about through multiple means viz., a mix of proprietary APIs, open standards, and ad-hoc integrations between vendors' tools. CSMA thereby offers an integrated view across the cybersecurity ecosystem which assists the cybersecurity teams to respond swiftly and effectively to security events.

Security analytics

We have observed that enterprises (businesses) use multiple cybersecurity analytics tools together with other analytics tools. There are two problems with this setup. Firstly, most of the analytics tools are domain-specific, secondly, these tools do not work in a unified manner.

Figure 4.15 depicts a cybersecurity approach that uses data collection, data aggregation and analysis tools for threat detection and security monitoring (referred to as **security analytics**):

Figure 4.15: *Security analytics illustration*

As discussed earlier, CSMA provides a united security framework and baseline support layers to secure enterprise (business) assets. Essentially it enables otherwise disparate cybersecurity services to work in cohesion to create a progressive and comprehensive cybersecurity posture. Due to this unification of cybersecurity tools/solutions, CSMA enables the usage of multiple cybersecurity analytics across cybersecurity domains.

This phenomenon has led to a trend/concept that we refer to as **Extended Detection and Response** (**XDR**), which is much advanced in nature. Usage of these lends enterprises (businesses) very mature cybersecurity operations.

Using cross-domain cybersecurity data analytics and machine learning, CSMA enables correlation at scale. This allows enterprises (businesses) to detect patterns in data across cybersecurity sources, thereby identifying more harmful threats. In essence, CSMA transforms observations into intelligence that cybersecurity teams can act upon before events become critical issues/disruptions.

Conclusion

We have observed that historically enterprises (businesses) have taken the path of implementing best-fit solutions (that were appropriate for their need). Examples of such solutions are mentioned in the section, *The need for CSMA*. The limiting factor was non-interoperability among cybersecurity tools which impeded the swift decision-making needed for effective incident management. Inadequacy interoperability and cohesiveness of cybersecurity tools/platforms results in increased overhead in operations,

increased risk due to incomplete mapping of attack surface, incomplete contextual information leading to ineffective decision-making and increased incident' MTTR and incident response.

As discussed in this chapter, CSMA leads to enhancement of visibility, reduction in complexity, sharing of intelligence, enhanced automation, consolidation of security products, and usage of security analytics across domains in a complex and distributed cybersecurity ecosystem. This results in driving a larger Return on Investment from the existing investment (which is the most difficult variable to draw out in cybersecurity), prioritizes risk based on business impact, and most importantly enables effective incident management and response through intelligence sharing (across domains).

As a concluding remark, we should say: *There is all the benefit in cybersecurity meshing.*

In the subsequent chapter, we shall further examine the key components of CSMA, discuss the outcome of the adoption of CSMA, and conduct a sneak preview of CSMA products/solutions.

Points to remember

- With the adoption and growth of Cloud and hybrid (decentralized) working, cyber ecosystems have become fragmented
- Securing yesterday's distributed security architectures is a difficult task
- This is where cybersecurity mesh comes into play. It is a new architectural approach that reduces the need to have one specific computing environment
- CSMA is an approach that allows the integration of security tools into a scalable and collaborative ecosystem. It aims to create a much more

stable and reliable security as compared to traditional distributed security architectures

- CSMA is a concept than a concrete end-to-end solution, however is a viable framework that holds analytics, controls, and threat hunting to its core
- CSMA works towards creating a decentralized cybersecurity ecosystem, where security tools are better aligned to complement each other and integrate across all network components

Key terms

- **CSMA**: A contemporary scalable approach to cybersecurity architecture that allows the distributed enterprise (business) to deploy and extend security controls where it is needed the most.
- **NAC**: The process of restricting unauthorized users and devices from gaining access to a corporate/private network.
- **IPS/IDS**: Systems that monitor the network and identify potential incidents (also log and report security incidents). IDS systems do the detection, while IPS tools work toward prevention.
- **EDR**: A set of tools used to detect and investigate threats on endpoints.
- **API**: A software in-between two applications that permits the two to talk to each other.

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

CHAPTER 5
Fundamental Components of Cybersecurity Mesh Architecture

Introduction

In the previous chapter, we discussed the concept of CSMA, its need for enterprises (businesses), and its benefits in detail. A security mesh architecture is a philosophy and not necessarily a single end-to-end security solution. Some fundamental aspects of CSMA, such as its key components and the merits of its adoptions by enterprises (businesses) will be discussed in this chapter.

Structure

In this chapter, we will cover the following topics:

- A re-look at CSMA
- Key components of CSMA
- The unified architecture of CSMA
- Major products/solutions of CSMA

Objectives

This chapter will discuss various layers (referred to as **key components**) that make up a CSMA, the interaction amongst these layers, and how this architecture contributes to a progressive enhancement of the Cybersecurity maturity posture of an enterprise (business). We shall further discuss the outcome of the adoption of the unified architecture as propagated by CSMA and have a look at CSMA products/solutions across various categories.

A re-look at CSMA

Layers of vulnerabilities and gaps due to the absence of interoperability of security tools/solutions are forcing security models to be redefined. Added to this equation is the ever-growing complexity of cloud (multi and hybrid) environments that is changing the threat landscape. Refer to section, **The current situation of the cybersecurity ecosystem** of **Chapter 4, The Need for Cybersecurity Mesh Architecture**, wherein most enterprises (businesses) use, on average, 45+ cybersecurity tools/solutions, which leads to unmanageable complications and maintenance overheads to manage each tool/solution.

CSMA addresses these issues by using modular technologies (also scalable and flexible) along with strong standards and policies. This creates an ecosystem of security tools/solutions that integrate across all its components and provide maximum security.

Another way of looking at this is the fact that each computing environment, such as **Infrastructure as a Service** (**IaaS**), **Software as a Service** (**SaaS**), virtual machines, endpoints, etc., is generally siloed (which means security controls are specific to the environment). CSMA enables a security posture through the integration of tools/solutions.

In effect, CSMA aids enterprises (businesses) to move towards an integrated ecosystem from a siloed/standalone philosophy. It provides a framework that revolves around analytics, controls, and threat hunting and follows Zero Trust objectives.

The benefits of implementing CSMA are depicted in the following illustration:

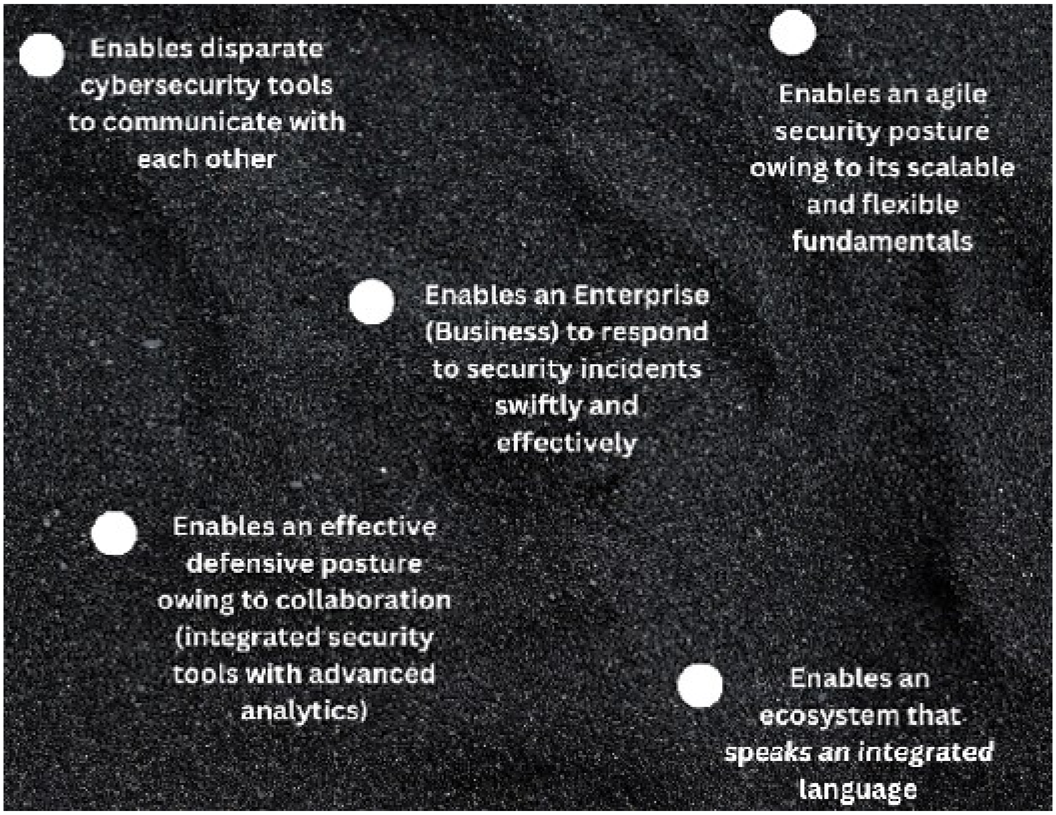

Enables disparate cybersecurity tools to communicate with each other
Enables an agile security posture owing to its scalable and flexible fundamentals
Enables an Enterprise (Business) to respond to security incidents swiftly and effectively
Enables an effective defensive posture owing to collaboration (integrated security tools with advanced analytics)
Enables an ecosystem that speaks an integrated language

Figure 5.1: *Key benefits of CSMA*

CSMA working relationship with zero trust

We have heard of zero trust many times over. Both CSMA and zero trust aim to improve the cybersecurity posture of enterprises (businesses) but have different areas of focus. Therefore, it is safe to state that CSMA does not replace zero trust or vice versa.

CSMA aids in the improvement of an enterprise' (business's) cybersecurity at an architectural level by removing silos and enabling a granular level of security. It improves the efficiency of security threat detection and incident response capabilities.

Whereas, zero trust is a philosophy of cybersecurity that needs to be implemented within a CSMA. There are some critical requirements of zero trust, such as principles of identity, authentication, access control, micro segmentation, consistent security enforcement, etc. which make up for an efficient building of CSMA.

Thus, one of the critical foundations of CSMA is zero trust, and CSMA is a wrapper for enterprises (businesses) to embrace zero trust through flexible and scalable services/tools/processes.

CSMA’s scalability relative to other architectures

Today's security architectures comprise tools/solutions that seamlessly do not work together, resulting in security gaps. Consider that you are putting together a building using interconnecting blocks. You can add pieces anywhere as part of the design, or you can take out some from a specific spot if it is not required there. You have the liberty to add or remove pieces in certain circumstances. Moreover, all the pieces work together under all circumstances.

This is known as **modular** (composable) technology and is the foundation of CSMA. This makes CSMA scalable and flexible. Such an architecture permits resources (real/virtual) to meet computing needs as they arise.

Working of CSMA

A vital principle of CSMA is to combine a set of computing tools/resources using a unified **application programming interface** (**API**). This allows the pool of available resources to be requested automatically as required for particular applications/workloads.

In CSMA, processes take an API-first approach, wherein programmers write software code after conceptualizing how an API will behave and address specific business requirements. CSMA incorporates regimented standards and security processes in the initial connections not only among applications but also between hardware and software.

When this happens, hardware becomes a secondary issue, and the connections as the process drivers become more secure and take precedence. Also, due to the usage of unified API, the new connections combine AI, M, and automation to make the enterprise (business) security scalable and less complex.

Key components of CSMA

CSMA has the following key components:

- Integrated data

- Distributed identity fabric
- Comprehensive security intelligence
- Automated operations
- Centralized operations
- Consolidated dashboards

The central themes of CSMA are modularity, scalability, and collaboration. These enable disparate security controls to work collaboratively and ease their configuration and management.

Figure 5.2 depicts the key components of CSMA:

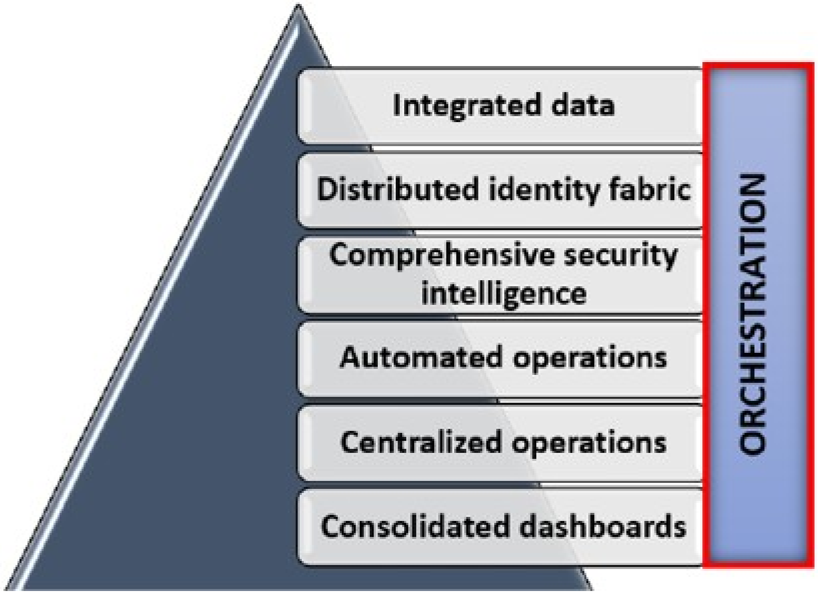


Figure 5.2: *Key components of CSMA*

Integrated data

This is the foundational component of CSMA. Integrating data from disparate sources across security systems is vital. There are distinct advantages to doing so. First, this enables security solutions/tools/products to talk to each other, which enhances each component's effectiveness and flexibility. Second, data analysis and data mining (which enhances intelligence) also become effective and meaningful.

For example, a security alert may be received from an IAM tool indicating an inappropriate access attempt or an account being created incorrectly. This could seem like an important notification, but there could be a weakness in the IAM tool, which can only be known with the assistance of other security tools/systems.

In the case of CSMA, a cloud monitoring tool may be able to correlate and associate unusual access to a cloud computing resource with a privileged account. This may lead to questioning the IAM tool for more information.

Therefore, the data integration component in CSMA is very powerful. It is not just data aggregation; it enables siloed security systems to work much more effectively through multi-event complex correlations.

Distributed identity fabric

This is a critical component that deals with IAM functions, such as directory services, management of identities that are distributed, adaptive access, authentication, authorization, and entitlement management capabilities suitable for today's distributed environments.

The need of the hour is for each verified identity to access the resources it needs from devices that are allowed and locations that are approved.

Traditionally, in standalone architecture setups, IAM functions are generally managed by different businesses, and this has the potential to leave security gaps. In CSMA, policy regarding identities is centrally managed and, therefore, applied consistently. This leads to better management of risk, lends more trust, more security, and enhanced user experience.

As an example, a **Cloud Access Security Broker** (**CASB**) continuously monitors what users are performing and will use the identity fabric to prompt the access control tool for MFA when appropriate. CSMA makes IAM tools more composable to manage the new IAM use cases.

Comprehensive security intelligence

The next component of CSMA is comprehensive security threat intelligence (and data analysis) on a real-time basis. This aspect deals with the processing of aggregated security data from disparate sources that enable cybersecurity teams to make meaningful and informed decisions. This further provides impetus to conducting data analytics to improve the overall threat intelligence for the enterprise (business). Threat intelligence is generally driven by technologies like **machine learning** (**ML**) and **artificial intelligence** (**AI**).

Many solutions operate at this level, such as:

- **Security Information and Event Management** (**SIEM**)
- **Security Orchestration Automation and Response** (**SOAR**)
- **Extended Detection and Response** (**XDR**) and
- **User and Entity Behaviour Analytics** (**UEBA**).

CSMA involves integration between solutions (such as above), enabling access to analytic tools in a central place for enterprises (businesses). This provides simplicity to both management and operational-level activities.

Automated operations

The previous components focused on integration and analysis. This one works towards streamlining management of 2Ps viz, Policy and Playbook. This is, therefore, the management component of CSMA and enables the setting up of policies. These policies govern how and when alerts are triggered and how data is processed for analytics. CSMA deals with centralization and integration and enables the setting up of policies for any component connected to the security mesh.

Whether it is SIEM logs, zero trust policies, or IAM controls, all can be configured from a central place. Similarly, event playbooks can also be integrated into security systems, lending a comprehensive security incident response.

Centralized operations

This component of CSMA covers dashboards and operational controls under one roof. A CSMA dashboard takes time to build and includes tools for investigating and reporting events and visualization tools.

Visualization tools can especially be utilized to generate a comprehensive risk score of the complete security stack in a mesh (this is only possible because of holistic security data aggregation).

Consolidated dashboards

The last component of CSMA deals with the overall security posture of an enterprise (business). Traditionally, in a standalone/distributed/siloed environment, security posture would be examined through specific dashboards, for example, an EDR dashboard for endpoints or a **Cloud Security Posture Management** (**CSPM**) dashboard for Cloud.

With CSMA, teams can have a unified (and consolidated) view of the security posture of all assets (on-premise/cloud) centered around identities in the form of dashboards. This enables swift and agile security incident response.

In summary, in CSMA, standalone/distributed/siloed solutions work together in a complementary (interconnected) manner, improving the overall security posture of the enterprise (business).

CSMA's most important component

Of these key components, we should mention the identity fabric is special because it enables security, which is driven by and based on identity. Identity is the most vital element in the security stack, as it is known to be the new edge (network), particularly in the cloud (where controls on identity are used to protect sensitive data).

In CSMA, let us remember that IAM systems provide context about events, which proves that identity is core to security.

The unified architecture of CSMA

CSMA covers a wide spectrum of integrated security capabilities across the cybersecurity ecosystem. It uses AI to power automation in order to improve an enterprise' (business') security posture in the wake of complex modern cyber threats.

Figure 5.3 depicts the core philosophies of CSMA:

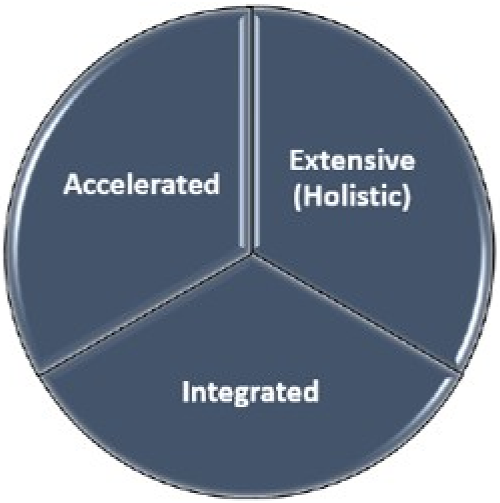


Figure 5.3: *Core philosophies of CSMA*

Let us now examine the core philosophies of CSMA, which progressively aid enterprises (businesses) in maturing their cybersecurity posture.

Extensive

A regimented CSMA needs a spate of integrated analysis tools to aggregate security data across the cybersecurity ecosystem. Please note that CSMA needs sufficient data to work and abstract the operations of the network, endpoints, and cloud security solution assuredly. enterprises (businesses) need a wide range of superior-quality security systems to support the implementation of CSMA.

For example, solutions such as zero trust access, network security, cloud security, etc., should have the required communication capabilities that would enable them to integrate into the larger cybersecurity ecosystem.

Integrated

CSMA includes an array of cohesive analysis and response mechanisms that help connect various components of a distributed IT/cybersecurity ecosystem. As mentioned earlier in this chapter (Refer to the section **Comprehensive security intelligence**), solutions such as SIEM, SOAR, EDR, etc., come under this roof. Moreover, each solution integrates with the cybersecurity ecosystem and provides the much-required threat intelligence for swift and efficient incidents.

CSMA takes time to build and progressively mature over time. It is intricate, which is evident from the fact that various features and services go into it, and is very flexible (scalable). Each part of the cybersecurity ecosystem can be tweaked over time to meet the needs of the enterprise (business).

The key to managing this goal is the integration of cybersecurity solutions. The underlying unified security architecture is thus able to reduce the complexity in the management of cybersecurity solutions/tools while enhancing threat intelligence.

Accelerated through automation

The best way to lessen operational overheads and increase the effectiveness of cybersecurity teams is through automation. We have discussed that automation is one of the key components of CSMA.

Automation (end-to-end) in detection, prevention, and threat hunting is vital to defend against a real-world cyberattack (coordinated). This enables enterprises (businesses) to proactively monitor, identify, and thwart cyber threats such as ransomware, phishing, other advanced attacks, etc.

It is equally important that policies for cybersecurity services in CSMA are managed centrally such that they can be executed swiftly and consistently when an attack occurs.

One word of caution here. There are claims that vendor products include AI and ML capabilities to enhance automation, but remember, AI and ML are as good as the data they are trained on and the people who train them. Enterprises (businesses), therefore, need to carry out their due diligence before picking up new technologies. CSMA aims to ensure that automation is trustworthy.

Major products/solutions of CSMA

Various products/solutions are required to satisfy the requirements of CSMA. Their products/solutions aid in closing the gaps and mitigation of risks.

Here is a list of major ones under categories:

Figure 5.4 lists the CSMA solutions that belong to the **Network** category:

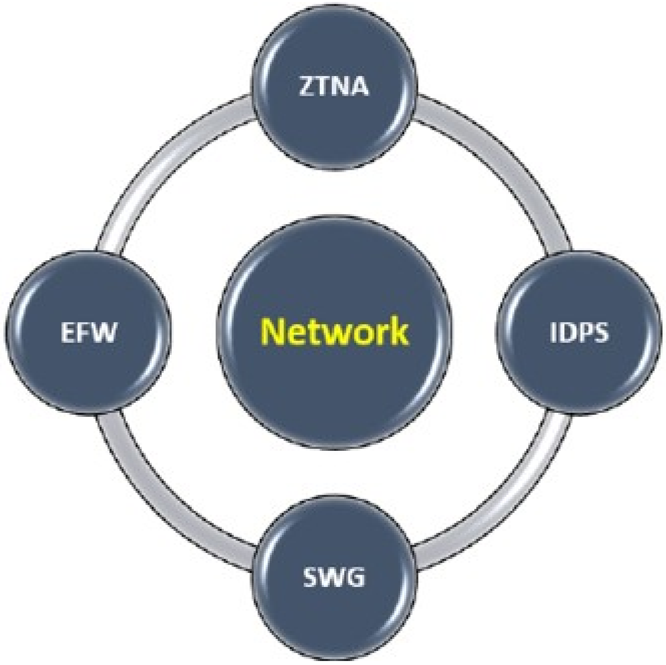


Figure 5.4: *CSMA solutions belonging to Network category*

- **Zero Trust Network Access (ZTNA)**
- **Intrusion Detection and Prevention System (IDPS)**
- **Secure Web Gateway (SWG)**
- **Enterprise Firewalls (EFW)**

Figure 5.5 lists the CSMA solutions that belong to the **Email** category:

Figure 5.5: *CSMA solutions belonging to Email category*

- **Secure Email Gateway (SEG)**

Figure 5.6 lists the CSMA solutions that belong to the **Identity** category:

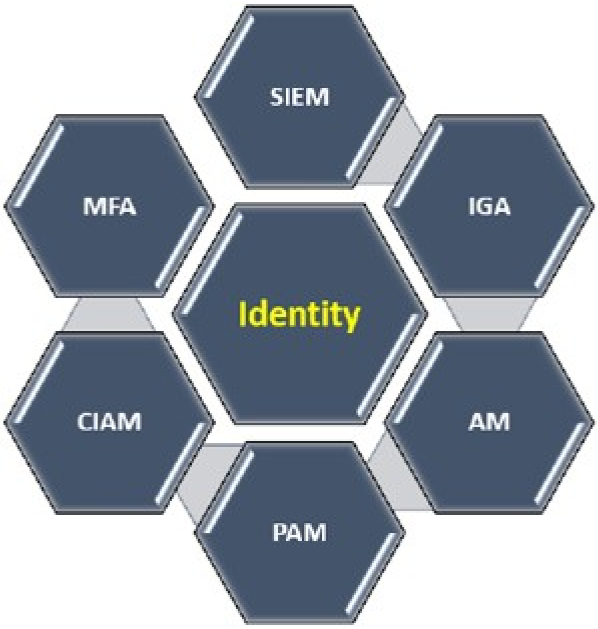


Figure 5.6: *CSMA solutions belonging to Identity category*

- Security Information and Event Management
- **Identity Governance and Administration (IGA)**
- **Access Management (AM)**
- **Privileged Access Management (PAM)**
- **Customer Identity and Access Management (CIAM)**
- **Multi-Factor Authentication (MFA)**

Figure 5.7 lists the CSMA solutions that belong to the **Data** category:

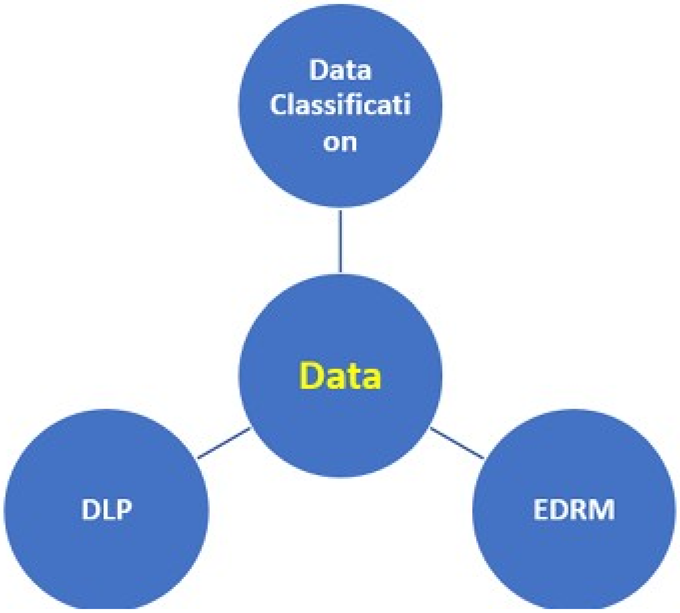


Figure 5.7: *CSMA solutions belonging to Data category*

- **Data Classification**
- **Enterprise Digital Rights Management (EDRM)**
- **Data Loss Protection (DLP)**

Figure 5.8 lists the CSMA solutions that belong to the **Applications** category:

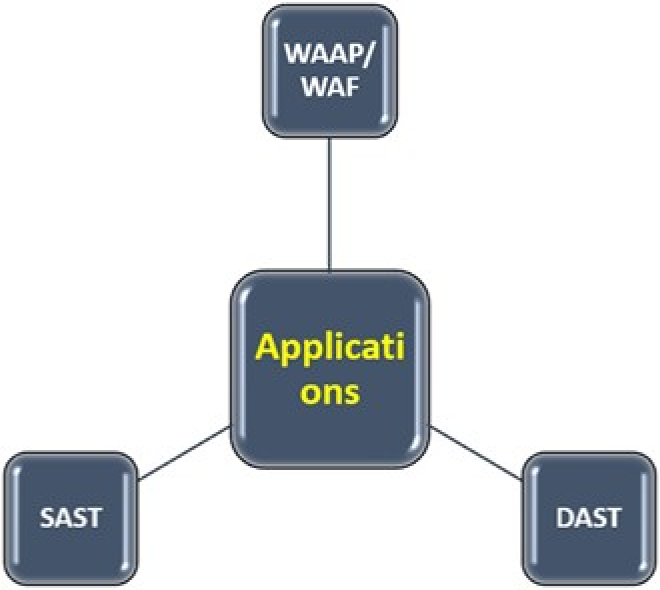


Figure 5.8: *CSMA solutions belonging to Applications category*

- **Web Application and API Protection (WAAP) / Web Application Firewall (WAF)**
- **Dynamic Application Security Testing (DAST)**
- **Static Application Security Testing (SAST)**

Figure 5.9 lists the CSMA solutions that belong to the **Devices/Servers** category:

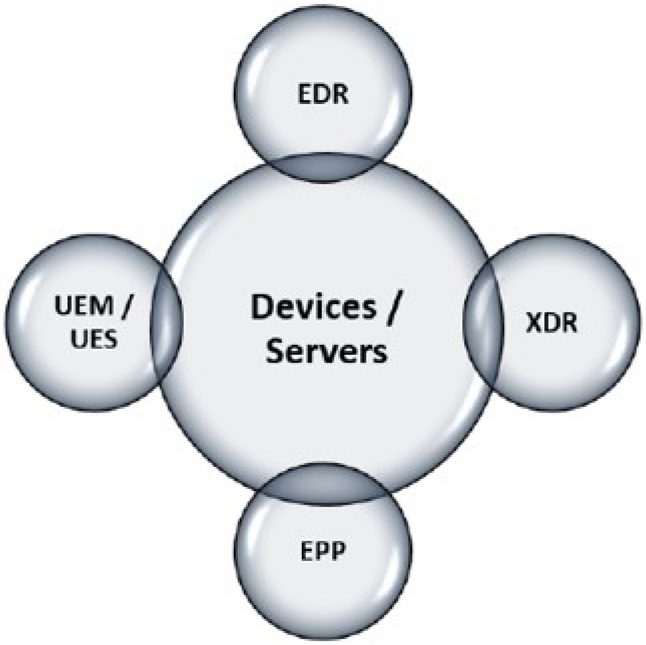


Figure 5.9: *CSMA solutions belonging to Devices/Servers category*

- **Endpoint Detection and Response (EDR)**
- **Extended Detection and Response (XDR)**
- **Endpoint Protection Platform (EPP)**
- **Unified Endpoint Management (UEM)/ Unified Endpoint Security (UES)**

Figure 5.10 lists the CSMA solutions that belong to the **Cloud** category:

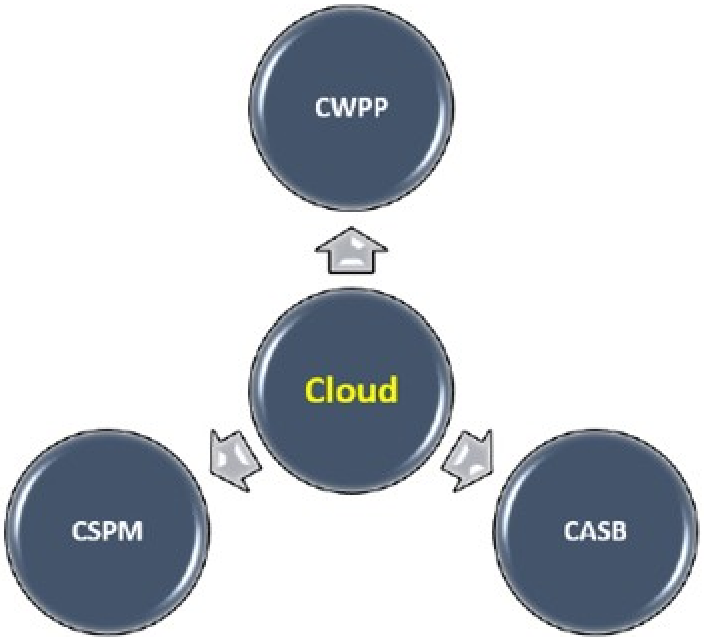


Figure 5.10: *CSMA solutions belonging to Cloud category*

- **Cloud Workload Protection Platform (CWPP)**
- Cloud Access Security Brokers
- **Cloud Security Posture Management (CSPM)**

Conclusion

Through this chapter, we understood that implementation of CSMA results in enhanced agility, flexibility, scalability, and cybersecurity posture. CSMA takes an enterprise' (business') cybersecurity infrastructure to an elevated level owing to the integration of various cybersecurity services. All communications coming in and going out of the network are protected, making it safer. A message to all enterprises (businesses) is to be future-ready. Choose cybersecurity solutions that facilitate integration. Use plug-in APIs to aid customization and interoperability (further aiding data analytics and threat intelligence).

Bridge security gaps due to weaknesses/vulnerabilities, if any, in cybersecurity solutions using current and enhanced CSMA security standards.

Implement all key components of CSMA by laying emphasis on all key components, such as data integration, identity fabric, policy management, security analytics, threat intelligence, and integrated dashboards. A combination of all components (aka overarching solution), provides an end-to-end and a holistic cybersecurity ecosystem. In the next chapter, we shall further into the unified architecture of CSMA, discuss the importance of integration, comprehensiveness, and automation in CSMA, and examine the key factors to consider while adopting CSMA.

Points to remember

- CSMA creates a way for distinct/standalone cybersecurity services to communicate and integrate.
- CSMA enhanced the cybersecurity posture of an enterprise (business) by making it more agile, scalable, and flexible.
- CSMA facilitates enhanced collaboration, analytics, and threat intelligence thereby greatly enhancing incident response.
- The key foundational layers of CSMA, viz., Integrated data, distributed identity fabric, comprehensive security intelligence, automated operations, centralized operations, and consolidated dashboards, provide a roadmap for implementation.
- CSMA and zero trust should not be used interchangeably.
- While CSMA focuses on granular and integrated security, the zero-trust principle removes implicit trust and provides visibility and control over each access request performed within its ecosystem.
- Zero trust is one of the critical foundations of CSMA.

Key terms

- **Zero Trust Network Access**: Technology and functionality set that enables secure access for remote users to internal applications.
- **Secure Web Gateway**: Protects enterprises (businesses) from online security threats by enforcing policies and filtering Internet traffic. It is available on-premise or via cloud
- **Enterprise Firewalls**: Controls network traffic between untrusted sources (e.g., public Internet) and trusted sources (e.g., the private

enterprise network).

- **Secure Email Gateway**: Security solution used for emails that filter emails for suspicious and potentially malicious content.
- **Identity Governance and Administration**: Facilitates security administrators to manage user identities and access across the enterprise (business) efficiently.
- **Access Management**: Practices that enable an entity to act on a particular resource when explicitly permitted.
- **Privileged Access Management**: Security solution that protects an enterprise (business) against cyber threats by monitoring, detecting, and preventing unauthorized privileged access to critical resources.
- **Customer Identity and Access Management**: Enables enterprises (businesses) to capture (securely), manage customer identity/profile data, and control access to applications/services.
- **Enterprise Digital Rights Management**: Controls and manages access to enterprises' (businesses') copyrighted material.
- **Data Loss Protection**: Cybersecurity solution to detect and prevent data breaches (through leakages).
- **Web Application and API Protection**: Cybersecurity technologies aimed at protecting web applications and APIs from sophisticated cyberattacks.
- **Web Application Firewall**: Protects web applications through monitoring and filtering HTTP traffic between the web application and the Internet.
- **Dynamic Application Security Testing**: A black-box testing to find out vulnerabilities in web applications from outside of the enterprise (business).
- **Static Application Security Testing**: A white-box testing that finds out vulnerabilities inside the application and code.
- **Extended Detection and Response**: XDR combines data from multiple security products, including EDR, network, cloud, and email security, to provide a holistic view of security threats across the enterprise (business).

- **Endpoint Protection Platform**: Cybersecurity solution built to detect and block threats at the device level.
- **Unified Endpoint Management/Unified Endpoint Security**: UEM solutions carry out general management of endpoints at scale. UES delivers some management capabilities however, it focuses on security.
- **Cloud Workload Protection Platform**: Security solution or cloud that protects cloud workloads in a multi-cloud/hybrid environment.
- **Cloud Access Security Brokers**: Provides security policy enforcement between CSP and consumers (can be on-premises/cloud-based).
- **Cloud Security Posture Management**: Security tools built to find out misconfiguration issues and compliance risks in the cloud.

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

CHAPTER 6
How to Effectively Adopt Cybersecurity Mesh Architecture

Introduction

In the previous chapter, we discussed the fundamental components of CSMA, which enable it to deliver a strong framework for security infrastructure. While the modern digital world witnesses advanced threats that are constantly evolving, various state-of-the-art edge security tools rise to the occasion to address this challenge (but in a highly distributed environment). CSMA takes this response to the next level by integrating these resources.

In this chapter, we will discuss what to expect when adopting a CSMA and how enterprises (businesses) can effectively prepare for the future.

Structure

In this chapter, we will cover the following topics:

- Performance
- Cybersecurity landscape of today
- Key aspects for CSMA adoption
- Getting started with CSMA
- Key factors to consider while adopting CSMA

Objectives

We discussed the key foundations of CSMA in *Chapter 4*, *The Need for Cybersecurity Mesh Architecture*. For new enterprises (businesses), these key foundations present a blueprint for designing and building the cybersecurity architecture. However, this is challenging for many enterprises (businesses) due to the existing legacy of the IT ecosystem comprising various security solutions.

No one vendor can provide all the required building blocks, comprehensive standards are in the works, and cybersecurity products/services do not generally interoperate. The objective of this chapter is to walk through the steps enterprises (businesses) can undertake to adopt a comprehensive CSMA.

Performance

Let us examine the treatment of cybersecurity challenges thus far. Standalone/siloed cybersecurity solutions have a tradition in dealing with these challenges. Enterprises (businesses) have thrown standalone solutions for endpoint security, cloud security, network security, email security, etc., in the fold and try to deal with the challenges.

This is unfortunately not workable. Modern-day IT infrastructure operational needs are complex. For example, IoT, hybrid clouds, an employee using more than one device, and offices that are geographically spread and separated are increasingly complex (resources are widely distributed).

There is no way this ecosystem will change because this is lending effectiveness and competitiveness to enterprises (businesses).

Problem with past solutions

While it may feel satisfying (the most suited course of action) to have a best-fit security tool for an individual component of the IT ecosystem, this treatment of securing the IT ecosystem misses something critical.

Large and mid-sized enterprises (businesses) generally have resources spread across multiple geographies and technologies, which means it is not a matter of securing each component of the ecosystem infrastructure, but what matters the most is how to secure all of the components simultaneously and effectively.

Best-fit security solutions/tools may be reasonable answers to specific security challenges, but that is now how the modern IT ecosystems are put together.

Modern-day IT ecosystem is about the co-existence of networks, end-points, cloud resources, and edge devices. They do not exist or work in isolation. These components are dependent on each other to function properly; therefore, they need to be secured together.

It is important to look at these components in an integrated manner. For example, advanced firewalls may get breached and there has to be a way to swiftly determine the other areas where an attack might have been perpetrated.

This is a known constraint of standalone/siloed security solutions. Their ability to communicate with each other is limited, which further hinders their capability to detect. Also, the potential for responding to security incidents and breaches gets impaired.

When IT ecosystems were simpler (with fewer IT components and more centralized), standalone/siloed security tools/solutions worked well. Siloed configurations are much less effective now, with complexities rising in the IT ecosystem.

When security tools/solutions do not talk to each other, security teams have less visibility of the attack surface. This has an impact on the teams as they get separated from each other, thus not benefiting from interactions with other experts.

Please remember that the security and operation teams in an enterprise (business) that interact with each other work more effectively. Therefore, it is imperative that security staff work on problems centrally, where holistic and comprehensive security controls enable them to adjust to newer cyber threats.

Answer lies in the unified architecture

In the past, we have seen the emergence of various security solutions, such as SOAR, which work to unify the security infrastructure. Though they have added value to many enterprises (businesses), they are missing the more extensive foundation that endorses philosophies of integration and aggregation of security data. It is vital for a successful ecosystem nowadays to have integrated visibility.

Attackers have a reasonable understanding of the attack surface of an enterprise (business) and, thus, know how to take advantage of weaknesses due to this awareness. It is the element of security tools'/solution's data generation to be centrally visible that a CSMA brings to life.

We have also realized that automation has been a savior to enterprises (businesses) and cyber attackers who utilize these tools to maneuver through compromised systems swiftly.

Two aspects are best suited to counter these evolving threats: security controls that are centralized and tools that are automated. Cybersecurity experts should solve complex problems where possible and not waste their precious time shutting down network ports to thwart a threat.

Another challenge discussed in the previous chapters is the lack of security talent. While the cybersecurity experts already on board should be leveraged to increase the security posture, CSMA makes automation of security and centralized policy management possible.

With the visibility of all vital security components and being centrally managed, security and operation teams can configure, detect, and reassess swiftly.

Cybersecurity landscape of today

The cybersecurity landscape today is like a game of table tennis between cybersecurity professionals and cyber attackers.

Exploring the game reveals that types of cyberattacks keep evolving (some attacks keep falling out, and others emerge), and cybersecurity experts, in response, keep innovating new defense techniques to counter this challenge.

Figure 6.1 depicts the top challenges for the adoption of CSMA:

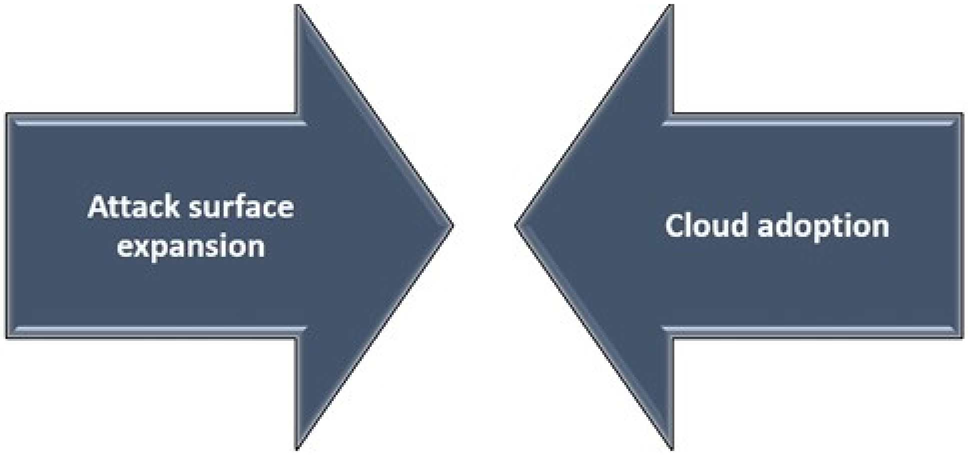


Figure 6.1: *Top challenges for CSMA adoption*

Attack surface expansion

The post COVID era has witnessed a major shift from work-from-office to hybrid working (owing to the push to work from home). Employees are increasingly taking corporate devices to their homes, connecting them to home networks, thereby becoming more vulnerable to attacks on the endpoint device/phishing attacks as compared to a situation when they were working from office premises.

The cybersecurity and operation teams need holistic visibility to observe how and when attacks take place, especially threats where it is not easy to identify sources. Let us consider a few examples in this context:

- An attack emerges from an endpoint device. As the attack surface expands, it becomes harder to determine the source of such an attack.
- An attack is noticed by way of network detection. This necessarily does not mean that the network is the source of the breach. A distributed IT ecosystem makes it even more difficult to investigate and analyze such an attack.
- An attack dealing with the exfiltration of data from a database. This could render cybersecurity teams clueless about its source. A siloed security system would have difficulty finding the source of the problem, not to mention other potential points of infiltration.

We know that analysis begins after a threat is detected and remediated. Even though cybersecurity teams become knowledgeable regarding system weaknesses through analysis, a lack of comprehensive visibility can impede investigations.

Modern-day IT ecosystems need cybersecurity tools that can carry out comprehensive analysis after an attack, and a CSMA enables this.

Adoption of cloud

Over the last few years, enterprises (businesses) have been working to move their workloads to the cloud, predominantly to utilize the benefits of cloud technologies. However, one common concern among everyone is the security concerns surrounding cloud adoption. Two common concerns in this light are inadequate visibility and the absence of comprehensive security controls.

We have seen how complex an IT ecosystem is. The adoption of the cloud adds a layer to this complexity. What increases the security risk are the following aspects: new entry points for attackers, new tools, and unfamiliarity of staff (administrative/engineering) with new technologies.

If the lack of visibility and absence of comprehensive controls is added to this mix, the challenge is further compounded. If this is not enough, many enterprises (businesses) work in a hybrid/multi-cloud mode where technologies differ, further adding to the complexity.

CSMA is a method of addressing security challenges in the cloud by aggregating security data from a wide variety of security resources and then centralizing security controls to ensure ease of use.

Security tools need integration and aggregation in the future, and CSMA is a flexible and scalable method to commence nurturing that kind of security ecosystem.

Key aspects for CSMA adoption

Truly modern security systems are more than just tools to meet today’s cybersecurity threats. They are collections of methods and solutions that meet those threats while allowing for flexibility in the ever-changing security landscape.

CSMA enables the creation and maintenance of dynamic security systems while also adding powerful integration and aggregation capabilities that promote a strong security posture.

In this section, let us review some of the key points of cybersecurity meshes that make it a strong, modern option for hardening your organization's resources against both old and new attacks.

Figure 6.2 lists the key aspects for adoption of CSMA:

Integration
Comprehensiveness
Automation

Figure 6.2: *Key aspects for CSMA adoption*

Integration

Amongst many vital aspects of a strong cybersecurity ecosystem are the visibility of data and infrastructure. This helps combine security resources centrally, thus aiding in preventing hackers from operating in a stealth mode and exploiting a weak spot.

CSMA works to create connections among security tools/solutions that were otherwise standalone/siloed and enables aggregation of security data for easier analysis and observability.

A holistic data collection capability also allows the system to learn from past cyberattacks and progressively improve the cybersecurity posture. CSMA enables the integration of security data sources. This supports security and operation teams in swiftly and efficiently collecting and analyzing information after an incident.

Similarly, visibility across the cybersecurity ecosystem in an integrated manner, with near- almost real-time updates, enhances the speed of detection and response.

Therefore, enterprises (businesses) need to address the absence of integrated visibility and lack of central control to maintain and secure a multi-cloud environment.

Comprehensiveness

We just referred to visibility as one of the vital aspects of a strong cybersecurity ecosystem. However, visibility does not have meaning if you cannot do much with it. Equally vital is for the cybersecurity ecosystem to be flexible (scalable) and efficient through strong control capabilities.

CSMA works towards centralizing security controls (as much as possible) by aggregating data and creating comprehensive dashboards (central consoles for efficient control). The benefits of central access are efficient reporting, swift investigation, and real-time alerting.

CSMA does not only lead to the integration of security data but also lends a centralization theme to control the IT ecosystem. Orchestration and policy management are centralized in a CSMA.

Policies are not required to be set on a one-on-one basis for a wide variety of security tools/solutions because, in a CSMA environment, tool/solution functionality is integrated.

Automation

When cybersecurity tools/solutions are integrated into a control system centrally, automation of security tasks becomes effective and powerful. It is not only cyber attackers who use automation to swiftly move laterally through systems to carry out complex attacks. Automation is equally useful for defense tools in the present circumstances (and will be in the future as well).

CSMA enables a variety of tasks to be automated with great flexibility. Device configuration tasks can be set up centrally, so they can be notifications/triggers freeing up the time of security and operation teams.

Overall, CSMA is built to weave automation of tasks through cybersecurity tool/solution integration (by leveraging AI and ML) that enables dynamic policies and configurations.

Getting started with CSMA

The key components of CSMA, as discussed in detail in *Chapter 4*, *The Need for Cybersecurity Mesh Architecture*, present a blueprint roadmap for designing, building, and implementing CSMA.

This is true for a greenfield setup, but for many enterprises (businesses), the start will be from a legacy IT ecosystem—a complex ecosystem with many cybersecurity tools/solutions already in place.

Many challenges need to be overcome for a successful adoption of CSMA. For example:

- A single vendor does not have all the building blocks required for CSMA
- Standards required for CSMA are still in the works
- Tools/solutions do not yet provide the required interoperability

Despite this, the following steps shown in *Figure 6.3* can help enterprises (businesses) advance toward an effective implementation of CSMA implementation:

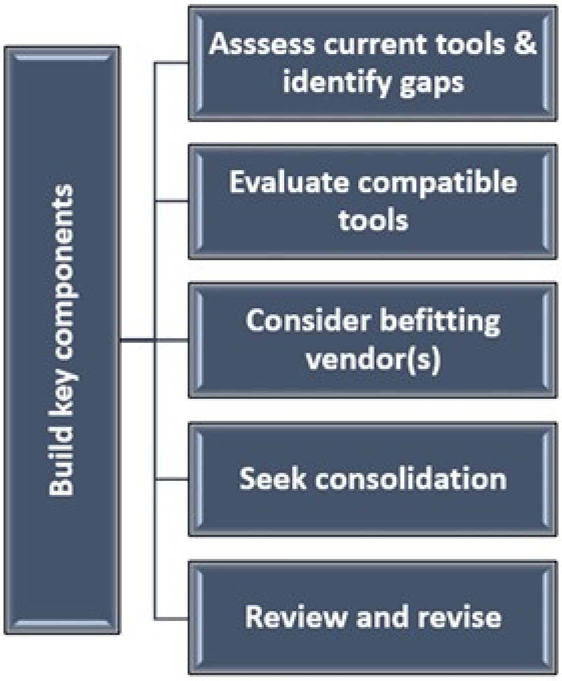

Build key components
Asssess current tools & identify gaps
Evaluate compatible tools
Consider befitting vendor(s)
Seek consolidation
Review and revise

Figure 6.3: *Key steps to get started with CSMA*

Assess current tools and identify gaps

As for any cybersecurity program, the first step is to review your existing cybersecurity strategy, risk profile, tools/solutions, controls, and skillsets. The need is to comprehensively map out the data flows between various tools/solutions.

The vital next step is to assess the maturity of the current tools/solutions based on their functionality and integration capability. Seek out the gaps leading to white spaces (blind spots) in your infrastructure. For example, are there missing risk signals about device status or an inability to track a user's activity (on-premises/on the cloud)?

Build the key components

Next, commence the development of key components (refer to section *Key components of CSMA* in Chapter 4, *The Need for Cybersecurity Mesh Architecture*) as follows:

- **Data integration**:
  - This is a powerful component in CSMA.
  - Evaluate tools/solutions that support data aggregation enabling effective working of siloed security systems with the ability to perform multi-event correlations.
- **Distributed identity fabric**:
  - This is the most critical component.
  - Seek tools/solutions that assist in the central administration of identities and can strictly enforce access policies (sophisticated) across the IT ecosystem.
- **Comprehensive threat intelligence** (**and analytics**):
  - Tools/solutions such as SIEM, UEBA, SOAR, XDR, etc., that can integrate well with the core cybersecurity and identity solutions.
  - Provide risk scoring that is dynamic and entity-based.
- **Automated and centralized operations**:

  - Look for tools/solutions that can streamline the management of 2Ps, such as policy and playbook.
  - Have the capabilities aligned with NIST, CIS, and ISO (globally recognized and established security standards).
- **Consolidated dashboards**:
  - Works towards an ideal dashboard that will provide clear visualizations of risk scoring and alerts on a real-time basis and comprehensive insights.
  - Decide whether you are seeking multiple views (for different IT security and stakeholder roles), as well as advanced features such as customizable widgets and reports.

Evaluate compatible tools

Enterprises (businesses) need to choose security tools/solutions and services capable of deep integration. As mentioned earlier, standards for CSMA are still in the works, but some of the current examples are as follows:

- OAuth 2.0
- OpenID Connect
- **System for Cross-domain Identity Management (SCIM)**
- **Open Policy Agent (OPA)**

Equally important is the principle of open APIs, which enables cybersecurity tools/solutions to share information seamlessly, including the context of identity and risk intelligence.

For example, if we want the network firewall and email gateway to be able to make decisions regarding authentication, the two entities should be able to communicate with each other first and foremost.

Consider befitting vendor(s)

So far, we have emphasized the choice of cybersecurity tools/solutions. Choosing a quality vendor(s) is as vital as the tool/solution. Suitable vendors with extensive experience and a proven track record of being receptive to changes in the cybersecurity landscape and adjustable in assisting customers secure their ecosystems.

Seek consolidation

Post-evaluation of suitable vendor(s) and cybersecurity tools/solutions, enterprises (businesses) should look to simplify their cybersecurity stack and licensing regime. This can be achieved through vendor and tools/solutions consolidation.

Many enterprises (businesses) in today's world have already commenced the journey of cybersecurity vendor consolidation.

This level of consolidation should be at an appropriate level. If an enterprise (business) is seeking one identity provider to limit its identity fabric, it may not be reasonable to effectively manage all the use cases.

There are various internal employee groups, external contractors, customers, partners, etc. All these entities have specific identity use cases that will be difficult to manage.

It is advisable to have a CSMA vision with an underlying cybersecurity roadmap of tools/solutions/services. The objective should be to have an integrated ecosystem of tools and standards that does not lead to elevating your technical debt in the long run.

Review and revise

Designing and implementing CSMA is not a one-time activity; rather, it is an ongoing project. It cannot be static since everything around the enterprise (business) is continuously changing, viz., business requirements, standards, technologies, available tools/solutions/services, threat landscape, etc.

It is vital to evaluate the performance and effectiveness of your cybersecurity posture in a regimented manner. This will enable you to make adjustments as required.

Here, you should specify the metrics that are required to be tracked and reviewed regularly and measure how a CSMA strategy is having an impact on business outcomes.

The key is to monitor areas where weaknesses exist. These can include tools/solutions/services that are deficient in functionality, do not integrate well with other entities in the ecosystem, and are not adequately supported by vendor(s).

Also, as a matter of agility (timely action), keep an eye on product enhancements. Any increase in the maturity of a tool/solution can present an opportunity for consolidation which can be a boon to simplifying the technology stack.

Key factors to consider while adopting CSMA

We have seen many advantages associated with the adoption of CSMA, but let us now explore reasons why enterprises (businesses) are considering going this route.

Figure 6.4 lists the factors for considering CSMA:

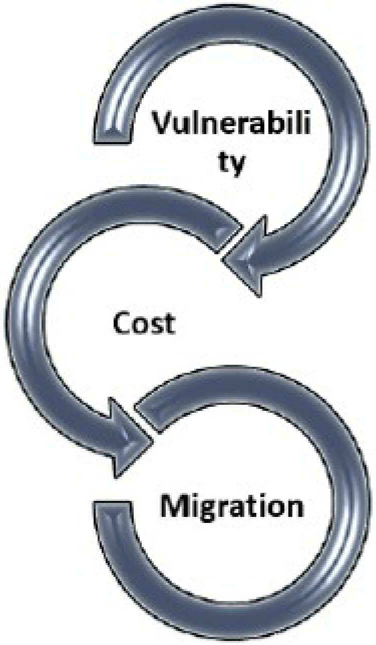


Figure 6.4: *Factors for considering CSMA*

Let us look at the following factors:

- **Vulnerability**:

  - IT ecosystems are vulnerable to phishing and ransomware attacks, both of which have been on a steady rise year-on-year.
  - If this is not difficult enough, there exists the danger of a zero-day attack (explained in the previous chapters, this is an attack by a method that was unknown previously).
  - CSMA enables an enterprise (business) to reduce these vulnerabilities significantly and prepares its cybersecurity infrastructure for such attacks.
- **Cost**:
  - Global ransomware damage costs will reach $20 billion by 2021 (57x more than it was in 2015), and the cost of cybercrime attacks is on the rise at about 15% per year over the next five years[1].
  - There is a huge cost of digital transformation as well for enterprises (businesses) whose infrastructure/architecture has to undergo redesign.
  - It is reasonable to state that the reduction in attacks (costly) and downtime due to leveraging CSMA far outweighs any initial cost.
- **Migration**:
  - Many clients/consumers have shifted to cloud computing owing to their benefits, which has led to an increase in data breaches.
  - CSMA enables migration to cloud computing by providing flexible and scalable protection.

The above-mentioned factors showcase the need for CSMA. *Figure 6.5* lists the add-on factors for considering CSMA:

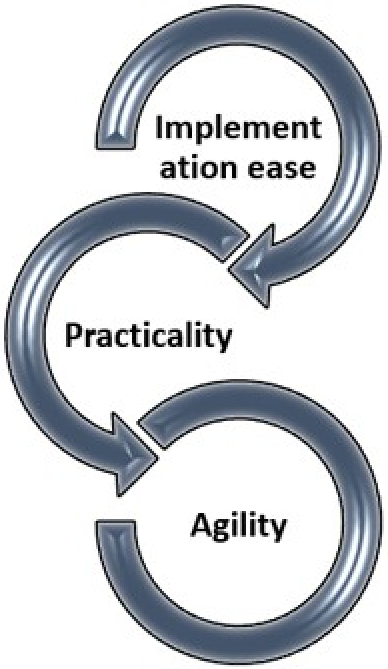


Figure 6.5: *Add-on factors for considering CSMA*

Let us have a look at the add-on factors that deliver more attractiveness to adopting CSMA:

- **Implementation ease**:
  - Accelerated growth of digitalization over the years has led to rendering traditional security models top-heavy and difficult to manage.
  - CSMA is distinctively tailor-made to enable simplicity and efficiency in designing, deployment, and maintenance.
- **Practicality**:
  - Old-style cybersecurity policies, methods, and techniques are complicated due to cloud computing technology, distributed data, and uncontrolled devices.
  - The CSMA strategy presents a practical way to deal with aspects/components that do not lie inside the traditional network perimeter of an enterprise (business).
- **Agility**:

- This has been previously discussed. The very nature of the CSMA approach renders an enterprise (business) to respond to security and expansion in a more agile manner.
- The benefits of modularity, scalability, and collaboration are as follows:
    - Nodes can be modified (added/removed) relatively easy
    - A central control point can be used to monitor and control new locations

Conclusion

CSMA is a modern approach (conceptual) to build a security architecture to address the challenges of a distributed enterprise (business) and to say the least, the continually evolving (changing) threat landscape/attack surface.

Various benefits of adopting CSMA in the wake of embracing digital transformation and the evolving sophistication of cyber threats are deployment of security controls where needed the most, establishment of granular access controls, prioritization of identity-centric security, collaboration amongst security tools/solutions/services, provision of centralized management, enablement of end-to-end automation, increased visibility and control, enhancement of scalability and flexibility, establishment of a strong framework to strengthen the overall cybersecurity posture and enhancement of business resilience.

Conclusively, the adoption of CSMA is an involved process and worth the investment by an enterprise (business). It delivers benefits swiftly in this progressive journey wherein every step taken leads to improvement in cybersecurity posture, simplification of operations, and positioning an enterprise (business) for a brighter future.

In the next chapter, we shall re-examine what necessitates the adoption of CSMA, the benefits of leveraging CSMA, discuss the characteristics of a CSMA strategy, delve into a few target use cases, and learn about the pitfalls of not leveraging CSMA.

Points to remember

- Principles for an effective CSMA involve the adoption and deployment of cybersecurity tools/solutions/services that are not only fit for purpose but also work within and across the ecosystem (integrated)
- An effective CSMA enables intelligence sharing, automated and coordinated response to cybersecurity incidents, and simplification of operations
- An effective CSMA transforms an enterprise (business) legacy fit-to-purpose ecosystem from a standalone/siloed to a fit-to-purpose and integrated ecosystem

In summary, the adoption of CSMA enables enterprises (businesses) to stay business (cyber) resilient in this ever-evolving digital world, maintain customer trust, and reduce the financial impact of security incidents.

Key terms

- **Open Authorization**: OAuth 2.0 is the industry-standard protocol for authorization.
- **OpenID Connect**: It is an identity layer on top of the OAuth 2.0 framework. It allows third-party applications to verify the identity of the end-user and to obtain basic user profile information.
- **System for Cross-domain Identity Management**: A specification and an open standard designed to manage user identity information.
- **Open Policy Agent**: OPA is an open-source engine that provides a way to write policies as code and then use these policies for decision-making.

---

[1] **https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/**

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

CHAPTER 7
Benefits of Adopting Cybersecurity Mesh Architecture

Introduction

Primarily in Chapter 1, *Cybersecurity: A Dynamic Changing Paradigm*, we had a look at the chronology of the evolution of cybersecurity, and some major trends that had a noteworthy impact. Chapter 2, *Cybersecurity: Understanding Today's Security Challenges*, dealt with understanding distributed systems (working and challenges) and overall cybersecurity challenges in the digital age. Whereas, Chapter 3, *Emerging Cybersecurity Trends*, covered the emerging cybersecurity trends and the importance of cyber resilience.

In Chapter 4, *The Need for Cybersecurity Mesh Architecture*, we first inked the need for CSMA and the benefits of its adoption. Chapter 5, *Fundamental Components of Cybersecurity Mesh Architecture*, covered the fundamental components of CSMA delivering a framework for security infrastructure. In Chapter 6, *How to Effectively Adopt Cybersecurity Mesh Architecture*, we discussed what enterprises (businesses) can expect when adopting the architecture and how they can effectively prepare for the future.

In this chapter, we will re-examine the need for CSMA, the benefits of adopting the same, and the pitfalls of not leveraging it.

Structure

In this chapter, we will cover the following topics:

- What is the necessity of CSMA

- Benefits of leveraging CSMA
- Characteristics of a CSMA strategy
- Target use cases
- Features to be considered for CSMA solutions
- Pitfalls of not leveraging CSMA

Objectives

We are living in a world that is witnessing an ever-increasing digital acceleration. This is leading to a swift adoption of new technologies across the IT ecosystem (including cloud migration). It is not surprising to see enterprises (businesses) moving first (say even to multi-cloud) and later asking themselves how to manage and secure these environments.

We also have many organizations with standalone/silos tools/solutions/services. This leaves their cybersecurity teams to manage the mesh and complexities of the resulting makeshift arrangements.

These standalone/siloed environments, related complexities, and visible gaps provide opportunities for cyber attackers to exploit. This is further exacerbated by resource and skill gaps in cybersecurity (Refer to section *Trend 14: Widening IT skills gap* in *Chapter 3*, *Emerging Cybersecurity Trends*).

It is time for enterprises (businesses) to transform their present approaches to cybersecurity that have a standalone/siloed approach. For this transformation, they need to adopt CSMA as the baseline (building block). This would enable them to integrate their distributed ecosystem and create consistency, interconnectivity, collaboration, and automation across the various tools/products/services to drive their digital acceleration initiatives.

In the subsequent sections of this chapter, we shall re-look at why CSMA is necessary to be adopted by enterprises (businesses), cover its benefits, discuss what a CSMA strategy should look like, take a deeper look at CSMA target use cases, and examine the downsides of not leveraging CSMA.

What is the necessity of CSMA

With the acceleration of remote work, adoption of public and private cloud, IoT intermeshed with traditional IT, the proliferation of ransomware, and lower barrier entry for startups to challenge large enterprises, there has never been a more critical need to adopt a CSMA. The network no longer has an edge, trust is at zero, assets are proliferating and managed by different teams, and visibility is partitioned to siloed teams.

Without a centralized place to assess if appropriate layers of security controls are properly implemented across the network, enterprises face a more complicated challenge in identifying and managing their attack surface than ever before.

The centralization of security control assessment enables enterprises to save operational overhead and prioritize business-impactful risk. With a centralized platform for CSMA, smaller teams achieve more, larger teams communicate and coordinate more effectively, and siloed teams leverage one another's tools to align to risk reduction based on business impact and not by irrelevant risk scores.

Benefits of leveraging CSMA

The benefits of adopting CSMA have been described in detail in section *Benefits of CSMA, Chapter 4, The Need for Cybersecurity Mesh Architecture*. Presenting in this section is a fresh perspective of describing the benefits in an abridged manner.

Refer to *Figure 7.1* that depicts the benefits of leveraging CSMA:

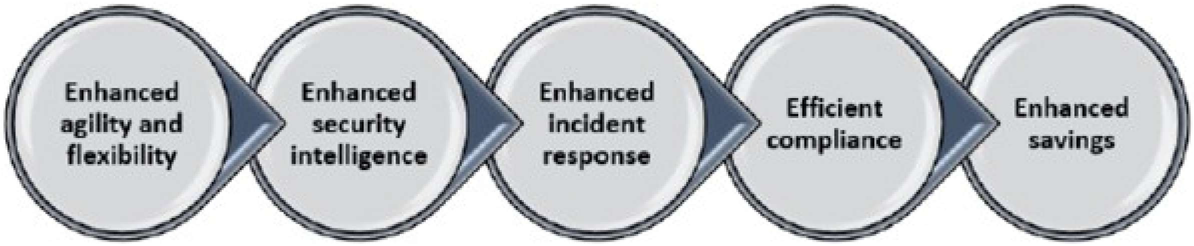

Enhanced agility and flexibility
Enhanced security intelligence
Enhanced incident response
Efficient compliance
Enhanced savings

Figure 7.1: *Benefits of leveraging CSMA*

Enhanced agility and flexibility

Due to leveraging CSMA for collective consumption, an enterprise's (businesses') security tool/service data integrates consistently and is structured. This leads to reliable validation and security policy enforcement. With this, it is possible to deploy new applications and infrastructure repeatedly and scalable (swiftly). Also, any nonconformities are identified regularly and submitted for remediation automatically.

As the utility of data sets increases, subsequent increases are seen in the **return on investment** (**RoI**) of existing technologies (security and infrastructure). Cybersecurity teams are no longer required to do any manual intervention with this data.

In summary, each cybersecurity solution (monitoring/alerting) in CSMA is intertwined with one another. This provides a mesh in the ecosystem that can be navigated easily.

Enhanced security intelligence

Security intelligence (cross-domain) is a reality since data is meshed together in CSMA. This allows all teams to entrench domain intelligence for their decision-making purposes.

Such security intelligence, when enabled, enables cybersecurity teams to make informed decisions that are non-disruptive while responding to security incidents (aka coordinated response). Since security and infrastructure services data is accessible for immediate analysis, as a resultant this provides:

- Availability of asset-wide security intelligence
- Identification of control gaps
- Visibility of network connections and dependencies
- Understanding of the business impact of quarantine/changes in the network
- Identification of insider threats

Due to the above-mentioned aspects, cybersecurity teams can leverage integrated security data to provide more contextual-centric responses and communicate discoveries (findings) via visualizations in an effective manner. As a result, analysis is reduced to minutes from hours during incident response.

The benefits for vulnerability management teams are also immense, as they can:

- Swiftly identify asset owners
- Have deeper visibility of business (applications) and network context, thus can:
  - Prioritize assets
  - Understand which vulnerabilities are the most prevalent
- Effectively communicate risk

Overall, CSMA leads to the elimination of manual activities such as control analysis of security gaps and remediation.

Let us consider an example of SIEM. Due to the integration of security tools/solutions/services (conversion of logs), the data aggregated by SIEM can be used across cybersecurity teams on an immediate basis for business risk reduction proactively (since prioritization of most exposed assets is known contextually). This is also a major consideration when arriving at ROI.

The key here is the accessibility of security data across cybersecurity teams that provides them the ability to:

- Derive business risk reduction through quantified and qualified methods
- Communicate with business (non-technical staff) effectively

Not only the cybersecurity teams but also the business teams are enabled to communicate technical subjects with their teams.

Enhanced incident response

Security intelligence (cross-domain) provides maturity to security processes. By virtue of this security, operations become increasingly efficient. In the past before leveraging CSMA, cybersecurity incident response teams would be subjected to correlating huge volumes of data sets manually to address questions related to asset intelligence. This would lead to stretching both **mean time to resolve** (**MTTR**) and **mean time to containment** (**MTTC**).

Generally, the context of most cybersecurity incidents and alerts is very limited and needs enrichment on a manual basis. Limited context means incidents/alerts may contain only:

- An IP address
- A hostname
- An interface
- Username (in case of insider threat)

Integration of multiple data sources in case of CSMA lends cybersecurity analysts to address the following queries swiftly and effectively:

- Which device is tied to the IP address (highlighted in the security incident/alert)?
- Which part of the core business function/service is the device a part of?
- Is sensitive data stored in the device?
- Will there be any business downtime due to containment activities?
- Which devices have an affected user logged into?

This exemplifies the need for CSMA. The limiting factor with previous ecosystems/architectures was the non-interoperability of cybersecurity tools. This inadequacy hampered swift decision-making for effective incident management.

In summary, CSMA brings about interoperability and cohesiveness of cybersecurity tools/platforms, resulting in effective decision-making owing to enhanced visibility of contextual information and a reduction in the MTTR of cybersecurity incidents and responses.

Efficient compliance

Leveraging CSMA leads to a reduction in compliance-related obligations and risks. This is due to the simplification of compliance monitoring, where the assessment process is centralized through maximization automation.

In addition, CSMA assists security teams in comparing their enterprises (businesses) standards to industry standards, viz., the **National Institute of Standards and Technology** (**NIST**).

Enhanced savings

The cost of ransomware attacks and cybercrime attacks is increasing year on year. Digital transformation incurs its own cost, too, especially if an enterprise's (business) infrastructure/architecture has to be redesigned. However, the reduction in costly attacks and business downtime realized by leveraging CSMA far outweighs any initial cost.

CSMA saves precious time and resources for cybersecurity teams by eliminating the need for aggregating data manually and the use of multiple query languages.

Characteristics of a CSMA strategy

The main characteristics of CSMA include:

- Integration
- Comprehensiveness
- Automation

Refer to *Chapter 6*, *How to Effectively Adopt Cybersecurity Mesh Architecture,* section, *Key aspects for CSMA adoption,* for more details.

These characteristics are vital for the reduction of complexity and increase of overall security effectiveness. To achieve this, enterprises (businesses) need to integrate their CSMA strategy across various cybersecurity tools/solutions/services portfolios.

Consequently, enterprises (businesses) can utilize this comprehensive portfolio of interconnected tools/solutions/services to solve their cybersecurity challenges across key components of CSMA. Refer to

Chapter 5, *Fundamental Components of Cybersecurity Mesh Architecture,* section, *The key components of CSMA* for details.

It is all the more important for enterprises (businesses) to break down vendor silos and standalone technology. This can be enabled and supported through a broad open ecosystem of technology partners, which allows flexibility in deployments. Also, such an ecosystem then consolidates security operations and visibility across. Not only does this setup lead to the implementation of an integrated and automated security experience, but it also preserves the existing tools/solutions investment.

Enterprises (businesses) can gain the following benefits of leveraging a CSMA today:

- Obtain visibility (in-depth) across its ecosystem.
- Manage and deploy solutions centrally (leading to consistent configurations and policies).
- Leverage cybersecurity intelligence (cross-domain) to obtain protection on a near real-time basis for cyberattacks.
- Automate actionable responses across the ecosystem.
- Data normalization and correlation.
- Employ advanced data normalization and correlation techniques to ensure consistency and accuracy in the information retrieved from different security tools. This process aligns disparate data formats, standardizes data representations, and identifies relationships between data points, enabling comprehensive analysis and contextual insights.

It is again vital to re-emphasize the importance of deployment of data normalization and correlation practices in the context of CSMA. These practices ensure consistent and accurate retrieval of information from various cybersecurity tools/solutions/services.

Target use cases

Refer to *Figure 7.2*, which lists some of the target use cases of leveraging CSMA:

Security operations
Vulnerability management
Compliance management

Figure 7.2: *Target use cases of leveraging CSMA*

Security operations

CSMA provides cybersecurity teams with an integrated (comprehensive) view of the security stack, thereby meaningfully enhancing security operations.

Also, this enables the cybersecurity teams to swiftly and conveniently obtain deep insights, recognize potential threats, and undertake proactive steps to mitigate risks.

Vulnerability management

There has been a multi-fold increase in phishing incidents over the years, and ransomware attacks occur every other hour. Current IT systems are, therefore, very vulnerable. Not only is it the existing vulnerabilities, but also there is the threat of a zero-day attack, an attack by a method previously unknown.

CSMA enables the identification and analysis of vulnerabilities across the security stack thereby lending support to vulnerability management.

It helps cybersecurity teams prioritize and address vulnerabilities basis their business impact (contextual) and associated risk levels.

CSMA approach also prepares an enterprise’s (businesses’) security infrastructure for zero-day attacks.

Compliance management

CSMA provides a centralized platform for compliance assessment across various cybersecurity tools/solutions/services thereby simplifying monitoring of compliance.

This eventually enables effective tracking of compliance status, identification of gaps, and streamlining the reporting process.

Features to be considered for CSMA solutions

CSMA vendors/players must provide a platform that gives security practitioners, executives, and security teams swift and easy access to contextual insights and responses across the security stack.

This is possible by building a comprehensive graph of APIs (covering cloud and on-premises security tools). The platform should enable users to navigate and understand the relationships between different data points effectively.

API Graph

It will be essential for a CSMA vendor/player to establish an interconnected (dynamic) graph of the APIs exposed by various security tools (covering cloud and on-premises-based solutions).

This holistic graph will provide a comprehensive view of the security stack and will assist in understanding how the data exposed by each tool relates to others.

Data normalization and correlation

A CSMA vendor/player will be required to employ advanced data normalization and correlation techniques. This will be required to make sure that the information retrieved from different security tools is consistent and accurate.

This will lead to an alignment of disparate data formats, standardization of data representations, and identification of relationships between data points. Eventually, this will lead to the enablement of a comprehensive analysis and contextual insights.

Natural language processing

A layer of **natural language processing** (**NLP)** should be integrated into the CSMA services. This will allow users to interact with the platform using natural language queries (thereby leveraging cutting-edge NLP algorithms).

The CSMA vendor/player should be in a position to understand the intent behind the queries and extract relevant information from the security stack, providing precise and contextual responses.

Generative AI for context enhancement

The CSMA vendor/player should consider utilizing generative AI algorithms to enhance contextual understanding and provide more accurate and insightful responses (through leverage of generative models, such as **language models** (**LMs**).

The vendor/player will thereby be able to generate free text responses that will go beyond simple keyword matching. This will enable users to gain a deeper understanding of the security stack and its implications.

Overall, a CSMA player/vendor should work towards a transformational platform by taking leverage of an API graph, data normalization, and correlation, and advanced NLP techniques, covering generative AI. Such a platform will empower security practitioners, executives, and security teams with contextual responses and insights.

Pitfalls of not leveraging CSMA

In this section, we will analyze the reasons for adopting CSMA, its key components, and the benefits of leveraging the same. Let us look at the other side of the coin and seek the pitfalls of not leveraging CSMA.

Refer to *Figure 7.3*, which lists the major pitfalls of not leveraging CSMA.

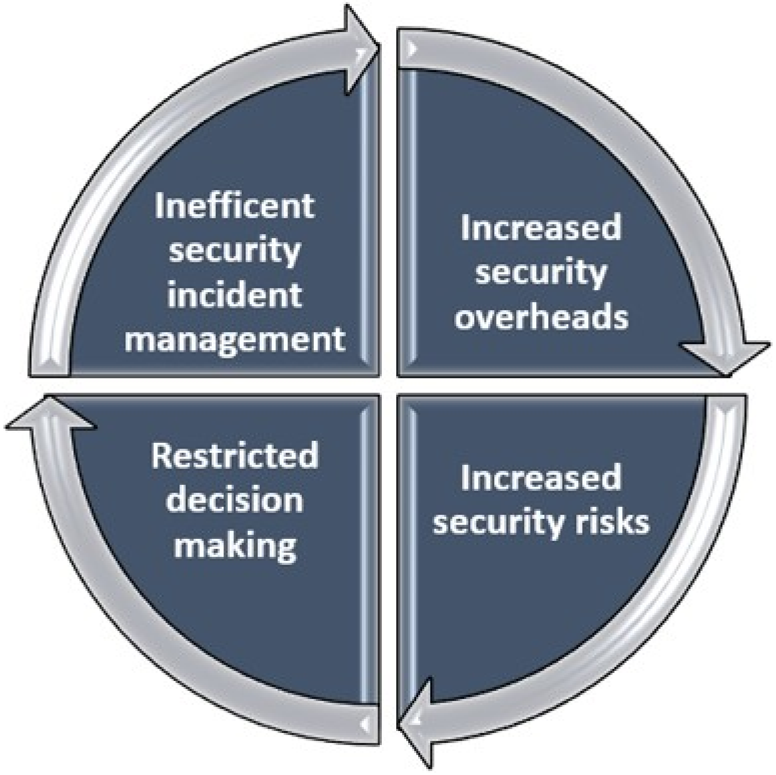

Inefficent security incident management
Increased security overheads
Restricted decision making
Increased security risks

Figure 7.3: *Pitfalls of not leveraging CSMA*

Increased security overheads

So far, we have realized that one of the biggest challenges for enterprises (businesses) is siloed data/expertise. When ecosystems do not have anything in place for aggregating each of these silos into a central repertoire (such as a data lake or SIEM), they require more staff to analyze cybersecurity events and threats.

In the absence of CSMA, cybersecurity teams oscillate between databases and consoles, use each tool’s query language (which is proprietary to the tool), and manually compile and analyze the data of each asset. All this is to obtain an understanding of its connections and validate security control implementation.

Cybersecurity teams, instead of involving themselves in value-added business risk reduction activities, spend most of their valuable time in simple auditing activities (which is a monotonous, tedious, and intricate process).

Let us consider the following real-life situation related to "increased security overheads":

- **Problem statement**: An enterprise (business) is required to retrieve data from two platforms: the vulnerability management console and the other is the asset inventory management system. Identification of gaps between inventories and assets that are not monitored requires data sets to be merged and then analyzed.

  Every other data point, such as the EDR agent, adds a data layer that is required to be retrieved and analyzed. Moreover, every asset that is not monitored will require a remediation ticket (creation and submission).

- **Challenges**: Simple activities such as this create a momentous challenge as and when the sheer volume of security control gaps surpasses the ability to remediate the gaps.

  In the absence of practical implementation of automation for identifying gaps in security controls, enterprises (businesses) will continue the practice of expanding headcount and reassigning their valuable analysts to low-value-adding manual activities.

- **Solution**
  - Prioritize analysis
  - If the activity is repetitive, automate it
    - Aggregate data sets contextually
    - Conduct predefined searches across data sets automatically
    - Manage security control gaps that are identified through appropriate triggers
- **Benefit**: Data being centralized and accessible leads to gaining intelligence about assets. This enables cybersecurity teams to reduce MTTR and MTTC of security incidents.

Increased security risk

Let us consider the following real-life situation related to *increased security risk*:

- **Problem statement**: As enterprises (businesses) expanded beyond the four walls of the office, cyber assets moved out of the perimeter to potentially become an ingress point (relatively easy to exploit) for a breach.

  Understanding the attack surface requires a repository (central) of all assets in the ecosystem, software running on those assets, vulnerabilities of each asset, and the way they communicate with each other. The absence of this makes the process of understanding the attack surface time time-consuming and often difficult to achieve.

- **Challenge**: Due to siloed network/security tools/platforms, the approach to risk becomes vacuumed. It is like missing the woods for the trees for network/security teams.

  In the absence of data convergence, a huge effort is required to manually correlate across huge data sets to be able to understand the attack surface. Moreover, any manual analysis is as good at a point in time and could quickly become irrelevant.

- **Solution**: Leverage CSMA to identify and automatically enable the mapping of the attack surface by converging identity, application, network, asset data, and security. This also leads to saving substantial effort by cybersecurity teams.
- **Benefit**: The availability of converged data leads cybersecurity teams to better understand each other's viewpoints on risk, such as unusual user behavior or network access related to exploitation.

Inefficient security incident management

Let us consider the following real-life situation related to *inefficient security incident management*:

- **Problem statement**: The availability of limited business context in decision-making, results in extended MTTR. There are risks of unexpected business disruptions when the implications of quarantine/service suspension are not well understood.

  > We often observe that inadequate awareness of business context often thwarts the ability of cybersecurity operation teams to respond due to fear of impacting the business.

- **Challenge**
  - Increase in dwell time of attacks
  - Increase in the probability of ransomware attacks, and
  - Increase in disruptions (unpredictable) across enterprise environments
- **Solution**: Leverage CSMA to automate security data aggregation and analysis and enable security intelligence (cross-domain) to provide an informed view of risks and threats.
- **Benefit**: Cybersecurity teams can reduce MTTR in situations where they can:
  - Identify the owner of a vulnerable server on an immediate basis
  - Identify the users of the server based on login activity
  - Identify the connections of the asset to other assets
  - Identify security events impacting the server

Incident responses can be adjusted and refined when dependencies (asset and application) are understood, minimizing business disruptions.

Restricted decision-making

Let us consider the following real-life situation related to *restricted decision-making*:

- **Problem statement**: Siloed ecosystems depend on data sets from their tools (individual and not integrated), thus decisions are arrived at without business context.

  Enterprises (businesses) have assets that run into hundreds of thousands with millions of vulnerabilities. In this situation, it is not possible to resolve all risks. To manage remediation, enterprises (businesses) either depend on vendor-provided risk scores or any other form of aggregated score.

- **Challenge**: Using risk scores that lack business (and network) context leads to ineffective risk prioritization and incorrect business impact. Without including context across the business and network, pursuing a non-contextually relevant risk score (lacking business/asset intelligence) results in ineffective risk prioritization, risk reduction, and uncertain business impact.

  The absence of business/network context has negative impacts on different teams:

  - Vulnerability management teams make incorrect decisions related to the priority of assets and patches
  - Security operations teams decide basis the context of the technology stack from SOC rather than the business
  - Networking teams decide based on routing and ambiguous IP addresses

- **Solution**: Leverage CSMA to enable domain intelligence (cross-domain). This aids the convergence of siloed knowledge and data leading to augmenting the cybersecurity team's decision-making ability.

- **Benefits**: A meshed ecosystem covering network and security services helps vulnerability management teams swiftly identify the vulnerable assets that are a part of crown jewels applications. This kind of analysis will otherwise require domain expertise across networking, vulnerability analysis, and penetration testing which is not easy.

By leveraging CSMA, the data aggregation, and analysis is automated leading to abstracting the result into a visual and interactive format that simplifies the complex.

The real benefit of adopting CSMA is to:

- Make security accessible to all
- Overcome Silos; and
- Enable well-informed vulnerability management decisions

Conclusion

CSMA works towards addressing the challenges presented by the distributed enterprise (business) and the continuously changing threat landscape/attack surface.

CSMA's adoption leads to deployment of security controls where they are needed the most, establishment of granular access controls, enhanced facilitation among security tools/solutions/services, increased visibility and control (centralized) across the ecosystem, increased agility due to reduction in deployment times and acceleration of digital transformation, increased resiliency by way of understanding interdependencies (context cross-domain) leading to better uptime and recovery, increased efficiency by allocating more experienced staff to higher-value activities and reduced risk by implementing business-centric risk reduction programs.

Overall, CSMA presents a robust framework that enables the strengthening of an enterprise (business) cybersecurity and protecting their valuable assets.

In the next chapter, we shall compare CSMA with traditional defense-in-depth approach, re-visit the salient points and goals for CSMA, present a list a systematic approach to implementing CSMA, list some of the key performance indicators) for assessing the effectiveness of the implementation of CSMA and introduce the ten commandments of CSMA.

Points to remember

- CSMA is a baseline foundation that enables disparate security tools/solutions/services to work in an integrated manner to create a dynamic security ecosystem.
- As enterprises (businesses) embrace digital technologies, CSMA lends a scalable and flexible base that enables bolt-on security for assets in hybrid and multi-cloud environments.
- Adoption of CSMA provides major benefits to enterprises (businesses). It leads to:
    - Reduction (significant) in the manual analysis of security data (freeing up cybersecurity teams for more value-added activities)
    - Consolidation of security analytics (predictive)
    - Consolidation of cybersecurity posture management
    - Enhanced security incident response
    - Effective business risk reduction

Key terms

- **Mean time to containment**: Average time it takes for an enterprise (business) to deal with a security breach or incident post-detection.
- **National Institute of Standards and Technology**: This is an agency of the US Department of Commerce, which has a mission to promote American innovation and industrial competitiveness. NIST has published a **cybersecurity framework** (**CSF**). This framework provides a set of guidelines for mitigating enterprise-wide (business-wide) cybersecurity risks.
- **Natural language processing**: An interdisciplinary subfield of computer science and artificial intelligence.
- **Dwell time**: Amount of time a cyber attacker has access to a compromised system before it is detected.
- **Return on investment**: Approximate measure of the profitability of an investment.

CHAPTER 8
CSMA Best Practices

Introduction

We have covered various topics in the first few chapters ranging from the chronology of the evolution of cybersecurity, understanding the distributed systems (working and challenges), cybersecurity challenges in the digital age, the emerging cybersecurity trends, and the importance of cyber resilience.

In the subsequent chapters, we took a first-hand view of the need for CSMA, and the benefits of its adoption, looked into the fundamental components of CSMA, and further discussed what enterprises (businesses) can expect when adopting the architecture and how they can effectively prepare for the future.

In the preceding chapter, we understood the need for CSMA, its benefits, and the pitfalls of not adopting it.

In this chapter, we will concentrate on the best practices that will help enterprises (businesses) to traverse the path to incorporating CSMA. It brings about an architectural and philosophical change that is an asset to enterprises (businesses) for all practical purposes.

Structure

In this chapter, we will cover the following topics:

- CSMA vs. defense-in-depth approach
- Salient points and goals for CSMA
- Systematic approach to implementing CSMA
- CSMA key performance indicators

- The ten commandments of CSMA
- Challenges in implementing CSMA

Objectives

In *chapters 5-7*, we learned that CSMA enables enterprises (businesses) with the strategy for proactive cyber risk mitigation. The cornerstones of this approach are aspects of interoperability and collaboration among cybersecurity teams and tools/solutions. This further nurtured an interconnected and context-aware cybersecurity ecosystem, which reduces business risk and enhances operational efficiency by disrupting traditional cybersecurity paradigms.

We will further discuss in detail how CSMA takes a vendor-agnostic approach and enables enterprises (businesses) to utilize the strengths of multiple vendors instead of living with the constraints of a single vendor's ecosystem.

This creates flexible (scalable) and adaptable enterprises (businesses). They can select the most appropriate security tools/solutions/products and technologies for their specific needs and stay ahead of emerging threats.

In this chapter, we shall revisit the goals of CSMA, seek a step-by-step approach to implementing it, and list the KPIs for assessing the effectiveness of the implementation.

CSMA vs. defense-in-depth approach

Over the years, enterprises (businesses) have relied on a defense-in-depth strategy for cybersecurity. Owing to this, they have implemented various security tools/solutions to address specific needs, leading to these enterprises (businesses) facing the challenge of security tool/solution sprawl.

Moreover, this approach has led to a complex and fragmented security infrastructure. Disjointed tools/solutions have become a scary proposition for enterprises (businesses) and resulted in an increase in operational costs and a decrease in efficiency. Management and integration of this situation require a sweeping transformation.

Overall, a cybersecurity mesh architecture:

- Advocates a security framework that is integrated and interconnected, thereby providing a solution to the challenge of security tool/solution sprawl.
- Promotes interoperability and collaboration among security tools/solutions.
- Does not rely on standalone/siloed security tools/solutions/services.
- Leads to reducing the complexity of managing disparate tools.
- Integrates disparate security tools/solutions into a unified ecosystem (by eliminating redundant/overlapping security tools/solutions).
- Leads to streamlining security operations (efficiency) and saving costs.
- Enables seamless communication and sharing of data among security tools/solutions, thus leveraging their collective intelligence.
- Facilitates a well-coordinated defense strategy that is rich in context.
- Leads to enhancing the overall effectiveness of the security infrastructure (by streamlining an approach to protecting digital assets).

Let us now examine (refer to *Table 8.1*) the major differences between CSMA and the traditional defense-in-depth approach:

Framework	**CSMA**	**Defense-in-depth**
Approach	Integrated Interconnected	Layered Multiple defenses
Focal point	Centered on identity	Centered on network/site
Communication	Seamless among key components (Refer to *Chapter 5*, section, *The key components of CSMA*)	Limited communication between layers
Topology	Centralized	Distributed
Contextual awareness	Strong context awareness due to continuous analysis and monitoring	Limited awareness of context

Scalability	Scalable	Complex and difficult to scale
Agility	Adaptable to emerging technology	Limited adaptability to emerging technology
Collaboration	Promotes collaboration and integration	Limited collaboration among vendors
Operations	Streamlined security operations due to consolidation	Tool/solution sprawl leading to inefficiency
Defense strategy	Proactive Enhanced business context leading to effective threat prevention, detection, and response	Reactive Siloed approach due to fragmentation

Table 8.1: *Comparison of CSMA vs. defense-in-depth approach*

Salient points and goals of CSMA

In *Chapter 5*, *Fundamental Components of Cybersecurity Mesh Architecture*, we discussed the key components of CSMA and the outcome of its adoption. In *Chapter 6*, *How to Effectively Adopt Cybersecurity Mesh Architecture*, we examined the importance of integration, comprehensiveness, and automation in CSMA and the key factors to consider for “its adoption. Furthermore, in *Chapter 7*, *Benefits of Adopting Cybersecurity Mesh Architecture,* we covered the characteristics of a CSMA strategy.

Figure 8.1 provides a view of the salient points and goals of CSMA:

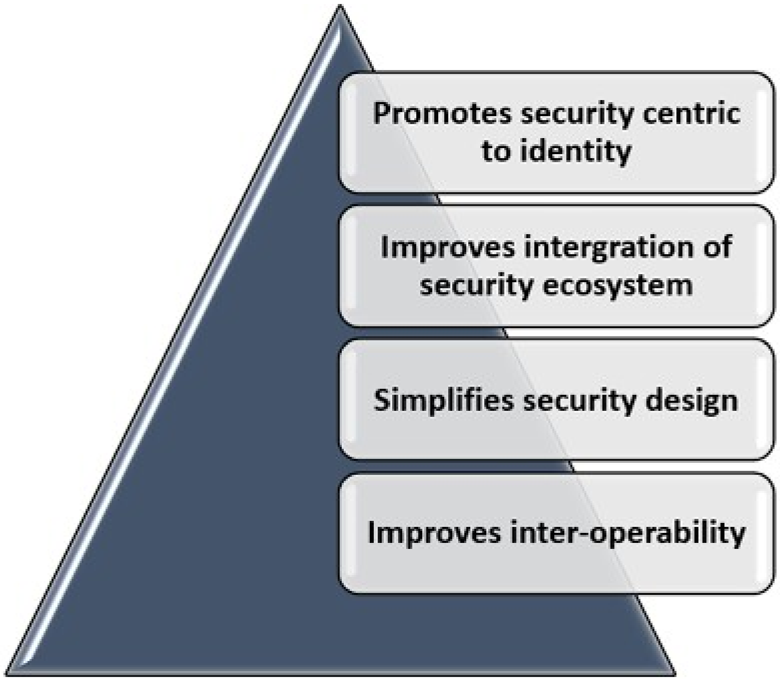

Promotes security centric to identity
Improves intergration of security ecosystem
Simplifies security design
Improves inter-operability

Figure 8.1: *Salient points and goals of CSMA*

In this section, let us re-examine the salient points and goals of CSMA:

- **Promotes security centered around identity**
  - Refer to *Chapter 5*, section *Does CSMA work with zero trust*, wherein we mentioned that zero trust is a security model that is centered around identity and has a strong focus on user authentication and authorization.
  - Salient point/goal of CSMA: Zero trust adoption is streamlined through ease of transition to identity-centric security.
- **Improves integration of security ecosystem**
  - Many enterprises (businesses) have a complex range of disparate, disconnected security tools/solutions.
  - Salient point/goal of CSMA: Bring about a reduction of complexity and improvement in performance by accelerating security integration and collaboration.

    Refer to *Chapters 6* and *7* for more details regarding collaboration and integration.

- **Improves interoperability**
    - Generally, enterprises (businesses) face challenges due to the absence of interoperability among standalone security tools/solutions from different vendors, which leads to gaps.
    - Salient point/goal of CSMA
        - Bridge these gaps through defining a framework for cooperation and collaboration.
        - Supports growth by using plug-in APIs to more easily support extensions, customization, analytics, and support for new regulations and standards.

    Refer to *Chapter 7*, section *Benefits of leveraging CSMA*, for more details regarding interoperability.
- **Simplifies security design**
    - Salient point/goal of CSMA: The key components enable enterprises (businesses) to plug in security tools/solutions as required to meet security requirements in a structured manner.

    Refer to *Chapter 5*, section, *The key components of CSMA*, and *Chapter 6*, section *Build the key components*, for more details.

    After considering the above, we should discuss a vital point: the approach to implementing CSMA should be vendor-agnostic. For details on this subject, refer to *Chapter 6*, section, *Build the key components*.

CSMA needs to be vendor-agnostic

Let us assess this subject through a real-life scenario detailed as follows:

- **Problem statement**:

    - In today’s cybersecurity field, enterprises (businesses) rely on multiple vendors for security tools/solutions.
    - A unique set of expertise and capabilities is offered by each vendor, and enterprises (businesses) generally select different products from different vendors to address their specific security requirements.
- **Challenge**:
    - Such an approach leads to challenges such as vendor lock-in and interoperability among security tools/solutions.
- **Solution**:
    - CSMA, by default, builds in a vendor-agnostic approach that aids in designing a resilient and scalable (flexible) security architecture.
    - Due to this approach, enterprises (businesses) can utilize the strengths of multiple vendors and avoid the limitations of the ecosystem of a single vendor.
- **Benefits**:
    - Enterprises (businesses) can choose the most befitting security tools/solutions/products basis specific needs instead of restricting themselves to a specific vendor’s offerings.
    - Vendor-agnostic approach supports and provides a fillip to integration and collaboration among vendors.
    - Enterprises (businesses) can utilize the expertise and collective intelligence of the cybersecurity ecosystem, due to security tools/solutions/products from different vendors that can seamlessly communicate and share information.
    - Collaboration leads to the enhancement of cyber defense capabilities and enables enterprises (businesses) to effectively respond to cyber threats.
    - Vendor-agnostic approach also provides adaptability and flexibility.

- enterprises (businesses) can incorporate new and emerging solutions and technology into their cybersecurity ecosystems, as they no longer are limited by a single vendor's roadmap.
- Overall, this approach enables enterprises (businesses) to steer ahead of evolving cyber threats by leveraging the latest innovations in cybersecurity.

Systematic approach to implementing CSMA

In continuation with Chapter 6, section *How to get started with CSMA*, let us re-visit the steps for systematically implementing CSMA. This will aid as a quick recap.

Figure 8.2 lists a step-by-step approach to implementing CSMA:

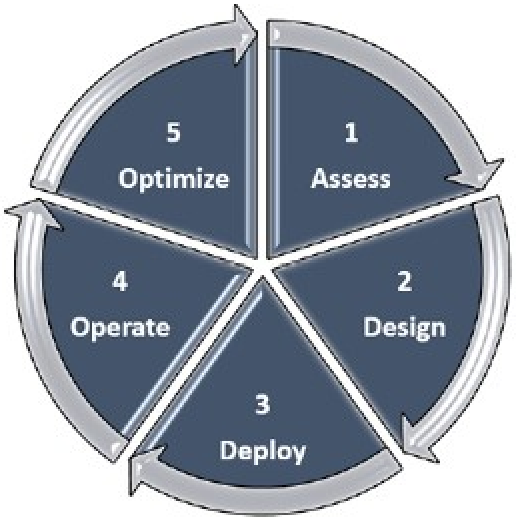


Figure 8.2: *Approach to implementing CSMA*

1. **Assess:**
    1. Assessing the present state and requirements of the enterprises' (businesses') technology environment and cybersecurity posture
    2. Identifying the gaps and **opportunities for improvement** (**OFI**)
    3. The key steps are:
        1. Conducting a security audit, risk assessment, and maturity assessment

2. Defining the security goals and objectives

2. **Design**:
   1. Designing the CSMA framework
   2. Selecting the cybersecurity tools/solutions and vendors to be included in the CSMA ecosystem
   3. The key steps are:
      1. Defining the cybersecurity requirements and specifications
      2. Evaluating and comparing the security tools/solutions and vendors
      3. Creating the cybersecurity roadmap

3. **Deploy**:
   1. Deploying and configuring the cybersecurity tools/solutions
   2. Integrating them with the CSMA key components (Refer to Chapter 5, section *The key components of CSMA* and Chapter 6, section *The key components of CSMA* for details)
   3. The key steps are:
      1. Testing the cybersecurity tools/solutions
      2. Establishing the security policies and rules
      3. Enabling the security data and communication channels

4. **Operate**:
   1. Operating and monitoring the cybersecurity tools/solutions and the CSMA ecosystem (ensure proper and effective functioning)
   2. The key steps are:
      1. Managing and maintaining the cybersecurity tools/solutions
      2. Collecting and analyzing the cybersecurity data
      3. Responding to security incidents and alerts

5. **Optimize**:

    1. Optimizing and improving the cybersecurity tools/solutions and the CSMA ecosystem (ensuring alignment and updation with the changing industry trends).
    2. The key steps are:
        1. Reviewing and evaluating the performance and outcomes
        2. Identifying and implementing the cybersecurity best practices and enhancements
        3. Planning and executing the cybersecurity changes and upgrades

CSMA standouts (in comparison to other architectures)

Refer to *Chapter 5*, section *CSMA's scalability relative to other architectures*, where this subject was first discussed. Let us summarize the ways CSMA is different from other security architectures:

- **Way 1**: **Composability**
    - Cybersecurity controls and functions are modular and can be deployed per the needs/preferences of each asset/user
    - Not constrained by a single vendor/platform
- **Way 2**: **Interoperability**
    - Cybersecurity tools/solutions can communicate and collaborate via key components such as data integration, comprehensive threat intelligence (and analytics), distributed identity fabric, automated and centralized operations, and consolidated dashboards (also consolidated policy, posture management, and modular security controls).
- **Way 3**: **Collaboration**
    - Cybersecurity tools/solutions can leverage and share the data and capabilities of each other

    - Provide a more consistent and comprehensive cybersecurity posture

Overall, CSMA:

- Enables the communication and coordination between the cybersecurity teams and stakeholders.
- Provides a common language/platform for cybersecurity management and governance.
- Well-suited for Enterprises (Businesses) that need to secure hybrid/multi-cloud/remote environments (also where resources/users are diverse and distributed).
- Enables a more flexible, scalable, resilient, and collaborative cybersecurity ecosystem.

CSMA key performance indicators

Enterprises (businesses) need to have KPIs that showcase how the CSMA is delivering the desired outcome. It is prudent to determine which KPIs are vital to be tracked and reported.

A high-level KP can be as follows:

- How is the CSMA strategy affecting the overall business outcomes?

Alternatively, KPIs can be technical/actionable and include (but are not limited to):

Figure 8.3 provides a comprehensive list of such CSMA KPIs:

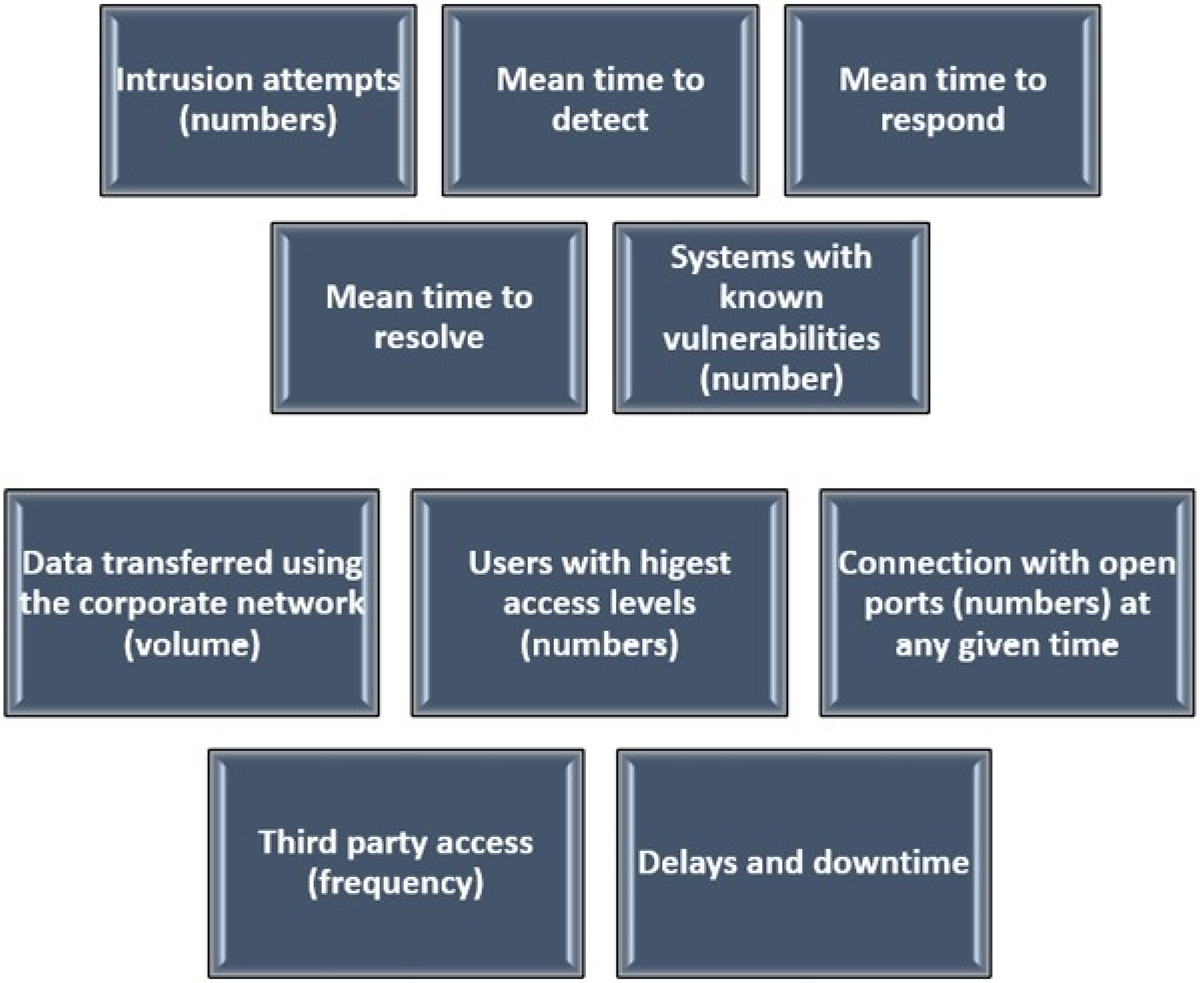

Intrusion attempts (numbers)
Mean time to detect
Mean time to respond
Mean time to resolve
Systems with known vulnerabilities (number)
Data transferred using the corporate network (volume)
Users with higest access levels (numbers)
Connection with open ports (numbers) at any given time
Third party access (frequency)
Delays and downtime

Figure 8.3: *CSMA KPIs illustrative list*

The above list is only indicative and should be considered as a starter. The KPIs chosen by an enterprise (business) to be tracked will depend on its environment (that is unique to that enterprise) and its CSMA ecosystem.

The ten commandments of CSMA

Cybersecurity mesh is an architectural and philosophical change that will be an asset to your business for many years to come.

Here are ten easily digestible bits of information that will help you get on the road to incorporating cybersecurity mesh.

Refer to *Figure 8.4* that lists the first five commandments of CSMA:

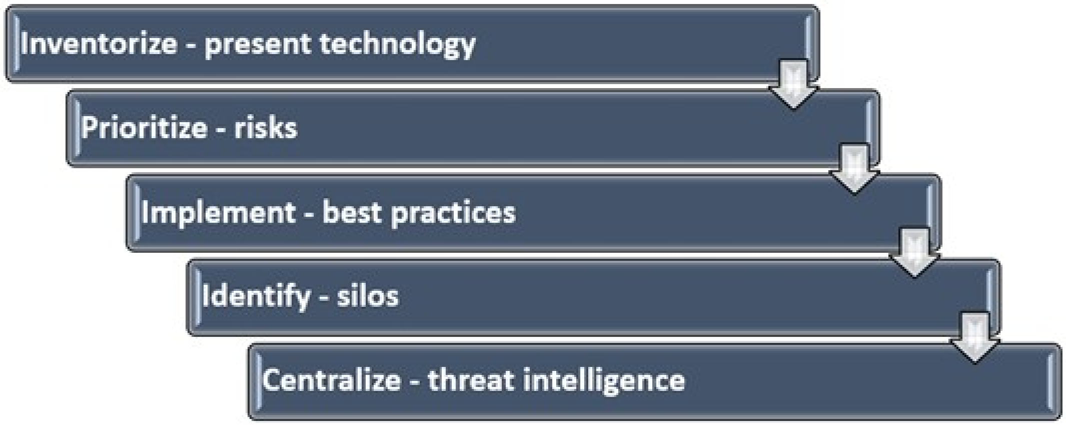

Inventorize - present technology
Prioritize - risks
Implement - best practices
Identify - silos
Centralize - threat intelligence

Figure 8.4: *CSMA 1-5 commandments*

- **Inventorize – present technology**
    - Understand how the present security system operates (aids in integration)
    - Identify weaknesses, inadequacy of tools, and possible points of failure
    - Prepare for the transition into a CSMA
- **Prioritize – risks**
    - Assess risks and potential vulnerabilities
    - Assess possible issues with the adoption of new technologies
    - Think like an attacker before implementing new security tools/solutions
    - Prioritize the identified vulnerabilities
    - Security operational teams should identify the most vital security weak areas that need to be addressed (this aids the direction for new technology adoption)
    - Consider enterprise-wide and managerial challenges that may be affecting security performance (this is beyond the technical challenges)
    - Assess security teams' structure
    - Ensure clear lines of communication between teams

- **Implement – best practices**
  - Best practices are a vital aspect of any cybersecurity ecosystem
  - Follow guidelines, viz., the principle of least privilege, and integrate any tool/solution that can be integrated (essential to fully secure resources)
  - Best practices are likely to change over time, hence it is important to keep reassessing the policies on a regular basis
- **Identify – silos**
  - Silos lead to locking meaningful data in separate containers thereby damaging the overall readiness of cybersecurity ecosystem
  - Due to unclear visibility and inadequate accessibility of the cybersecurity ecosystem, cybersecurity teams are unable to access/control their tools/solutions intelligently or set policies proactively
  - Key to breaking Silos is to move security controls closer to systems/assets they govern (this leads to decreasing detection and response times)
- **Centralize – threat intelligence (analytics)**
  - As discussed above, integrated (unified) cybersecurity systems not only lead to lowering detection and response times), but also lead to effective gathering of intelligence and analytics
  - Centralization of cybersecurity system information
    - Enables speeding up of security incident response plans
    - Leads to a deeper and contextual understanding of the cybersecurity landscape

Refer to *Figure 8.5*, that lists the next five commandments of CSMA:

Leverage - AI and ML
Automate - security stack
Identify - skill gaps
Partner - with ecosystem players
Improve continuously

***Figure 8.5**: CSMA 6-10 commandments*

- **Leverage – AI and ML**
  - Leverage recent developments in AI and ML for security-related applications
  - Vet AI and ML tool providers and ensure they provide holistic and effective tools/solutions/products
- **Automate – security stack**
  - Streamline cybersecurity operations through automation (integrated cybersecurity ecosystem). Automate as many tasks as possible such as device updates, tasks related to analysis (saves the crucial time of security staff to spend on evaluation tasks).
  - Automate threat response and threat analysis to generate swift security intelligence.
  - Define security policies and design playbooks.
- **Identify – skill gaps**
  - It is increasingly hard to find cybersecurity talent.
  - Different skills are required to manage modern cybersecurity tools/solutions such as for endpoints, edge devices, cloud assets and applications, and the skill gap is continuously widening.
  - Use of CSMA leads to simplification of cybersecurity processes. It also enables the narrowing of skill deficiencies by assigning new security tasks to more familiar zones.

    - External raining or outsourcing skills can be utilized to manage the more serious skill gaps.
- **Partner – with ecosystem players**
    - There is no Enterprise (Business) that has all the expertise required to maximize its cybersecurity posture.
    - It is vital to contact industry experts regarding security concerns, potential attack surface vulnerabilities, etc.
    - Leverage the know-how of the industry experts who are specialized professionals (better equipped than an average security team in an enterprise (business).
- **Improve continuously**
    - Every cyberattack presents an opportunity to:
        - Evaluate the current policies and playbooks
        - Identify areas of improvement for the cybersecurity systems
    - Keep pace with the latest industry practices to ensure that the threat readiness is at par with current potential cyber threats.
    - Conduct assessments of the security architecture on a regular basis.

Challenges in implementing CSMA

Enterprises (businesses) may face challenges while implementing CSMA.

The most common challenges are:

- Managing the transition from the existing security framework to CSMA
- Managing integration of disparate security tools/solutions into a unified ecosystem

Solution

- Carrying out a thorough assessment of the enterprises' (businesses') cybersecurity infrastructure
- Finding redundancies
- Prioritizing integration efforts
- Designing a roadmap
- Collaborating with vendors
- Carrying out holistic user awareness training and education to cybersecurity teams on CSMA, its key components, and benefits (including the best practices)

Conclusion

Enterprises (businesses) need to adopt CSMA and build a solid baseline for safeguarding their digital assets. This becomes increasingly important in an ever-changing cybersecurity threat landscape.

We have seen that the implementation of CSMA presents its challenges. These can be managed via thorough assessments, vendor collaboration, and comprehensive user training (education).

In the last chapter, we shall examine use cases in three distinct environments where CSMA works (viz., work from home, cloud, and **operational technology** (**OT**)) and have a sneak preview of the CSMA market overview, its growth factors, dynamics, and opportunities for growth.

Points to remember

- CSMA is a paradigm shift in cybersecurity and offers a holistic and integrated approach to protecting digital assets. Enterprises (businesses) that adopt CSMA can augment their cybersecurity posture. By establishing cybersecurity centered around identity, they can detect and respond effectively to security alerts/incidents.
- The key to benefiting from the full potential of CSMA is collaboration and integration (interoperability).

- The tips for an effective implementation of CSMA are as follows:
    - Carry out a present state security assessment
    - Understand existing strengths and weaknesses (part of SWOT analysis)
    - Adopt a collaborative culture among cybersecurity teams and vendors (enable seamless communication)
    - Prioritize the implementation of IAM solutions (identity-centric security)
    - Leverage AI and ML for:
        - Continuous monitoring
        - Proactive threat detection
- Choose tools/solutions that are vendor-agnostic thus providing flexibility (scalability) and integration
- Impart awareness training and education to cybersecurity teams on CSMA
- Carry out phased implementation
- Assess and improve cybersecurity posture on a continuous basis

Key terms

- **Key performance indicators**: A measure (quantifiable) of performance over time for a specific objective.
- **Opportunities for improvement**: In simple terms, it is an opportunity to improve your enterprise (business) system.

CHAPTER 9
Potential Outlook for CSMA Adoption

Introduction

In the previous chapters, we concentrated on the benefits of adopting CSMA and explored its best practices. We conducted research on many aspects of CSMA viz, its necessity, its target use cases, downsides of not leveraging CSMA, characteristics of a CSMA strategy, its salient points and goals, **key performance indicators** (**KPIs**), and eventually its ten commandments.

In this chapter, we shall examine some distinct use cases where CSMA works. We will take a specific example of the healthcare industry and examine how healthcare systems can leverage CSMA (potentially adopted). Lastly, we will understand another important aspect of the global market overview and dynamics of CSMA.

Structure

In this chapter, we will cover the following topics:

- Work-from-home environment
- Cloud security environment
- OT security environment
- CSMA in the healthcare system
- CSMA

Objectives

We have seen that CSMA is a holistic approach to safeguarding information assets and infrastructure. Consequently, CSA works in varied situations, and this chapter aims to examine different use cases, viz., work-from-home environments, cloud environments, and **operational technologies** (**OT**) environments. These environments present variations/distinct security challenges, and CSMA can address these by significantly contributing to maturing security in each of these scenarios.

Work-from-home environment

COVID-19 brought about a transformational change wherein employees started to work from home on devices that enterprises (businesses) had no/little control over. We say transformational for the reason that these enterprises (businesses) were pushed into a rare situation that required fundamentally new ways of working.

CSMA approach for security work-from-home environment entails:

- Deployment of **zero-trust network access** (**ZTNA**)
- Usage of **endpoint detection and response** (**EDR**), and
- Implementation of best practices for home network security

All of the above-mentioned key factors will be discussed subsequently.

Zero-trust network access

Problem statement

Remote workers have since ages been using **virtual private networks** (**VPN**) to access enterprise (business) networks. By using a VPN, enterprises (businesses) can limit access to their infrastructure and systems based on the user’s network connection. It was presumed that if a user is on a secure network, he/she can be granted access to the systems.

This reasoning will hold if there is strong physical security guarding access to buildings that house your systems and only people in those buildings have access to those systems. As soon as you allow a remote worker to access those systems, this security control does not hold anymore.

Logically networks can be extended to remote locations by using VPNs. Communications are encrypted (between endpoints and the central network). This is to thwart others on the network from understanding what is being communicated. Unfortunately, this level of security is no longer adequate.

Perceived risk

An employee (user) can always have a reason (legitimate) to use a VPN to access an enterprise (business) resource however the user may not have any reason to access many other resources. Consider a scenario where a laptop that was configured for remote access is lost/stolen. This scenario to the enterprise (business) could seem like a legitimate use case of the VPN whereas, in reality, the lost/stolen laptop (endpoint) is being used to steal confidential data from the network.

Solution

The need of the hour is for a better approach to address these scenarios. The approach is to follow a **zero-trust network access** (**ZTNA**) approach. In this approach, an enterprise (business) will not trust a user simply because they have access to a VPN. The fundamental difference in this revised approach is that not only the user but also the device must be authenticated.

With this approach, an attacker would not be able to gain access to enterprise (business) infrastructure just by gaining access to a VPN but would need to possess the device that was allowed access to the infrastructure (that will require authentication and authorization checks).

Endpoint detection and response

Problem statement

Devices used for remote work can be used from home, cafes, and flights, from anywhere where there is availability of wireless connection. A publicly accessible network can be used to connect to an office environment.

Perceived risk

With this kind of setup, cyber attackers can explore ways to use these networks to perpetrate attacks on other devices on the network. This can also be used to spoof users into connecting to a network that seems legitimate but is controlled by attackers.

Solution

CSMA ensures that all endpoints in the enterprise (business) are configured and monitored to detect and prevent attacks. It is vital to maintain endpoint protection in the wake of a fast and constantly changing threat landscape. A holistic endpoint detection and response services are important to block and remediate attacks (e.g., ransomware attacks) on the endpoints.

Home network security

Problem statement

It is quite reasonable to assume that a normal user of a home network may be running an insecure network. Moreover, home networks are typically secured using wireless routers that are shared among other users.

Perceived risk

Home wireless routers may be configured with weak administrator passwords or they may have older software with known vulnerabilities that could be exploited by an attacker.

Solution

CSMA can lend a helping hand to extend enterprise (business) security to networking devices in the home. This not only provides visibility into the state of home networks that are used for work but also control over the extended enterprise (business) network.

Cloud security environment

Enterprises (businesses) are swiftly adapting cloud computing services because they offer major advantages. New technologies such as cloud computing services are associated with new ways of doing things (aka developing and managing software) and also present distinct security challenges. To understand the specific security challenges of cloud computing, let us review some characteristics of cloud-native applications.

Problem statement

Characteristics of cloud-native applications

The deployment model or applications that run in the cloud are markedly different from applications that have traditionally been used in on-premise systems. In the case of on-premises applications, physical servers and **virtual machines** (**VMs**) are used widely, however, cloud platforms use containers for optimization. The distinct advantage of using containers is that it uses fewer resources as compared to VMs. Hence in the case of containers, a single server can run more applications effectively as compared to VMs.

Management challenges grow with the growing number of containers. The challenge lies in the deployment of containers such that servers can effectively be used, as well as in securing the containers. Containers are required to be monitored regularly as well to ensure they are running as per expectations. Upon failure of a container, an application or associated service will become unavailable until a replacement container is brought up.

These and other operational challenges encountered during large-scale deployment of containers are addressed by Kubernetes. Kubernetes is a platform for orchestrating the dynamic deployment of containers on a large-scale basis. This is useful when applications are being developed using architectures based on microservices.

In microservices, complex systems are disintegrated into small functional units/services that independently operate. Every microservice can be deployed in its container, allowing administrators to update and manage microservices without the fear of disruption of other services.

Perceived risk

Cloud computing has associated security and operational issues that need to be addressed. For example, the OWASP Top 10 list recognizes some important security issues for web applications that need to be managed.

Another aspect that makes things challenging is the concept of a multi-cloud environment. Many a time, enterprises (businesses) are required to deploy their applications across multiple clouds that may include hybrid cloud environments (here on-premises deployments aka a data center leveraged alongside cloud instances).

For enterprises (businesses) that are working towards achieving digital acceleration, this is great, however, it has the potential challenge for cybersecurity and cloud operations teams who are required to manage security across all cloud instances.

Solution

CSMA assists in simplification by enabling and leveraging an integrated (single point) view across all cloud instances thereby eliminating gaps related to visibility.

Additionally, CSMA assists in the implementation of predefined policies related to best practices. Policies diminish the chances of human error as they are defined consistently and monitored continuously through automated processes. CSMA also entails transparent, holistic logging and monitoring and is scalable based on demand.

OT security environment

Problem statement

At the core of OT is a collection of **industrial control systems** (**ICS**) which can be a combination of sensors/monitors/other technologies used in industrial settings. These are markedly different compared to a normal back-office application and exhibit specific characteristics. Especially OT generates large amounts of data continuously.

Perceived risk

Components in an ICS have implicit trust wherein if a component is accessible, it is assumed that it is a part of the same ICS. An ICS is explicitly required to be isolated from other systems. Now, if an ICS device is accessible over the Internet, it no longer has the security benefits of isolation.

Similar to the security challenges that are unique to remote work and cloud environments, OT environments also have a distinct set of challenges that need to be addressed.

Solution

CSMA assists with OT security best practices including asset identification and classification. Enterprises (businesses) should prioritize the value of different types of OT assets (some are likely to be more valuable as compared to others). The top priority is to know what is the most important and secure them. Equally vital is the ability to analyze traffic together with threats and vulnerabilities. We have seen earlier in use cases sections that even devices that are on-premises in remote work locations or the cloud have similar requirements. CSMA helps in the reduction of the overall risk to an enterprise (business) infrastructure and services significantly by reducing the number of tools required to achieve security optimally.

CSMA in the healthcare industry

The evolution of digitalization in the healthcare industry is all about advanced patient care amidst complications related to cyber threats. Healthcare enterprises (businesses):

- Function in an environment that is highly complex
- Rely on a wide spectrum of third-party service providers
- Depend on legacy infrastructure (outdated) and unpatched systems (that present cyber challenges)
- Need to look beyond zero trust and employ CSMA to manage cybersecurity issues

Usage and integration of connected devices in healthcare offer immense benefits related to patient care through improved diagnostics and streamlined operations is no less than transformative. The connected devices include smart medical devices, wearable health trackers, remote patient monitoring tools, etc, and deliver data and analytics on a real-time basis. All this enables healthcare providers to make informed decisions, thereby enhancing patient care.

The downsides of the swift adoption of such technologies entail exposure of the industry to cybersecurity risks. It is also important to note is the fact that the industry has traditionally lacked investment in cybersecurity infrastructure. Since the connected devices (as mentioned above) collect and transmit sensitive patient data, protecting this data from breaches is vital. Any unauthorized access can lead to identity theft/fraud or even put patients' lives in danger. Connected devices also, by default, lack robust security features that make them susceptible to cyberattacks.

Equally important are the regulatory challenges wherein healthcare enterprises (businesses) are obligated to follow stringent regulations such as the **Health Insurance Portability and Accountability Act** (**HIPAA**) in the US and the **Network and Information Security** (**NIS2**) Directive in Europe. Regulations stipulate severe penalties for non-compliance.

What makes these challenges even worse is the dependency on legacy (outdated) infrastructure. Many healthcare enterprises (businesses) have a reliance on archaic and unsupported operating systems and software that make them vulnerable to security vulnerabilities (since these systems are often unpatched and not updated promptly). Also, they are often not compatible with today's cybersecurity solutions which leads to complicated efforts in securing the infrastructure.

These challenges have no easy solution. Replacement of legacy infrastructure calls for major financial investment, and many healthcare enterprises (businesses) are restrained by budget constraints and rising costs. Furthermore, due to the interconnections among complex systems, standard cybersecurity solutions are not very effective.

Patient care is typically delivered from multiple locations with the involvement of multiple actors with every actor having the requirement to share patient data and operate in their own systems (separate and distinct). Thus, cybersecurity solutions need to be designed accordingly to meet the needs of the system.

This means a zero-trust architecture may not be suitable for healthcare systems since it is not designed to manage the complex nature of healthcare systems. For hospitals, the top priority and core competency is patient care and not technology systems. In case they need an **electronic health record** (**EHR**) for patients, they shall take the help of a third-party service provider. If that EHR requires APIs from a government department or some other data source, that source in itself will become a fourth party.

Consider these typical scenarios where a hospital is required to authenticate an IP that has not come from a third-party EHR provider but may have come from a fourth party. This becomes a source of breach at the hospital. The hospital neither has any direct relationship with the fourth party nor has any way to verify their security arrangements. They have no choice in this situation but to have the third party do the needful.

In this scenario, zero trust does not help. Applications utilizing zero trust will be unable to accept data from those legacy systems since these systems are not within the zero-trust perimeter.

This means that healthcare enterprises (businesses) need to implement CSMA that is distinctively suited to meet their demands. CSMA facilitates the extension of security controls across assets that are widely distributed. It is very flexible and suitable for modular approaches (viz., hybrid/multi-cloud architectures) wherein data is stored in multiple locations (on and off-premise).

CSMA provides control over multiple systems and solutions by bringing them together. It builds on the already made security investments by the enterprise (business) instead of asking for huge investments in new systems and infrastructure.

Concepts such as zero trust, secure by design, and defense in depth need not be discarded. Typically, the healthcare industry or other critical infrastructure environments have legacy systems in place and these setups rely on third and fourth-parties. Therefore, the emphasis and focus are on interoperability and collaboration. Zero trust and defense in depth can be an inhibitor to both.

In this increasingly interconnected world, the healthcare industry can lessen vulnerabilities, protect patient privacy, and defend the trust of stakeholders by implementing risk mitigation strategies and investing in innovative security frameworks on a priority basis.

Implementation of CSMA can boost the resilience of the healthcare industry against growing cyber threats. Enterprises (businesses) can form robust cybersecurity defense mechanisms by decentralization of security controls and emphasizing on identity-based access.

The need of the hour is CSMA that can adapt to the dynamic nature of modern healthcare ecosystems.

Summarizing CSMA in healthcare

The cybersecurity challenges in the healthcare industry are unique. This is due to a combination of factors. Firstly, the industry is a complex operating environment with multi-stakeholders. Secondly, the industry has a reasonable reliance on legacy infrastructure systems.

Solutions and concepts such as zero trust will not be suitable in isolation. The need of the hour is to embrace CSMA, which can accommodate existing cybersecurity solutions/systems and deliver robust security levels.

Also, CSMA can be a focal enabler for the widespread adoption of AI in the healthcare industry. CSMA essentially fosters a security-centric approach there by ensuring the integrity and confidentiality of sensitive patient data. It enables reinforcing trust among stakeholders while facilitating the seamless implementation of AI-driven solutions.

CSMA

The adoption of CSMA has gained positive traction, especially with the increase in remote work arrangements and the widespread use of cloud solutions. Enterprises (businesses) have been prompted to reassess data access and control policies due to the evolving landscape, which has led to the implementation of new technologies.

The increase in cyberattacks in recent years has further emphasized the need for comprehensive cybersecurity measures, leading to the growth of the cybersecurity mesh market.

Global market overview and growth factors

We have, over the course of all previous chapters, realized that CSMA enables modern-day cyber defense strategy that is different (rather transformational) from the traditional security practices, wherein there is often reliance on a single perimeter to protect an entire IT environment. CSMA protects each device independently, thereby aligning well with the distributed nature of remote work and cloud environments. In short, CSMA brings about a holistic approach to cybersecurity.

We have also noticed that the increase in remote work and extensive use of cloud computing (that distributes devices across varied locations) has led to a corresponding increase of momentum in the adoption of CSMA.

What has also prompted the enterprise (businesses) to reassess their data access and control policies is the ever-evolving threat landscape. Further, the emphasis on comprehensive and robust cybersecurity measures has been increasing with the increase in the frequency of cyberattacks. This is the main driver of the growth of CSMA (characterized by being more advanced and adaptive in nature).

Demand for CSMA has been growing substantially across industry verticals viz., banking and financial, technology, IT-enabled services, healthcare, energy, and utilities, amongst others. This growth is testimony to the industry's acknowledgment of the effectiveness and importance of CSMA in addressing modern-day cybersecurity challenges.

Market dynamics

Let us now seek some of the key drivers of the adoption of CSMA.

Driver: Management of evolving threat landscape

The growth in sophistication of cyberattacks, combined with the movement of workloads to hybrid cloud environments, is leading to an increase in demand for CSMA. Enterprises (businesses) are increasingly recognizing the need for a scalable and composable (modular) design to integrate security products/tools/solutions into a collaborative ecosystem. This is precisely what CSMA brings to the fore.

The cybersecurity landscape has been reshaped by the COVID-19 pandemic by pushing cyber assets outside traditional logical and physical security boundaries. As a response, enterprises (businesses) have turned to CSMA as a practical and effective solution.

CSMA enables enterprises (businesses) by establishing security parameters around devices and identities and providing a strong base for scalable and adaptable cybersecurity controls. CSMA presents a strategic and future-looking solution for enterprises (businesses) to maneuver the ever-evolving and complex cybersecurity landscape in the modern digital world.

Overall, CSMA enables disparate technologies to communicate through various key components, such as security intelligence, centralized policy management, and identity fabric. These advantages over traditional siloed cybersecurity strategies are anticipated to drive the market demand for CSMA in the coming years.

Threat: Shortage of skilled expertise

A major challenge for enterprises (businesses) in the implementation and adoption of CSMA is the shortage of skills. Demand for skilled (with specialized knowledge and skills) cybersecurity workers has been on a constant rise due to the increase in the complexity of the cybersecurity threat landscape (which leads to growth in the number of entry points for cyber threats).

Unfortunately, the industry is grappling with a paucity of trained cybersecurity professionals capable of understanding and responding to advanced cyberattacks. This shortage of trained security professionals exposes enterprises (businesses) to heightened risks of facing cyberattacks. Moreover, hiring and retention of a skilled cybersecurity professional is a bigger challenge.

The increase in sophistication of cyber threats (rise of new zero-day threats) undermines the importance of deployment of CSMA to detect and remediate attacks. However, inadequate end-user awareness regarding advanced cyber threats and a lack of spending on cybersecurity awareness training contribute to the industry's skill gap.

Enterprises (businesses) are required to build specialized teams to manage the complex threat landscape, and address the skills gap in the cybersecurity domain is a critical imperative.

After all, the adoption and implementation of CSMA requires a specialized and trained workforce that is skilled enough to effectively protect enterprises (businesses) against evolving cyber threats.

Opportunity: Growing adoption of multi-cloud

While leveraging services from multiple cloud providers, enterprises (businesses) have increasingly been adopting multi-cloud deployments. However, this setup presents challenges related to fragmentation due to the need to manage distributed IT assets across multiple clouds.

Management of a unified interface in a single-cloud environment is simpler than in a multi-cloud environment, which requires management of multiple interfaces. Understanding each component across various clouds in a multi-cloud environment adds complexity. Moreover, establishing a consistent security posture in a multi-cloud environment is difficult to achieve since all cloud providers have distinct security methodologies and support varying policies.

CSMA serves as the base for protecting all digital assets of enterprises (businesses) by securely connecting users and compute environments over hybrid/multi-cloud environments and across varied application generations/channels.

Another major challenge today is the inadequacy of the existing identity and security architectures to adapt to the evolving needs of enterprises (businesses). CSMA manages this challenge by provisioning a comprehensive and integrated security framework that can protect assets in on-premises, data center, and cloud environments.

CSMA facilitates collaboration among standalone security tools/products/solutions by standardizing the way these components communicate with each other which leads to the strengthening of the overall security posture.

Conclusion

Enterprises (businesses) need to adopt CSMA and build a solid baseline for safeguarding their digital assets. This becomes increasingly important in an ever-changing cybersecurity threat landscape. We have seen how the implementation of CSMA presents its challenges. These can be managed via thorough assessments, vendor collaboration, and comprehensive user training (education).

In summary, CSMA unveils the future of cybersecurity through a holistic and integrated approach, and enterprises (businesses) can strengthen their cybersecurity posture by adopting CSMA.

Points to remember

As we take on board a future dotted with pervasive connectivity and sophisticated cyber-attacks/threats, it is understood that approaches to cybersecurity that are traditional and siloed will not serve well. The shift towards CSMA is not just preferred, it is vital.

Toward the end of this chapter, let us summarize the practicalities of how enterprises (businesses) can adopt this innovative approach to cybersecurity:

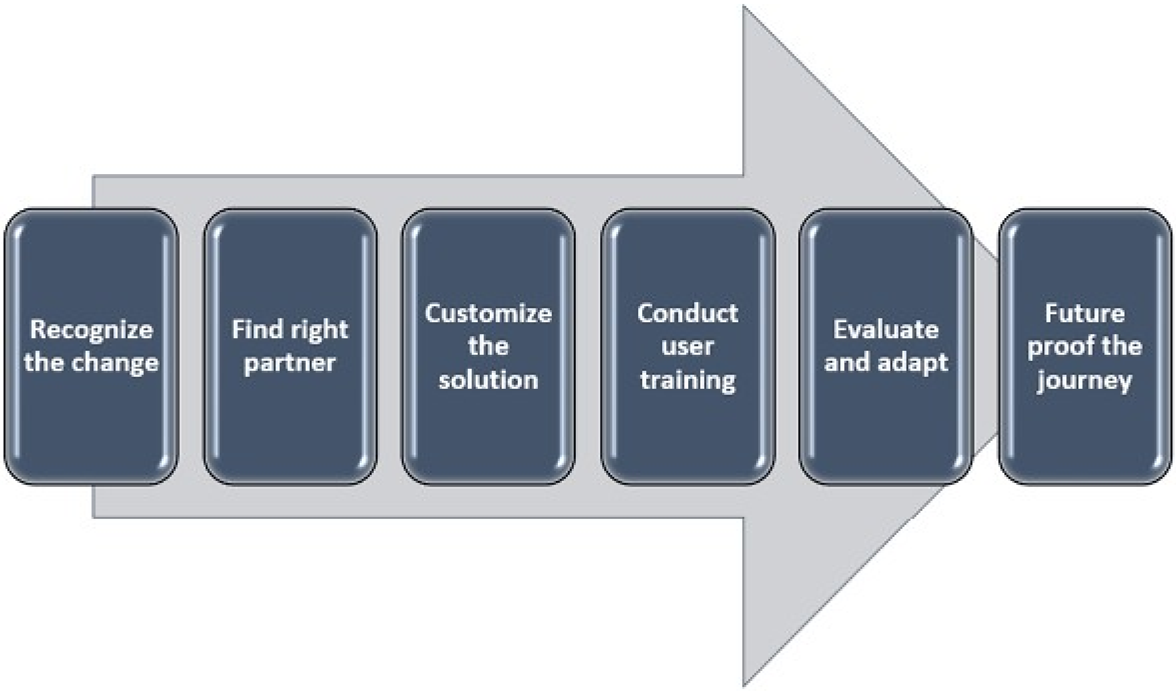


Figure 9.1: *Steps for adopting an innovative approach to cybersecurity*

- **Recognize the need for change:**
  - First vital step towards implementation
  - Acknowledge the constraints of current cybersecurity practices
  - Acknowledge the necessity for a more unified, scalable, and flexible approach
  - Work towards getting a holistic evaluation done for the existing security infrastructure and potential vulnerabilities
- **Partner with the right provider**: Choose a befitting partner (with recognized expertise and solid track record) such as a **managed security service provider** (**MSSP**) that can provide built-on CSMA
- **Customize the solution**:
  - Adopt and implement CSMA based on an enterprise's (businesses') specific needs
  - The following aspects will have a bearing on the final solution - the size of the enterprise (business), the nature of its operations, its regulatory environment, and the specific threats it faces

- **Prioritize user training and education**:
  - Comprehensive and robust cybersecurity solutions can be weakened by human error
  - The need to understand the importance of cybersecurity is crucial and needs to be emphasized through periodic user training and education
- **Regularly evaluate and adapt**:
  - The CSMA journey is not a one-time effort but an ongoing phenomenon.
  - It is vital to conduct evaluations regularly. This is to enable the assessment of the effectiveness of the existing security measures and to make adjustments if required.
  - The CSMA journey in an enterprise (business) needs to adjust to the emergence and evolution of new threats.
- **Future proof the journey**:
  - This is non-negotiable for any enterprise (business) – it is vital to choose a solution that evolves with the times (for example., swift technological advancement in AI, ML, etc. should be widely embraced
  - It is equally vital for the potential service provider to be committed to staying at the forefront of cybersecurity developments

The journey towards robust and unified cybersecurity may come across as complex, but the rewards are commensurate with the effort. By adopting CSMA, enterprises (businesses) can safeguard the present and make the way for a safe and secure digital future.

As we conclude this book, remember that cybersecurity is a continuing and endearing journey. A journey that necessitates constant vigilance, continuous learning, and an inclination to adapt and evolve.

Key terms

- **Key performance indicators**: A measure (quantifiable) of performance over time for a specific objective.
- **Operational technology**: The hardware and software that is used in industrial settings to monitor and control devices, processes, and infrastructure.
- **Virtual private network**: A mechanism for creating a secure connection between a computing device and a network, or between two networks, using the public Internet.
- **Virtual machines**: Is a physical computer's digital version. The digital version uses software (instead of a physical computer) to run programs and deploy applications.
- **Microservices**: An architectural approach to software development wherein software comprises small independent services that communicate over APIs.
- **The Open Worldwide Application Security Project**: An online community that provides free resources viz., articles, methodologies, documentation, tools, and technologies in the fields of IoT, system software, and web application security.
- **Industrial control systems**: An electronic control system and associated instrumentation used for industrial process control.
- **The Health Insurance Portability and Accountability Act**: A federal law (national standard) aimed at protecting sensitive patient health information from being disclosed without the patient's consent or knowledge.
- **NIS2**: EU-wide legislation on cybersecurity that provides legal measures to enhance the overall level of cybersecurity in the EU
- **Electronic health record**: Collection of patient health information in a digital (electronic format)

Multiple choice questions

1. **What is the main focus of CSMA?**

    1. Centralized security model

   2. Hybrid security model
   3. Decentralized security model
   4. Perimeter-based security model

2. **Which aspect of CSMA places emphasis on the authentication and authorization of individual users and devices?**
   1. Zero trust architecture
   2. Adaptive security
   3. Identity-centric security
   4. Distributed security services

3. **What security model does CSMA align with?**
   1. Trust-first model
   2. Decentralized model
   3. Centralized model
   4. Zero trust architecture

4. **What is the reason for CSMA prioritizing adaptive security measures?**
   1. Reduce the impact of potential breaches
   2. Lessen the need for continuous monitoring
   3. Centralize security controls
   4. Lessen the use of interconnect security fabrics

5. **Owing to what characteristics does CSMA facilitate comprehensive protection in the digital environment?**
   1. By isolating security elements
   2. By centralizing security measures
   3. Through interconnected security fabrics

4. Through security controls

6. **CSMA's scalability leads to what advantage?**

    1. Reduced security measures
    2. Organizational growth due to seamless adaptability
    3. Centralized security controls
    4. Limited protection of endpoints

7. **Through which of the following attributes can CSMA lead to an enhanced security posture?**

    1. By relying on a centralized ecosystem
    2. Through a distributed approach thereby reducing single points of failure
    3. By ignoring zero trust architecture
    4. By lessening the need for adaptability

8. **How does CSMA manage the ever-changing cyber threat landscape?**

    1. Through the adoption of static security measures
    2. Through the adoption of dynamic and adaptive features
    3. By way of relying on traditional network perimeters
    4. Due to inadequate continuous monitoring mechanisms

9. **Which of the following is the biggest reason for the success of CSMA implementation?**

    1. Overlooking industry challenges
    2. Getting complacent in risk assessment
    3. Carrying out a holistic risk assessment
    4. Lack of collaboration with vendors

10. **Which vital ingredient can assist in overcoming challenges in CSMA implementation?**

    1. Lack of user awareness and training
    2. Competition amongst vendors
    3. Governance (collaborative) involving key stakeholders
    4. Reliance on a single security measure

Answer key

1. **Decentralized security model**: CSMA moves away from outdated security models that are centralized, and distributes security controls across the digital ecosystem, thereby making a provision for a decentralized and adaptive defense ecosystem.
2. **Identity-centric security**: CSMA does not only rely on traditional network perimeters but also emphasizes authentication and authorization of individual users and devices thereby enhancing visibility and control.
3. **Zero trust architecture**: CSMA has a zero-trust security model at its core. This requires continuous verification (for every user/device/application).
4. **Reduce the impact of potential breaches**: CSMA uses adaptive security that facilitates the adjustment of security controls on a real-time basis. This leads to a reduction in the impact of potential security breaches.
5. **Through interconnected security fabrics**: CSMA propagates that interconnected security fabrics be created. This facilitates collaboration and provides holistic protection across the entire digital ecosystem.
6. **Organizational growth due to seamless adaptability**: A key component of CSMA is scalability. This facilitates seamless adaptability to the expansion of digital ecosystems.

This further ensures that security measures do not hinder organizational growth.

7. **Through a distributed approach thereby reducing single points of failure**:

   CSMA facilitates the dispersion of security controls. This leads to the minimization of the risk of a single point of failure and enhances overall security posture.

8. **Through the adoption of dynamic and adaptive features**: The basic nature of CSMA is its ability to dynamically adapt which enables it to respond in a real-time basis to emerging threats in this ever-evolving cyber threat landscape.

9. **Carrying out a holistic risk assessment**: A comprehensive risk assessment is vital for the identification of vulnerabilities and prioritizing security measures during the adoption of CSMA.

10. **Governance (collaborative) involving key stakeholders**: The involvement of key stakeholders (IT, security, and business units) in governance (collaborative) enables the comprehensive implementation of CSMA.

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

Index