Practical Cyber

Practical Cybersecurity Decisions

Two New Chapters - Cyber Security Incident Reporting in Malaysia and Post Quantum Cryptography

Featuring:
Ir. Dr. Megat Zuhairy Bin Megat Tajuddin
Prof Dr. Muhammad Rezal Bin Kamel Ariffin
Professor (Dr) Shaikh Harun Bin Mustafa

MALAYSIA EDITION

ETHAN SEOW

NACSA
AGENSI KESELAMATAN SIBER NEGARA
NATIONAL CYBER SECURITY AGENCY

PTPKM
PUSAT TEKNOLOGI DAN PENGURUSAN
KRIPTOLOGI MALAYSIA

Practical Cybersecurity Decisions: Malaysia Edition

This book was written and published by **Practical Cyber,** a brand of **Verixiom Pte Ltd,** as part of the **Cyber Intel Group,** which includes **Cyber Intel Training** and **First Experts Sdn Bhd.**

Partner organisation: **Centre for AI Leadership (C4AIL)**

Licensing

- **Ebook & Print Book:**
  This edition is for **personal use only.** No part of this book may be copied, redistributed, or reproduced in any form without written permission, except as permitted under **Creative Commons Attribution 4.0 International License (CC BY 4.0)** for excerpts and non-commercial use.

- **Framework (Open Source):**
  The framework discussed in this book is licensed under the **MIT License** and can be freely accessed on https://github.com/practicalcyber/practical-cybersecurity-decisions?tab=readme-ov-file

To obtain the open-source framework, visit:
https://github.com/practicalcyber/practical-cybersecurity-decisions

To purchase a copy of this book, visit:
https://practical-cyber.com/framework

ISBN: 978-969-8592-10-3

Contents:

About the Lead Author and Featured Co-Authors

(Malaysian Edition)

Ethan Seow

Ethan Seow is ISACA Singapore's 2023 Infosec Leader, ISC2 2023 APAC Rising Star Professional in Cybersecurity, TEDx and Black Hat Asia speaker, educator culture hacker and entrepreneur with over 11 years in entrepreneurship, training and education.

He is the CEO of Practical Cyber and Cyber Intel Training, two arms of cybersecurity education designed for holistic cybersecurity education. Practical Cyber focuses on educating non-IT and business personnel in organisations in cybersecurity, simplifying and making cybersecurity relevant and actionable at every level. Meanwhile, Cyber Intel Training specialises in technical cybersecurity training across different experience levels, focusing on real-world simulations and engaging pedagogy. He is also the Director of Technology for First Experts Sdn Bhd, the sister company of Cyber Intel Training and Practical Cyber based in Malaysia.

He is also a head crew of Divison Zero (Div0), Singapore's largest cybersecurity community, and SINCON, Singapore's top local technical conference with attendees across different public and private sector top brass.

Additionally, he spent several years with ST Electronics, integrating and securing large-scale military systems.

Ir. Dr. Megat Zuhairy Bin Megat Tajuddin

Ir. Dr. Megat Zuhairy Bin Megat Tajuddin is a distinguished technology leader with over 25 years of experience, currently serving as the Chief Executive of the National Cyber Security Agency (NACSA), Malaysia.

Grounded in his background as a Professional Engineer, his career has been dedicated to developing and securing Malaysia's critical Information and Communications Technology (ICT) infrastructure. Prior to leading NACSA, he was the Director of Engineering at the Public Works Department (PWD), where he was instrumental in developing policy and strategic plans for the nation's Industrial Revolution 4.0 (IR4.0) agenda.

His vast experience includes supervising major national ICT projects for hospitals, airports, and government offices. Dr. Megat holds a Doctor of Business Administration in the field of Technology and Innovation Management from Universiti Teknologi MARA, Malaysia, a Master of Science in Communications Technology from Ulm University, Germany, and a Bachelor of Science in Electrical and Computer Engineering from Johns Hopkins University, USA.

Professor Dr. Muhammad Rezal Bin Kamel Ariffin

Professor Dr. Muhammad Rezal Bin Kamel Ariffin is a leading expert in mathematical cryptography and a pioneer of Post-Quantum Cryptography (PQC) in Malaysia. He is the Director for the Malaysia Cryptology Technology and Management Centre and a Professor at the Department of Mathematics and Statistics, Faculty of Science, Universiti Putra Malaysia (UPM). As a founder and the current President of the Malaysian Society for Cryptology Research (MSCR), his work is dedicated to developing and analysing the next generation of cryptographic algorithms.

His research focuses on designing and analysing practical PQC systems, with the goal of creating seamless "drop-in" replacements for the non-quantum resistant algorithms in use today. Professor Dr. Muhammad Rezal Bin Kamel Ariffin has played a key role in shaping Malaysia's national cryptography policies, including the MySEAL initiative, and has represented Malaysian innovation at international forums such as the NIST PQC Standardization Conference. He has published over 150 scientific documents and supervised numerous PhD and MSc students in the field of Mathematical Cryptography.

Professor (Dr) Shaikh Harun Bin Mustafa

Professor (Dr) Shaikh Harun Bin Mustafa brings over three decades of strategic leadership across the legal, technology and business development landscapes.

A Barrister by training, he holds a Bachelor of Law from the University of Leeds, which led to the establishment of his own legal practice, Shaikh Harun & Co. During his time in practice, his interest in digital assurance and identity security began to take shape – ultimately prompting his transition into the technology sector. He went on to hold senior executive roles at Datasonic Group Berhad, where he led innovations in biometrics and drove international business expansion.

He currently serves as Director of Business Development at Valet Technology Sdn Bhd, specialising in cybersecurity, identity management and telecommunications security. In recognition of his contributions to entrepreneurship, he was awarded an honorary Professorship and Doctorate by the Netherlands Maritime University College.

Beyond his professional achievements, he is active in the regional economic circles. His broader commitment to industry and community is reflected in his roles as Chairman of the Regional Bilateral Trade and Investment Association, Committee Member of the Education Bureau under the Malaysia China Business Council and former Advisor to the SME Association of Malaysia.

Introduction to the Malaysia Edition

When we first created Practical Cybersecurity Decisions, our mission was simple: to demystify cybersecurity for business leaders. We wanted to bridge the gap between technical practitioners and the boardroom, transforming cybersecurity from a source of fear into a practical, business-aligned function designed to protect profits and foster resilience. The Practical Cyber Framework was born from this idea—an open-source tool to empower any leader to make better, more informed decisions.

For any framework to be truly practical, however, it must be applied within a real-world context. The legal landscape, national strategies, and emerging technological innovations of a country shape the specific challenges and opportunities its business leaders face. It is with immense pride and a deep sense of purpose that we have collaborated with key national institutions to create this special Practical Cybersecurity Decisions: Malaysia Edition.

This book represents a landmark public-private partnership. We are honored to have worked closely with the National Cyber Security Agency (NACSA) and the Malaysia Cryptology Technology and Management Centre to enrich this guide with unparalleled local expertise and strategic foresight.

This edition has been made possible by an incredible team. I extend my deepest gratitude to Ir. Dr. Megat Zuhairy Bin Megat Tajuddin, the Chief Executive of NACSA, for graciously providing the Foreword and for the close collaboration from him and the NACSA legal team, whose consultation was essential in ensuring the accuracy of our new chapter on the Cyber Security Act 2024.

I am equally indebted to Professor (Dr) Shaikh Harun b Mustafa, who led the writing of this critical chapter, lending his immense legal and technical expertise to the project.

And I am incredibly grateful to Professor Dr. Muhammad Rezal Bin Kamel Ariffin for authoring our visionary chapter on the post-quantum era.

The book you hold in your hands is a testament to what we can achieve together. It is a guide that is not only practical in principle but also directly applicable to the Malaysian business landscape.

It is therefore with great honour that I present the Foreword for this special Malaysia Edition, written by Ir. Dr. Megat Zuhairy Bin Megat Tajuddin, who will officially set the stage for the journey ahead.

Foreword

By IR. DR. MEGAT ZUHAIRY BIN MEGAT TAJUDDIN
Chief Executive
National Cyber Security Agency (NACSA), Malaysia

In an era defined by digital transformation, the security and resilience of our nation are no longer merely technical concerns; they are strategic imperatives that underpin Malaysia's economic stability and sovereign integrity. To navigate this complex landscape, we require a unified whole-of-government, whole-of-nation, and internationally coordinated approach, built on strong public-private partnerships. This is the foundation upon which we will build a secure and prosperous digital future.

A key objective of this national strategy is to strengthen the partnership between the government, businesses, and the community. It is this goal that drew my attention to the work of Ethan Seow of Practical Cyber. His book, Practical Cybersecurity Decisions, successfully bridges the long-standing gap between business leaders and technical experts. Furthermore, the decision to make the accompanying Practical Cyber Framework open-source is a significant factor in this collaboration. It ensures that practical, vital knowledge is made accessible to everyone, which is fundamental to empowering our entire ecosystem.

While the Cyber Security Act 2024 places specific duties on our National Critical Information Infrastructure (NCII) entities, the principles of cyber resilience are universal. This book is therefore suitable for all leaders, including those from Small and Medium Enterprises (SMEs) and non-NCII organisations. A cyberattack on any business can disrupt our national supply chain and erode community trust. By embracing the practical guidance in this book, every business leader can protect their own profits and sustainability, and in doing so, contribute to the strength and security of the broader community.

To that end, this edition has been enhanced with two crucial chapters. I am pleased to see that it now includes a dedicated chapter on incident reporting, which provides clear and actionable guidance on the new national policies under the Cyber Security Act 2024. It is designed to help leaders understand and fulfil their duties with confidence.

This is complemented by a forward-looking chapter on Post-Quantum Cryptography (PQC) by Professor Rezal, which not only prepares leaders for future threats but also showcases Malaysian innovation in cryptology.

This initiative is a deliberate step in our mission to empower leaders across the entire business landscape. The knowledge contained within these pages directly supports the pillars of our forthcoming Malaysia Cyber Security Strategy (MCSS) 2025-2030, a key part of our ongoing national effort to build capacity from the ground up.

This is a journey of continuous improvement, and we are committed to seeing it through. Together, we can build a secure and resilient digital Malaysia.

Prologue by Emil Tan

In today's digital era, businesses are presented with extraordinary opportunities to scale and innovate through technology. However, with these opportunities come complex cybersecurity challenges that many organisations struggle to address effectively. Rather than confidently integrating cybersecurity into their business strategies, many leaders approach it with uncertainty and hesitation. This lack of clarity often results in cybersecurity being treated as a mere compliance exercise – something to be delegated to IT teams and forgotten once lacklustre security software are in place. The reality, however, is that cybersecurity requires a more thoughtful and proactive approach that aligns with business objectives and operational needs.

In fact, reality is far more complex. Cybersecurity is not just about technology; it is an integral part of modern business strategy. As our businesses become increasingly reliant on technology to operate, cybersecurity risk is ranked one of the top risks to businesses. As a result, it influences how businesses operate, how they build trust with customers, and how they sustain long-term success in an increasingly interconnected world. Cyber risks are not meant to be isolated to IT departments; they affect every aspect of an organisation – from supply chain logistics to customer data management, from regulatory compliance to brand reputation.

Practical Cybersecurity Decisions: The Practical Cyber Way of Securing Your Profit therefore serves as a valuable guide for business leaders and cybersecurity professionals alike. It does not merely provide a set of technical recommendations; instead, it offers a strategic framework that aligns cybersecurity with business objectives. It emphasises that cybersecurity should not be seen as a cost centre, but rather as a key enabler of trust, resilience, and competitive advantage.

My journey in cybersecurity has been deeply personal and professionally fulfilling. I have had the opportunity to work alongside governments and critical infrastructure organisations, helping them defend against evolving threats and future-proof their operations. My primary focus has been on transforming cybersecurity strategies – aligning concepts of operations (ConOps) and security operations (SecOps) with broader national security and organisational objectives. Cybersecurity is not just about addressing today's challenges; it's about anticipating the future by exploring emerging technologies, digital trends, and evolving business landscapes to better prepare organisations for what lies ahead.

Through these experiences, I have come to understand that cybersecurity is more than just protecting data – it is about ensuring resilience, safeguarding public trust, and enabling organisations to thrive despite adversity. From refining and rethinking operational frameworks, my approach has always been to foster a culture where cybersecurity becomes an intrinsic part of business operations rather than an afterthought.

Cybersecurity isn't just about defending against the high-profile, headline-grabbing nation-state attacks. Often, the real threats lie in the day-to-day vulnerabilities – misconfigurations, lack of staff awareness, and poorly managed digital footprints. Attackers are opportunistic; they, too, seek high returns on investment (ROI), targeting not just the "big players" but also Small to Medium Enterprises (SMEs) and supply chain partners that can serve as stepping stones to larger targets. This book provides a crucial perspective on why businesses, regardless of size, must take ownership of their cybersecurity posture and embed security into their core operations.

Ethan Seow and his team have taken on the challenging task of distilling the vast and often overwhelming world of cybersecurity into practical insights that resonate with business leaders. They emphasise that cybersecurity is not about chasing the latest technologies but about making informed decisions that balance risk, cost, and business objectives. Practical Cybersecurity Decisions invites readers to think beyond the myths, beyond the fear-driven spending, and towards a pragmatic, business-aligned approach to security.

This book is not a one-time read; it is a guide that business leaders and security professionals should revisit regularly. Whether you're making your first cybersecurity investment or refining an existing strategy, this book serves as a roadmap for making better, more informed decisions. The Practical Cyber Framework within these pages provides actionable steps to help you understand what to protect, why it matters, and how to align security with your business goals.

Ultimately, cybersecurity is no longer just the domain of IT departments – it is a business imperative. As digital threats continue to evolve, so too must our approach to security. By reading this book, you are taking an important step towards building a more resilient and trustworthy business in the digital age.

Let this book serve not just as a resource, but as an invitation to engage, learn, and take ownership of your cybersecurity future.

CHAPTER

01

Why? And How?

Why We Wrote the Book

The advent of the transistor and the subsequent technological transformation, in the form of computers, networks and smartphones, has brought unparalleled opportunities for businesses but also unprecedented risks.

For business owners, operators, and managers, understanding cybersecurity isn't just a technical requirement—it's a necessity for sustaining operations and protecting profits.

At the same time, cybersecurity practitioners need a business-oriented language to communicate risks and strategies effectively within their organisations.

Majority of the time, the buying of security solutions, related services, or advisory are due to fear, pressure, compliance, and liabilities. Often, we buy the latest technologies due to a "fear of missing out" be it cloud, AI, blockchain, unique methodology or unique positioning – even when we do not truly understand the impact.

This leads to stakeholders continuously adding to the technological silos or buying packages of solutions that result in common misconceptions about cybersecurity in the eyes of business stakeholders:

- **Cybersecurity is expensive:** Only if you spend a lot of money can you get enough security to fend off attackers, which isn't true once you understand how it can work in your favour.

- **The risk and impact of a cyber-attack are low:** Even though >70% of organisations have reported that they experienced a cyber-attack, many organisations still believe they will not be the target. This often leads to the majority of organisations being hit with cyber-attacks being woefully unprepared, costing them more than they would ever imagine.

- **Cybersecurity is hard to understand:** One of the biggest problems facing cybersecurity is that unlike many other topics that have been around for many years, Information Technology (IT) and cybersecurity have only been around for decades and seem hard to understand. It is not, we just have to take it step by step and simplify it for you.

Therefore, **Practical Cyber,** as a brand, was born from the urgent need to address this communication gap. This book is designed to empower two key audiences:

- **Business Leaders:** To grasp and navigate their organisation's cybersecurity needs, integrating it seamlessly into their business continuity and risk management plans while managing costs. This would enable them to understand their duty as a board member, director, leader, or manager, and remove the fear of it.

- **Cybersecurity Professionals:** To articulate risks and solutions in a manner that aligns with business priorities and goals.

Therefore, this book, **Practical Cybersecurity Decisions**, is designed to demystify cybersecurity, presenting it not as an isolated technological concern but as an integral component of business processes.

We do so by starting with the business concerns, not cybersecurity concerns. This manual and the accompanying **Practical Cyber Framework** are designed to make cybersecurity accessible, actionable, and essential to protecting the core assets and operations of your business.

This book is designed to help you make any considerations about buying any solutions or services, and to empower you to make a more considerate decision.

This is only the first of many potential books that we will be writing – it is the gateway to making cybersecurity practical for business owners and operators. We start this book as an overview, and deep dive into each area of interest in the future editions, whether it is **Practical Cyber for AI, Practical Cyber for Manufacturing,** or any other interesting topics that people want to contribute to and want to create with us.

Whether you are a subject matter expert or a business leader, we would love to engage with you. Feel free to reach out to us at book@practical-cyber.com for more information.

Why Does Cybersecurity Matter?

Every business, regardless of size, exists to achieve sustainability and profit. These goals are constantly under threat from various factors—economic downturns, regulatory shifts, or unforeseen events like pandemics. Cybersecurity risks, including data breaches, ransomware, and corporate espionage, are increasingly becoming part of this equation.

In the crowded business world today, trust is increasingly a needed commodity to gain our customers. From the perspective of a customer: think of the website where we buy our daily essentials online. Extend that to food delivery, taxi services and online apparel shopping where our digital identity, credit card and various payment method details are saved. These websites and the organisations behind them store all the history of what you do, when you do and how you pay and work on their sites.

Now, if any of these services encounter a breach and discover that they have not been the most diligent with the data you trusted them with – would you still trust them and continue the next day to run your daily needs? Likely not. There are plenty of options for you to switch to their competitors.

Now, take the perspective of an organisation fighting to gain new customers and retain its existing pool – what happens if you don't set up effective defences and your operations come to a halt due to a ransomware and this information got released to the public? Would your customers stay? Would you be able to win the trust of your future customers?

That is where trust and security have a direct relationship to business growth. Securing your profits and revenue includes building trust, which will bring more customers and increase your organisation's market share.

In this modern world, where only the fittest businesses survive, with the frequency of cybersecurity breaches, it is an edge for your business to have proven handling of cybersecurity incidences well, to win the trust of your customers.

Just to give more perspective through the statistics:

- 61% of Small to Medium Enterprises (SMEs) were victims of a cyberattack in 2023 (Blackfog, 2024)

- 72.7% of surveyed businesses worldwide were affected by ransomware (Statista, 2024)

- The average cost of ransomware has increased to $1.54 million (Sophos, 2023)

- Only 4% of organisations are confident their assurance of security to "users of connected devices and related technologies are protected against cyberattacks." (World Economic Forum's State of the Connected World, 2023)

- Cybercrime economy is expected to reach $10.5 trillion by 2025 (Cybersecurity Ventures)

- At a macro level, the absence of tailored policies for the SME sector leads to further disparity in effective protection strategies.

There are many anecdotes of organisations shutting down or being badly affected by cybersecurity attacks, and we want to ensure that your organisation is not next.

Addressing The Gap

The stakes are high, but our approach is **practical:** instead of fearing the inevitable, be prepared for it. Cybersecurity isn't about eliminating risks entirely, but instead about fortifying your operations to withstand them.

A lot of it follows the 80/20 rule, where 80% of the effectiveness is achieved by 20% of the work and cost. That is why it is important to understand cybersecurity to ensure you get the maximum protection.

However, technical jargon and perceived complexity of cybersecurity often deter business owners and operators from engaging meaningfully with cybersecurity strategies.

We believe this is a solvable issue.

Through this book, we aim to:

- **Simplify Cybersecurity Concepts:**
  Break down intricate cybersecurity topics into understandable business language, making them accessible to non-technical stakeholders.
- **Integrate Cybersecurity into Business Processes:**
  Illustrate how cybersecurity measures can be seamlessly incorporated into existing business goals and operations, enhancing overall resilience. Or how to choose different solutions that enhance resilience without impeding operations.
- **Empower Decision-Makers:**
  Equip business leaders with the knowledge to make informed decisions regarding investing in cybersecurity solutions and creating cybersecurity policies.

A Little Bit of Backstory

Ethan started the process of writing this book two years into joining cybersecurity as an industry because he found a massive gap in the way businesses and cybersecurity practitioners were talking about cybersecurity.

This often leads to business owners and operators neglecting cybersecurity, leaving it to the Chief Information Security Officer (CISO), IT department or technology departments. However, business owners and operators miss an opportunity to use and understand cybersecurity to their advantage, such as building trust in key areas of the business.

There is immense value in understanding and utilising the concepts of cybersecurity to create resilient businesses, especially in this world where we are all dependent on our digital information systems to do our work. But it is gated by the difficulties of learning the topic. To be a practitioner, we need a deep understanding of networking, operating systems, hardware, programming languages, etc. However, business leaders do not need that.

That is why a change in approach was in order.

Ethan then gathered a team of experienced cybersecurity and risk practitioners to create this book and framework, mixed in with his own learnings from attending various top conferences internationally such as Mandiant's mWise and RSA Conference.

As a person who learned business the hard way in this harsh world, Ethan dived into cybersecurity in the last few years, bringing his perspectives and the ability to bring the different experts' experiences and tie them into a single framework.

We believe that this can help solve the current problem. This book has been more than a year in the making and counting, and we hope to keep it going for many years to come as we gather more sector specific stories and go deeper into each business-enhancing technology.

How to Use This Book

“Practical Cybersecurity Decisions” is structured to serve as both an educational resource and a practical guide:

1. **Foundational Understanding:** Your first read will never be complete. Start by skimming through the book to build a general idea of how we can break down your business goals into the relevant digital and IT systems before going into cybersecurity needs.

2. **Framework Application:** As you read, use the provided framework to assess and enhance your organisation’s cybersecurity posture, aligning it with your specific business goals. Understand that your first run would never be perfect but knowing how much you know would help you understand what to learn more and what solutions to get.

3. **Start Trying:** Ask your technology vendors the questions that you’ve gained from this book – What should you protect? How do they protect it? What ensures the resilience of the data in your technology stack? After using the framework, you would gain a lot more about what matters in your organisation in terms of resilience and therefore what should be protected and how do you protect them.

4. **Reference Tool:** Refer to this book when faced with cybersecurity decisions or challenges, using it as a roadmap to navigate complex issues. As we come up with industry-specific versions and technology updates, you will get access to the best practices to ensure that your cybersecurity strategies are sound.

5. **Engagement and Feedback:** We encourage you, the readers, to reach out for clarifications, share experiences, and provide feedback to foster a community of continuous learning and improvement. We have purposefully designed this to be open-sourced, which means that we welcome any contributions to it and want to share the information freely.

By following this approach, you can transform cybersecurity from a daunting challenge into a manageable and integral part of your business strategy.

For the Practical Cybersecurity Framework, which you will be using throughout the book, please go to https://practical-cyber.com/framework to get access to it for free!

CHAPTER

02

Understanding What to Protect

Cyber Posture Begins with Understanding What to Protect

(and what you should pay to protect)

The foundation of a good cybersecurity strategy is not blindly following standards and frameworks with technical jargon (and their massive checklist), but rather, beginning with business goals. From the business goals and operations, you will gain an understanding of your business-critical assets.

As business owners and operators, together with your management team, you need to know the relevance of what you are protecting, commonly known as the "crown jewels".

Cybersecurity, at its core, is about protecting what matters most to your business—your revenue, reputation, and the systems that enable your operations. It is through understanding the relevance of these assets that we understand if the investments in time, energy and money are going to be worth the effort.

This approach then aligns with a core principle of the **NIST Cybersecurity Framework:** identifying and prioritising assets based on their importance to your business.

By focusing on your organisation's unique context, you can establish a cybersecurity posture that would not only be effective, but also sustainable.

Defining Protection from the Root

Before we begin to build the cybersecurity side of things, we even need to understand what your business is about.

A common issue with many organisations is the perception that they have **too much business** to protect – they have too many streams of revenue, sensitive clientele information, fancy new technologies to optimise their processes, etc.

However, knowing what is essential to the survival of the business is the root.

There are only 3 things that typically a business needs to be concerned with:

- **How to generate revenue (Top Line)**
- **How to manage operations and costs (Bottom line)**
- **How to stay out of trouble (Regulations/Compliance)**

In our Practical Cyber Framework, we identify what's most important by beginning with business name, industries it's involved in, revenue sources and annual revenue.

This is in the frame called "Risk Profiling of Organisation". These categories focus on the Top Line. From filling these categories, there are multiple considerations that we can start discussing about:

1. Just by the industries the organisation is in, it'll change the cybersecurity risk profile:

   a. Some industries are considered "high-risk" regardless of annual turnover.

   b. Some industries have regulations placed on them such as DORA in the European Union, CCoP in Singapore, or HIPAA in the USA.

2. Revenue streams are the lifeblood of any business. Knowing them and keeping track of them before diving into the cybersecurity elements is key to maintaining our focus as business-first, therefore practical.

3. Please note that the industries and revenue channels should be ranked by criticality – the safe, bills-paying revenue channels should be at the top of the list, before the larger revenue channels that are more for extra profit. This is because we're looking at essential parts of the business first.

4. Annual revenue decides another large portion on the risk profile of the organisation, as cybercriminals are generally financially motivated and will always target organisations according to their revenue.

From our revenue-generating parts, we will explore point 2, the costs of operations (Bottom line) in the second part of the framework, called Identifying Key IT Assets.

The reason for this is that IT assets often take up key roles in the operation process, which supports revenue generation. We can protect and reduce costs where needed thereafter.

On top of these key business operations technologies, we would also need to concern ourselves with the regulatory and compliance requirements that are placed upon us in our industries (How to stay out of trouble).

Sector	Collected Data
Hospitality	1. Personal Identifiable Information of customers 2. Credit card information of customers 3. Various audit requirements to enhance reputation
Finance	1. Government regulations for any financial-related organisations 2. Audit requirements for access to payment networks 3. Financial sector often gets targeted by cybercriminals and threat actors, which is why security is a must, rather than just a plus
Manufacturing	1. Many manufacturing organisations need audit requirements to serve larger clients 2. Some parts of manufacturing are considered critical infrastructure in their jurisdictions
Retail	1. Many manufacturing organisations need audit requirements to serve larger clients 2. Some parts of manufacturing are considered critical infrastructure in their jurisdictions 3. If you collect personal identifiable information of customers for loyalty programmes 4. Credit card information of customers 5. Generally, smaller retail organisations are not often regulated aggressively

There are too many sectors for us to list, but this should provide a good idea of what are the common cause for compliance and regulation – the data an organisation collects and the sensitivity of the industry.

The truth is that the methodology of analysis across the industries will be similar in terms of the types of risk that prevent your business from achieving its goals
(Eventually we'll have dedicated pages from open-sourced and verified information about what each industry in each state needs to adhere to.)

Why Threat Profile

What we did above was a very cursory threat profiling exercise, which is to gauge the risk of an organisation under the threat of cyber-attacks. Every organisation faces cyber threats, but the nature and intensity of those threats vary significantly based on the organisation's size, industry, and perceived value to attackers.

Threat profiling helps organisations understand who their potential adversaries are, the methods they might use, and the level of effort they're likely to invest in an attack. By aligning defences with the organisation's specific risk profile, businesses can allocate resources more effectively and prepare for the most probable threats.

Profiling Threat Levels by Organisational Risk

1. Low-Risk Organisations: The Bot-Driven Threat Landscape

- **Who Are the Attackers?**

  Low-risk organisations, such as small businesses or early-stage startups, are primarily targeted by **opportunistic attackers.** These attackers often use automated tools or bots, casting a wide net, seeking easy-to-exploit vulnerabilities rather than focusing on specific targets.

- **Common Threats:**

  Credential Stuffing: Bots use stolen credentials to attempt logins across multiple sites.

  Automated Social Engineering: They send out cookie-cutter emails to every email they can hoping for someone to take the bait.

  Web Scraping: Automated tools extract data from public-facing websites.

  Exploiting Misconfigurations: Bots scan for unpatched systems, default passwords, or misconfigured cloud services.

  Day-One Vulnerabilities: Bots scan for unpatched systems with known vulnerabilities that are preventable.

2. Medium-Risk Organisations: Targeted but Not Persistent

- **Who are the Attackers?**

  Medium-risk organisations are attractive to **cybercriminal groups** that are more deliberate in their efforts. These attackers are willing to invest time and resources in exploiting specific vulnerabilities to achieve financial or strategic gains.

- **Common Threats:**

  All Automated Attacks Listed Above: Medium-risk organisations receive the same automated attacks as well.

  Phishing and Social Engineering: Tailored emails or messages designed to steal credentials or deploy malware. Sometimes, they do spear-phishing, which is highly targeted phishing campaigns customised to each high value target.

Ransomware: Attackers will find their way into the system from vulnerabilities as mentioned above, lock systems and/or data until a ransom is paid.

Supply Chain Attacks: Criminal groups might use a less secure company that provides services for the more secure company to find ways of entering through email systems or vendor portals.

Business Email Compromise (BEC): There have been cases of criminal gangs compromising the email systems of an organisation to wait and watch, then impersonating executives or partners to fraudulently authorise transactions.

3. High-Risk Organisations: Facing Sophisticated Attackers

- **Who Are the Attackers?**

  High-risk organisations, such as financial institutions, government entities, or critical infrastructure providers, are targets for **advanced persistent threats (APTs).** These attackers may include nation-states, highly organised criminal groups, or industrial espionage actors. Their attacks are often well-funded, patient, and sophisticated.

- **Common Threats:**

  All Attacks Listed Above: High-risk organisations receive all the above attacks, while having more higher risk activities listed below.

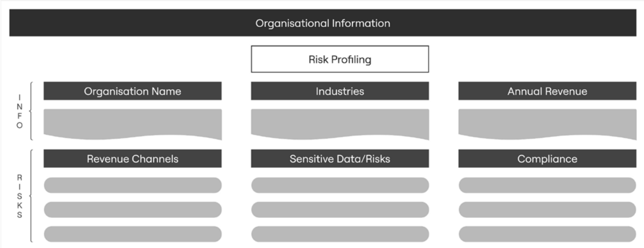
  Long Dwell-Time Attacks: Long-term, stealthy campaigns aimed at stealing sensitive data or causing disruption. The attackers will be constantly testing the security of the organisation, and once they find entry, they might bide their time to find the perfect time to make their moves to avoid detection.

  Zero-Day Exploits: There are zero-day vulnerabilities that are unknown to the technology vendor or public being sold on the market that the attackers will use on the organisations.

  Insider Threats: Next level of social engineering – paying or convincing employees or contractors to provide access to sensitive systems. Can be through money, ransom or other means of espionage.

  DDoS and RansomOps: APTs can plan coordinated efforts to disrupt operations or demand large ransoms. These efforts are often planned for a long time with compromised systems around the world gathered by the APTs.

How To Do Basic Threat Profiling


Organisational Information
Risk Profiling
INFO
Organisation Name
Industries
Annual Revenue
RISKS
Revenue Channels
Sensitive Data/Risks
Compliance

As what we have done, you have listed the key information that helped you:

1. **Assess Organisational Value**
   Identify assets that could be valuable to attackers, such as customer data, intellectual property, or financial systems.

   Understand the industry-specific risks you face (e.g., healthcare, finance, or retail).

   Typically, if your organisation has little to no assets that are of value to attackers, you are considered low risk.

With some amount of assets such as personal details, or sensitive details, medium risk.

If your organisation has thousands of points of sensitive data, typically it would be under high risk.

2. **Analyse Potential Threat Actors**
   Consider who might target your organisation (e.g., opportunistic hackers, cybercriminals, nation-states).

   From the list above, you can have a good idea of what your organisation is likely to face.

3. **Evaluate Attack Likelihood and Impact**
   Assess the likelihood of different types of attacks based on your organisation's size, visibility, and sector, as mentioned above.

   Estimate the potential impact of a successful attack on your operations, reputation, and finances.

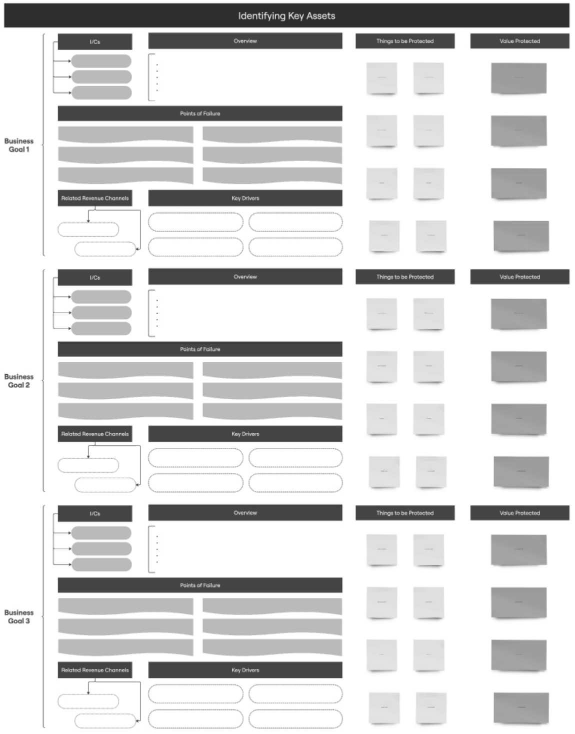
While this is very cursory, it is very helpful to provide an estimate of the amount of effort and investment needed to protect your organisation.

Many of you reading this might have low risk if your organisation is an SME with little to no exposure to sensitive data. While those with medium risk would need to start assessing the likelihood and impact of cyber-attacks.

For organisations under high risk, if your organisation does not already have a security team, it is time to seriously consider equipping your organisation with the right talents.

While we can go deeper into threat profiling, the goal of this book is not to provide you with the full plan, but to help you understand how to structure your cybersecurity strategy within your organisation. With that, we can move to the next portion, which is identifying your key IT Assets.

Identifying Key IT Assets



After identifying the key areas of concern of the organisation in general, we then need to break down the key assets that are essential to the three most important things above.

On top of that, every organisation has distinct business goals, whether it's maintaining uninterrupted operations, delivering quality products or services, or protecting customer trust. These goals provide the lens through which you can identify your business-critical assets.

These may include:

- **Revenue-Generating Systems:** E-commerce platforms, point-of-sale systems, or customer relationship management (CRM) software.

- **Intellectual Property:** Proprietary software, secret processes, or unique frameworks that give your business a competitive edge.

- **Sensitive Data:** Personal data of customers and employees, financial records, or confidential agreements.

- **Vendor and Partner Dependencies:** Key third-party tools and services that enable your operations.

- **Reputation Touchpoints:** Digital assets like websites, social media accounts, and public-facing customer portals.

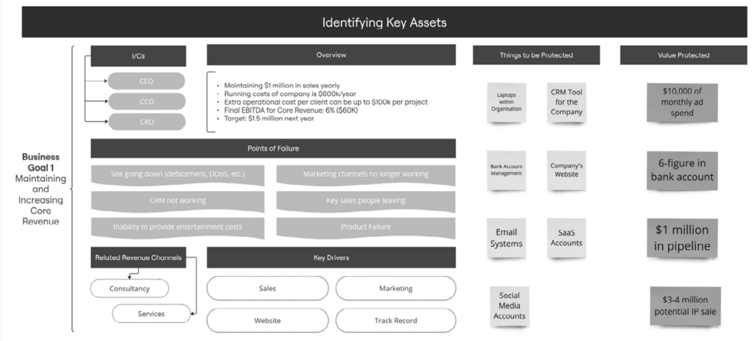
Technology is a necessary enabler of our business, and every component includes its risk – whether it is cyber-attacks or downtime.

By identifying these key points in our technology stack where we need to maintain high availability, or to be protected from leakages, we can start to protect our business from negative impacts from cyber-attacks or IT outages.

But to deepen our understanding, it is important to not focus on the IT assets first. Instead, we begin with the business goals that your organisation has.

To go through the practice, we need to start with the business goals, which are organised in such a way that we need to name it, identify the people who are in-charge of it, and the revenue channels it is related to.

For more organisationally wide goals such as human resource, governance, and legal frameworks, it is important to specify which revenue channels it affects the most. That would help to identify the business impact as well.



Identifying Key Assets

Business Goal 1
Maintaining and Increasing Core Revenue

I/Cs
CEO
CCO
CRO

Overview
- Maintaining $1 million in sales yearly
- Running costs of company is $600k/year
- Extra operational cost per client can be up to $100k per project
- Final EBITDA for Core Revenue: 6% ($60K)
- Target: $1.5 million next year

Points of Failure
Site going down (defacement, DDoS, etc.)
Marketing channels no longer working
CRM not working
Key sales people leaving
Inability to provide entertainment costs
Product Failure

Related Revenue Channels
Consultancy
Services

Key Drivers
Sales
Marketing
Website
Track Record

Things to be Protected
Laptops within Organisation
CRM Tool for the Company
Bank Account Management
Company's Website
Email Systems
SaaS Accounts
Social Media Accounts

Value Protected
$10,000 of monthly ad spend
6-figure in bank account
$1 million in pipeline
$3-4 million potential IP sale

In the example version of the Practical Cyber Framework, we highlighted a common, almost-too-generic goal of "Maintaining and Increasing Core Revenue".

Though this can be applied to every organisation, the key differences lie in the fact that it should be tied to specific revenue channels and need to be meaningfully measured. The reason why the people in-charge (I/Cs) are important is because they are often also the biggest target points for cyber-attacks and have access to sensitive information.

Also, the current numbers and growth targets should be included in the overview, as listed in the example, as it provides the perspective as to how much money is on the line.

One of the biggest struggles in cybersecurity is to explain the financial impact of the protection afforded, especially because it is not effective to **measure what did not happen.**

Instead, through this method, we can look at the value of what we are protecting, and therefore the impact is tied to the revenue, reputation and other important business assets.

Key Drivers

When we talk about maintaining and growing core revenue, we need to recognise on a business level what is driving that. In the case of the example used in the framework, the sales team is a major driver as they do account management, customer success and sales all in one. This is when it is important to recognise that whatever facilitates their success is essential to the business goal.

Marketing is also a key driver, which generates new leads and creates a better impression on their existing clientele. Therefore, their marketing processes have to be seen as essential to the sustainability of the business.

Next up, the website and track record are both key selling points of the company – the website is the first touch point with most potential clients, and the track record is often what wins the accounts.

The way it is organised is according to what is the most day-to-day driver, not just importance. Because sales and marketing are constant processes, they are listed at the top. Meanwhile, the website is something that can sustain a few days of downtime if managed right. And for the track record, it is something that can be communicated through other means beyond digital presence.

Points of Failure

As the name suggests, it points where the goals will be thwarted in relation to the key drivers. When thinking about what can cause the key drivers to fail, what would be the answers?

In the list provided in the example, one was website defacement which hurts the reputation of the company and prevents them from getting new clients.

Another one is sales team leaving (which is not IT related), which is also a major point of failure.

To create this list, it is better to do this on sticky pads and digitally so that we can fill in as many ideas as we want and choose the most probable and plausible to put into the framework. For example, here is a list of potential points of failure:

1. Clients closing down
2. Website defacement
3. Contract failure leading to cancellation
4. Mass resignation of staff
5. Key sales members leaving
6. CRM data loss
7. Marketing Channels Failure

When we place it into the framework, we can recognise that clients closing down is not something that the organisation can control or predict, therefore, recognising it as a point of failure in this framework does not help.

From here, we start thinking about the parts of the business where IT plays a major role in our processes. From the email systems being the key communication point with their clients, to their website being the first point of contact with their clients, the impact of any IT infrastructure issue can and will have an impact on.

For some organisations, like those in the food and beverage (F&B) sector which is mostly manual and human-based, the digital touch points would not be of as much significance. Whereas for a consultancy as in the case of the example organisation, it could play a major role in their ability to canvas for clients, do sales, and maintain relationships with their clientele.

Also, when the Customer Relationship Management (CRM) software stops working or loses data, the ability for sales to follow up and manage clients might be greatly diminished if it has been a key aspect of managing the pipeline of potential clients.

Also, for some organisations, their book of contacts is their biggest value, and the CRM holds this value, which is why it is essential to ensure that things are properly stored and indexed. (On a side note, for SaaS, it is important to also understand the liabilities of the service provided by the SaaS companies in terms of data storage, availability and backup.)

This awareness of key drivers in the organisation would allow us to understand what to protect when it comes to IT systems, whether it is against failure or cyber-attacks that lead to leaks.

Things to be Protected

When we start looking at the process that is required for business to flow, it is often surprising how much or little technology plays a part in it. In some parts, where the bank accounts are controlled through internet banking and key personnel have it, their devices are part of the assets to be protected.

Furthermore, as key personnel's laptops and software contain key information about clients, project progress and are also the basis for communication with the clients, laptops failing and becoming unavailable can set back projects and management of services.

For some organisations that do not actively leverage technology, many of the conversations might be on their work mobile's business WhatsApp or Telegram accounts where a lot of communication with end clients is centred around. Those might be more important to protect than their laptops.

When we look at these "Things to be Protected", they range from devices to applications to access to resources (bank accounts, social media accounts, etc.). The key questions always go back to:

1. How essential is this device in day-to-day operations, or is part of essential processes within the organisation?

2. What data is in the application, the sensitivity of it and the need for it in the day-to-day operations?

3. What is the access to resources that we need to maintain operations and gather new clientele?

4. Who has access to the data?
   Are they the right people?

5. What information is sensitive, and if revealed to the public or competitors, can hurt our organisation?
   It could be reputational damage, loss of competitive edge or regulatory fines that create the hurt.

This exercise is not about accuracy but about increasing the awareness of the importance of the IT systems that we use in our organisations.

Very often, only when something fails would we understand the value of it – our mobile devices failing, creating problems in mobile banking, or our laptops failing, causing us to lose track of key information for clients.

This exercise is, instead, a pre-emptive look at what could go wrong, gathering of experience of the different people within the organisation to understand what to protect more effectively.

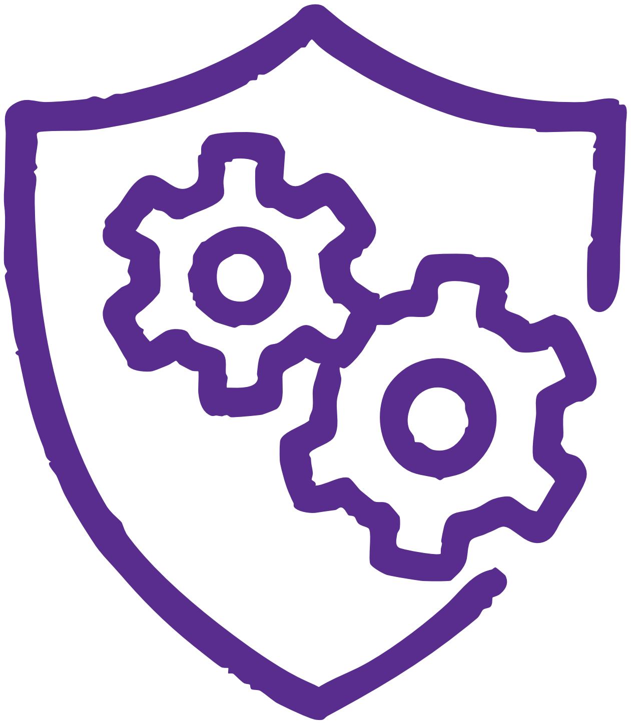
Value Protected

As mentioned above, the best way to identify the importance of protecting something is the value of the assets they are protecting. In the example that is provided, we have included information such as the pipeline and monthly ad spend as things that we are protecting.

The reason is simple – for the team to do their business with peace of mind and not be waylaid by IT failures or cyber-attacks allows a smooth flow of operations and therefore stronger operations.

Of course, those processes contain many moving parts and many stakeholders that are important to make it happen.

Cybersecurity is one aspect of this many-faceted process called doing business and should have a seat at a table. As much as we advocate for good cybersecurity, we believe that it is best used in the context of business.



CHAPTER

03

How To Protect

Let's Protect Our Business

Now that we have spent time on identifying **what** to protect and **why** to protect, we can start the process of how to protect. There are several layers of this.

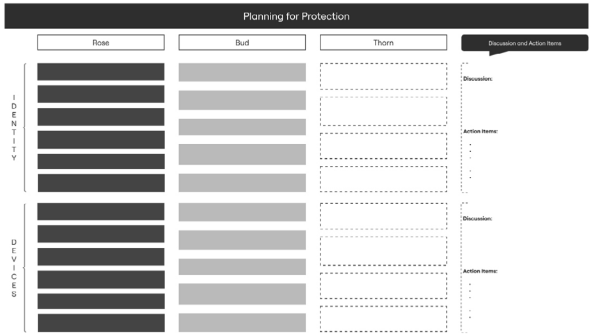
If we were to follow the **NIST Cybersecurity Framework,** it goes from **Protect, Detect, Respond and Recover** as the main concepts. In this book, though, we are going to bring another framework of understanding cybersecurity, **Zero-Trust Architecture (ZTA),** into the fold to organise the information.

Why do we choose **Zero-Trust Architecture?**

The core pillars of ZTA are simple, Identity, Devices, Network, Application and Data. There are technical security-focused pillars of Automations and Orchestration, and Visibility and Analytics, which we will not go into detail in this book, and the Practical Cyber Framework as this is just the starting point.

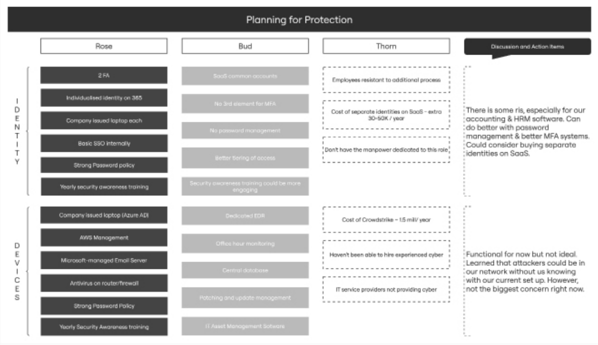
We would instead focus on the five pillars to form a strong base of understanding how to protect.

However, before we start going into each section, we will dive into how to use the **Practical Cyber Framework** to write out different parts to create an understanding of the cybersecurity posture of the organisation.



There is a User Experience Design process called **Rose, Bud, Thorn,** where we talk about what is going well (Rose), what are the potential places for improvement (Bud) and what are the limitations (Thorn). We discovered this to be a great way to create honest conversations around the risk we are willing to take on when it comes to cybersecurity.

In the example version of the framework, we would cite that 2-factor authentication (2FA) is turned on, that using Microsoft 365 Enterprise allows each individual to have their own identity, and that the company issues individual laptops with basic Single-Sign-On features internally. These are great starting points to work from that allows security to be built onto the existing features that the organisation has in terms of Identity.



Planning for Protection

	Rose	Bud	Thorn	Discussion and Action Items
IDENTITY	2 FA	SaaS common accounts	Employees resistant to additional process	There is some ris, especially for our accounting & HRM software. Can do better with password management & better MFA systems. Could consider buying separate identities on SaaS.
	Individualised identity on 365	No 3rd element for MFA	Cost of separate identities on SaaS - extra 30-50K / year	
	Company issued laptop each	No password management	Don't have the manpower dedicated to this role	
	Basic SSO internally	Better tiering of access		
	Strong Password policy			
	Yearly security awareness training	Security awareness training could be more engaging		
DEVICES	Company issued laptop (Azure AD)	Dedicated EDR	Cost of Crowdstrike ~ 1.5 mill/ year	Functional for now but not ideal. Learned that attackers could be in our network without us knowing with our current set up. However, not the biggest concern right now.
	AWS Management	Office hour monitoring	Haven't been able to hire experienced cyber	
	Microsoft-managed Email Server	Central database	IT service providers not providing cyber	
	Antivirus on router/firewall	Patching and update management		
	Strong Password Policy			
	Yearly Security Awareness training	IT Asset Management Software		

The buds are areas to improve on, for example, that the online SaaS accounts are using common accounts rather than individual accounts (such as HR Management software) because only 2-3 people have access to this account and there is an unwillingness to pay for full features. There is also a lack of a third portion for Multi-Factor Authentication (MFA) like authentication key or mobile-based challenges due to a lack of features in their current set-up.

Also, the hierarchy of access to certain data is not tiered effectively in terms of digital identity, which also presents a risk that someone might have access to data that they should not have. This visibility allows the organisation to weigh the risks according to the sensitivity of data and the urgency of the problem.

Finally, we talk about the thorns. This is where we can be as honest as can be to say what the struggles are. Is it time? Is it someone with knowledge? Is it the fact that there needs to be a dedicated employee in order to implement such policies? This framework is designed to bring out honesty if possible, allowing us to find the real pain points.

We then go into the discussion section.

This is where we weigh in on the costs and value of each of the features. Eventually, we will be open sourcing a list of important security features that can support a much stronger cybersecurity posture for the organisation without much cost. This comes in the form of existing features of platforms, developing simple connections and coming up with configurations and practices that support the posture that the organisation would like to grow towards.

In this book, we're all about the **practical** means of getting to a better cybersecurity posture, and while we have started this book, it's just to raise awareness of how to begin.

We will eventually provide materials and best practices to support organisations to get more secure, depending on their industry, their threat profile and their unique requirements.

CHAPTER

04A Identity

Identity – Cornerstone of Cybersecurity

At the core of every business are its people—employees, partners, vendors, and even customers. Businesses succeed or fail based on the actions, decisions, and trustworthiness of the people who make up their ecosystem. This human-centric reality is why **identity** sits at the very foundation of cybersecurity.

In today's digital-first world, people interact with systems, access data, and collaborate across platforms using digital identities.

These identities are often tied to the company's corporate email address, employee number, or a digital identity provided by the organisation. By individualising and ensuring that identities are well-tracked and managed, we have the foundation of cybersecurity.

1. **People are the Business**
   All business begins with people, accessing their email systems, applications and data, creating materials and services through those channels.

   Every one of these stakeholders interacts with your systems using some form of digital identity.

2. **Access is the Common Thread**
   Whether it's an employee logging into a CRM, a partner accessing shared documents, or a customer engaging with a service portal, the common denominator is **access through identity.** If identities are compromised, attackers can exploit access to steal data, disrupt operations, or damage reputations.

3. **Trust and Accountability**
   Identities are not just about access; they also establish accountability. Knowing who did what, when, and how is essential for both operational efficiency and forensic investigations.

   By securing identities, you maintain the trust that underpins relationships with employees, customers, and partners – you manage who gets access to what information, when and how.

The modern business environment is dynamic. Employees work remotely, vendors need temporary access, and customers expect seamless experiences. This fluidity makes robust identity management critical:

- **Preventing Unauthorised Access:** Identities ensure that only the right people have access to the right resources.
- **Reducing Insider Threats:** By limiting access based on roles and responsibilities, businesses can reduce the risk of accidental or malicious actions by insiders.
- **Enabling Secure Collaboration:** With proper identity controls, businesses can confidently extend access to third parties without exposing sensitive systems.

At the end of the day, every breach, system downtime, or compliance failure boils down to one question: **Who had access?** If the wrong person had access—whether due to weak passwords, stolen credentials, or improper configurations—the fallout can be catastrophic. We always go back to identity because the most common cause of cybersecurity breaches is still through social engineering and stolen credentials.
What is Identity in Cybersecurity?

In cybersecurity, identity refers to the unique characteristics used to verify an entity—whether a person, device, or application. Typically, it comes in the form of a User Identity (corporate email when you login, username when you access certain applications).

Identity forms the basis for access control, which dictates who can access specific data, systems, or resources within your organisation.

Effective identity management involves:

- **Authentication:** Verifying that a user or system is who they claim to be (e.g., passwords, biometrics, multi-factor authentication).

- **Authorisation:** Determining the level of access and actions a verified identity is permitted to perform.

- **Accountability:** Keeping records of who accessed what and when for auditing and forensic purposes.

Aligning Identity with Cybersecurity Frameworks

To align what we do with existing frameworks, we would like to compare what we have listed with established frameworks. Frameworks like **NIST** and **ZTA** prioritise identity as a key pillar of cybersecurity. They provide practical guidelines to implement strong identity management.

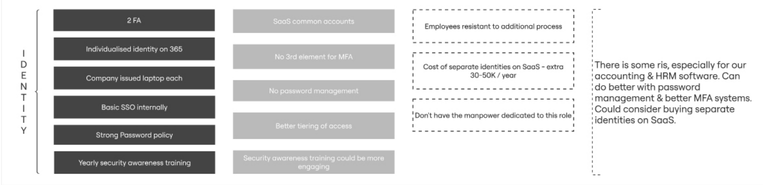
NIST Cybersecurity Framework: Protect Function

The **Protect** function of the **NIST Cybersecurity Framework** emphasises access control and identity management as foundational to cybersecurity. Key practices include:

1. **Identity Management Policies:** Develop clear policies for managing user identities and access levels. This includes creating individual user logins with differentiated access levels for different types of data and applications.

2. **Multi-Factor Authentication (MFA):** Require multiple layers of verification to strengthen authentication. The most basic form would be 2-Factor Authentication (2FA), while some would have use multiple means of verifying the authenticity of the login.

3. **Least Privilege:** Limit user access to only what is necessary for their role, reducing potential damage from a compromised account. For example, most employees do not have requirement to access payroll data on a day-to-day basis and therefore should never have access to that information. However, if they require it for their role, they can request and get approval for a limited time period.


IDENTITY
2 FA
Individualised identity on 365
Company issued laptop each
Basic SSO internally
Strong Password policy
Yearly security awareness training
SaaS common accounts
No 3rd element for MFA
No password management
Better tiering of access
Security awareness training could be more engaging
Employees resistant to additional process
Cost of separate identities on SaaS - extra 30-50K / year
Don't have the manpower dedicated to this role

There is some ris, especially for our accounting & HRM software. Can do better with password management & better MFA systems. Could consider buying separate identities on SaaS.

Zero-Trust Architecture: Identity as a Core Principle

The **ZTA**, an approach gaining significant traction, takes identity management to the next level:

1. **Continuous Verification:** Trust is never assumed. Users and systems must continually verify their identity during interactions. This means that whenever impactful decisions are made on the applications or data level, verification should be required to make these changes.

2. **Granular Access Control:** Access decisions are made in real time, based on the user's identity, device status, and other contextual factors. This ensures accountability and verification that the access is by the person.

3. **Segmentation:** Resources are segmented so that even authenticated users have limited access, reducing exposure in case of a breach. This also reduces the potential for insider threat as there is limited access for people who do not need the access.

Practical Steps to Strengthen Identity

1. **Assess Your Current Identity Management Practices**
   Do you have a clear inventory of all user accounts (employees, vendors, partners)?

   Are unused or outdated accounts promptly deactivated?

   Are I/Cs accountable to check User Access Rights at a frequency dependent on the risk profile of the organisation?

   Do you monitor account usage for anomalies (e.g., access from unusual locations or times)?

2. **Implement Multi-Factor Authentication (MFA)**
   Use MFA for all sensitive systems and data. This adds a layer of security by requiring users to provide two or more forms of identification.

   For example, combine something the user knows (password), something the user has (a mobile device or token), and something the user is (biometric data). This can also include hardware keys that are unique and are only owned by the individual.

3. **Adopt a Role-Based Access Control (RBAC) Model**
   Define roles within your organisation and assign access permissions based on those roles.

   Regularly review and update these roles to ensure they align with current responsibilities.

   Actively remove users that are no longer relevant (change of roles or leaving the organisation) to ensure access is only to relevant individuals.

4. **Strengthen Password Policies**
   Require strong, unique passwords for all accounts.

   Encourage or mandate the use of password managers to simplify compliance with this policy.

5. **Utilise Identity and Access Management (IAM) Tools**
   Deploy IAM systems to centralise identity management and enforce consistent policies. There are in-built systems with Google and Microsoft, and understanding these systems can be a first step.

   These tools can automate account provisioning, monitor activity, and ensure compliance with access control policies.

6. **Regular Training and Awareness**
   This is the first but not the last time that employee training and awareness are highlighted, because employees are the weakest link and the strongest defence against cybersecurity issues. It depends on whether you utilise them well.

   Train employees on the importance of secure identity practices, and rather than using boilerplate learning processes, the more personalised the learning, the more effective.

   Include guidance on recognising phishing attempts and safeguarding credentials. This can come in the form of phishing exercises or having a champion that shares the information regularly.

Identity and Business Alignment

Strong identity management does not just protect systems—it supports business goals by enabling secure collaboration and productivity. For example:

- **Secure Remote Work:** Identity controls like MFA ensure employees can access systems securely, even from outside the office.

- **Vendor and Partner Access:** Granular identity controls enable third-party collaboration without exposing unnecessary resources.

By making identity a focus, you create a foundation upon which the rest of your cybersecurity measures can stand.

The next step involves mapping identity practices to business-critical assets and processes, ensuring alignment with organisational priorities.

CHAPTER 04B Devices

Protecting Devices

After Identity is set, devices are the next to be protected, as devices are the lifeblood of any modern organisation. From employee laptops and smartphones to point-of-sale systems and IoT devices, these tools enable productivity, communication, and business operations.

However, they also represent a critical entry point for cyber threats. As with the story of the casino's internal networks being penetrated through a fish tank's thermometer system, every device can be a weak point. Protecting these devices—often referred to as endpoints—is therefore essential to securing your organisation's digital ecosystem.

Understanding Inherent Endpoint Risks

Devices act as gateways between your users and your business systems. Whether it's an employee accessing the company network remotely or a vendor using a shared application, every device introduces potential access for unwanted visitors.

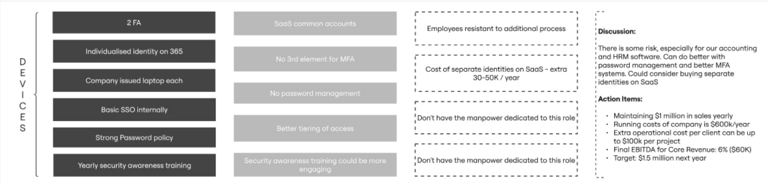
Key Risks Associated with Devices:

1. **Unauthorised Access:** Lost, stolen, or unsecured devices can give attackers a foothold in your systems. They can either gain access to it through unsecured credentials or social engineering with malware to gain access to the devices.

2. **Malware and Ransomware:** Compromised devices can be infected by and therefore serve as launch pads for malware, ransomware, or other malicious activities.

3. **Outdated Systems:** Devices without up-to-date patches or security configurations are easy targets for attackers.

4. **Shadow IT:** Unapproved personal devices or applications used for work can bypass security measures, exposing sensitive data.



DEVICES

2 FA
Individualised identity on 365
Company issued laptop each
Basic SSO internally
Strong Password policy
Yearly security awareness training

SaaS common accounts
No 3rd element for MFA
No password management
Better tiering of access
Security awareness training could be more engaging

Employees resistant to additional process
Cost of separate identities on SaaS - extra 30-50K / year
Don't have the manpower dedicated to this role
Don't have the manpower dedicated to this role

Discussion:

There is some risk, especially for our accounting and HRM software. Can do better with password management and better MFA systems. Could consider buying separate identities on SaaS

Action Items:

- Maintaining $1 million in sales yearly
- Running costs of company is $600k/year
- Extra operational cost per client can be up to $100k per project
- Final EBITDA for Core Revenue: 6% ($60K)
- Target: $1.5 million next year

A Comprehensive Approach to Device Protection

Protecting devices requires a combination of policies, processes, and technologies that address both organisational and individual responsibilities.

We will go through what are the ideal processes that can be used to maximise protection, but what your organisation needs is to scale it according to the needs of your organisation based on its threat profile.

1. **Device Inventory and Classification (Fundamentals)**

   Knowing What You Have: Maintain an up-to-date inventory of all devices used within your organisation, including company-owned and employee-owned (BYOD). This is all devices which have access to or contain company-related information.

   Classify Devices: Identify critical devices based on their access to sensitive data or systems. From our previous breakdown, you can identify what devices are critical for each business goal. For example, a server hosting the vendor portal warrants stricter controls than a personal tablet that has access to company emails for a low-access employee.

2. **Device Configuration and Hardening**

   Baseline Security Standards: Establish and enforce minimum security standards for all devices. This includes enabling firewalls, disabling unnecessary services, and using secure configurations. This requires regular maintenance and is often enforced by the IT or security team.

   Endpoint Protection: Deploy endpoint protection tools, such as antivirus software, endpoint detection and response (EDR) systems, and/or data loss prevention (DLP) solutions. These span from cheap to expensive depending on the needs of your organisation. You do not always need to buy the best in class, but also, knowing the quality of the solutions will be essential to peace of mind.

   Encryption: Ensure all sensitive data on devices is encrypted, both at rest (in storage) and in transit (being sent via email, transfer, etc.). This ensures that only the people with the access can have access to the information, and even if insider threats or attackers get their hands on the information, it will be hard to crack.

3. **Access Control and Authentication**
   (As mentioned in Identity)

   Enforce Strong Authentication: Require multi-factor authentication (MFA) for accessing critical systems.

   Implement Role-Based Access: Limit device access to systems and data based on user roles.

   Zero Trust Principles: Continuously verify device trustworthiness before granting access to sensitive resources.

4. **Regular Updates and Patch Management**

   Automate Updates: Use centralised tools such as IT Asset Management tools to push security patches and software updates to devices.

   Monitor Compliance: Regularly audit devices to ensure they meet the latest security requirements.

5. **BYOD (Bring Your Own Device) Policies**

   Create Clear Policies: Define acceptable use, security standards, and support limitations for personal devices.

   Use Mobile Device Management (MDM): Implement MDM solutions to enforce policies, monitor compliance, and remotely wipe data from compromised devices.

6. **Network Segmentation**
   (To be discussed more in the next section)

   Isolate Devices: Place high-risk devices (e.g., IoT devices, guest devices) on separate network segments to reduce exposure.

   Restrict Access: Limit device communication to only what is necessary for business operations. This prevents extra communication that can be hijacked by potential attackers.

Building a Culture of Device Security

Device security is not just a technical challenge; it's a cultural one. Employees play a significant role in maintaining the security of their devices, and their actions can significantly impact your organisation's cybersecurity posture.

Training and Awareness

- Educate employees on the importance of securing their devices. Sprinkle in their own benefits, such as protecting their own personal devices through these learnings.
- Train them to recognise and report potential threats,

such as phishing attempts or suspicious device behaviour.

Accountability

- Define clear responsibilities for device security within your organisation.
- Hold users accountable for adhering to security policies and reporting issues promptly.

Measuring Success in Device Protection

To ensure your device protection measures are effective, regularly evaluate your practices using these metrics:

- **Patch Compliance Rate:** Percentage of devices running the latest software updates.
- **Endpoint Detection Time:** How quickly threats are identified on devices.
- **Incident Response Time:** How long it takes to address and resolve device-related incidents.

As you go through the framework, **the Roses, Buds and Thorns** might not be very clear. It is okay to put them all down, and weigh in the ideas only afterwards.

While there are many security features you might not need as an organisation today, it'll be helpful to know what is in the market to know what is possible, and what is affordable.

Most organisations wouldn't have most of the technologies we are referring to in this book because there are many options of what we can do to secure an organisation.

However, the fundamentals are – the devices and endpoints need to have clear protection and systems in place for security to be able to withstand the majority of attacks.

CHAPTER

04C

Network

Protecting Your Network

The network serves as the central nervous system of any modern organisation, connecting devices, applications, and users to critical data and services.

While it enables seamless operations and communication, the network also represents a key attack vector for cyber threats, from data exfiltration to ransomware propagation.

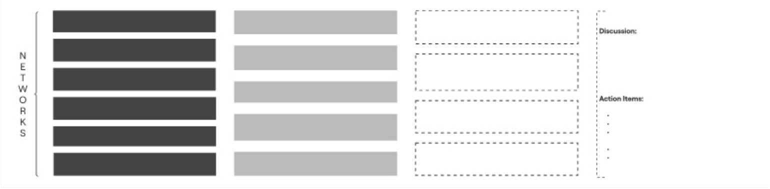
Therefore, understanding your network and the existing defences can provide a much clearer means of optimising security for the organisation. However, we recognise that this is not an area of knowledge for many business operators, so we need to deep dive further into this.

Why Network Security Matters

Networks are inherently interconnected, and this connectivity brings both benefits and risks. A compromised network can lead to:

- **Unauthorised Access:** Attackers can find and exploit weaknesses to infiltrate systems and steal data.
- **Data Loss:** Sensitive information can be intercepted during transmission. That is why encryption, even in internal networks, is essential.
- **Operational Disruption:** Malware or Distributed Denial of Service (DDoS) attacks can cripple network functionality.
- **Propagation of Threats:** Once inside, attackers can move laterally through the network to compromise other systems. They can find their way through the different layers of networks to find their way to your organisation's crown jewels.

To protect against these risks, organisations must adopt a proactive and layered approach to network security.



Core Principles of Network Security

1. **Visibility and Monitoring**
   You can't protect what you can't see. Continuous monitoring of network traffic is essential to detect anomalies, unauthorised access, or potential breaches.

   Use tools like Security Information and Event Management (SIEM) systems, Network Traffic Analysis (NTA), and Intrusion Detection Systems (IDS) for comprehensive oversight.

   On the most basic front, even having network logs on your organisation's firewalls, routers, applications and all would do wonders.

2. **Segmentation and Isolation**
   Divide your network into segments based on functionality and sensitivity. For example, separate employee's personal devices, IoT devices, and critical servers into different segments.

   Implement micro-segmentation to limit access within segments, reducing the risk of lateral movement during a breach. It is all about increasing the difficulty in getting to our crown jewels and business-critical assets.

3. **Zero Trust Approach**
   Apply Zero Trust principles by verifying every connec-

tion to the network, whether internal or external.

Enforce strict access controls, requiring authentications for all devices and users.

4. **Encryption**
   Encrypt data in transit across the network using protocols like HTTPS, TLS, and VPNs. This prevents people who are sniffing from being able to steal information in transit.

   Ensure sensitive communications are secure, especially when traversing untrusted or public networks when your employees are working remotely.

5. **Resilience and Redundancy**
   Design your network with resilience in mind. Redundant connections, failover systems, and disaster recovery plans ensure continuity in the event of an attack.

   While this is usually a technical process, understanding how this takes place and what risks the systems mitigate will be of great value.

Key Technologies for Network Security

1. **Firewalls**
   Firewalls act as a barrier between your internal network and external threats. Use Next-Generation Firewalls (NGFWs) that include features like deep packet inspection, application awareness, and intrusion prevention.

2. **Intrusion Detection and Prevention Systems (IDS/IPS)**
   IDS monitors network traffic for suspicious activity and alerts administrators.

   IPS goes a step further by automatically blocking or mitigating threats.

3. **Secure Access Service Edge (SASE)**
   SASE combines network security functions, like VPN and firewall, into a cloud-based model, ideal for securing remote access and cloud environments.

4. **Virtual Private Networks (VPNs)**
   VPNs encrypt traffic between devices and the network, providing secure access for remote workers and off-site operations.

5. **Network Access Control (NAC)**
   NAC ensures that only authorized devices can connect to your network and enforces compliance with security policies.

Best Practices for Network Security
(Not expected for all organisations to follow at all times)

1. **Perform Regular Audits**
   Have your team periodically review your network architecture, configurations, and policies to identify vulnerabilities and areas for improvement.

2. **Implement Access Controls**
   Restrict access to network resources based on roles and responsibilities. Use principles like least-privilege and need-to-know to minimize exposure.

3. **Enable Logging and Analytics**
   Capture logs of network activity and analyse them for trends, anomalies, and potential threats. Automation tools and AI can help process large volumes of data efficiently.

4. **Maintain Up-to-Date Equipment**
   Ensure network hardware and software are regularly updated with the latest patches and firmware.

5. **Train Employees**
   Educate staff about the importance of secure network practices, such as avoiding unsecured public Wi-Fi and

recognising phishing attempts.

Adapting Network Security for Modern Challenges

1. **Remote Work**
   As remote work becomes the norm, secure network access for distributed teams is critical. Use solutions like Zero Trust Network Access (ZTNA) and endpoint security to protect remote connections.

2. **Cloud Integration**
   Many organisations now operate in hybrid or fully cloud-based environments. Extend network security to the cloud with solutions like Cloud Access Security Brokers (CASBs) and SASE.

3. **IoT and OT Security**
   IoT devices and operational technology (OT) introduce unique risks due to their often-limited security capabilities. Segment these devices and monitor their activity closely.

Measuring Network Security Success

To ensure your network security measures are effective, monitor key performance indicators (KPIs), such as:

- **Time to Detect and Mitigate Threats:** How quickly can you identify and neutralise potential breaches? This is why organisations run red team exercises to see if the systems can detect and mitigate attacks.

- **Unauthorised Access Attempts:** The frequency of access attempts blocked by your security systems. At different threat profile levels, the quality of access attempts also changes, and therefore need to be considered.

- **Bandwidth Usage Trends:** Spikes in bandwidth may indicate malicious activity, such as a DDoS attack.

Your network connects every part of your organisation, making it a vital foundation for cybersecurity.

By implementing strong controls, leveraging advanced technologies, and fostering a culture of vigilance, you can ensure your network is not only a tool for productivity but also a fortress against evolving cyber threats.

Next, we will be discuss the security of applications – the computer software and web applications that drive our organisations today.

CHAPTER

04D Applications

Protecting Applications: Securing the Digital Interfaces of Your Business

Applications are the digital interfaces of modern business operations. They are the front-facing parts of the technologies that interact with your employees, customers and vendors, that power everything from internal workflows and customer interactions to supply chain management and financial transactions.

Whether it is Software-as-a-Service (SaaS) application, internally developed portals or key computer software that runs complex work, applications allow us to run our businesses.

However, their ubiquity also makes them prime targets for cyber threats. They can become the windows of opportunity for attackers to gain access to sensitive data, or your networks to find their way around. That is why it is also a key part of protecting your organisation.

Why Application Security Matters

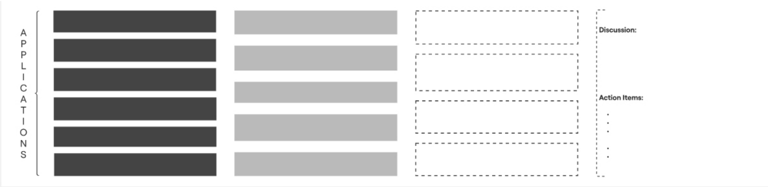
Applications often handle sensitive data, connect to critical systems, and operate across complex environments, including on-premises, cloud, and mobile platforms. As a reference, the OWASP Top 10 can give you a strong indicator of the potential weaknesses on applications.

Therefore, a breach at the application layer can have cascading effects across your business:

- **Data Breaches:** Exploited vulnerabilities can expose sensitive information, such as customer data or intellectual property. This is because the applications often have unfettered access to the database of information.
- **Operational Disruption:** Attacks like Distributed Denial of Service (DDoS) can render applications unavailable, halting critical business processes.
- **Reputational Damage:** Compromised applications erode

customer trust and damage brand reputation if defaced or manipulated to serve the goals of the attackers. This is especially important for companies that are doing high value work.

- **Compliance Violations:** Applications that fail to meet regulatory standards can result in imposition of fines and other legal consequences. Especially if discovered by a third party and reported to the organisation, there could be regulatory fines or other impact on the organisation.



Core Principles of Application Security

1. **Secure Development Practices** (For organisations that develop their own applications)

   Security begins in the development phase. Implement secure coding standards and practices to reduce vulnerabilities.

   Use Software Composition Analysis (SCA), Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) to identify issues early in the development lifecycle.

   It is impossible to eliminate all vulnerabilities, but it is imperative to have processes that reduce the most common and risky vulnerabilities, and to have a process to mitigate if reported.

2. **Authentication and Authorisation** (For applications developed in-house and from other vendors)

   Ensure robust user authentication and role-based access control (RBAC) within applications. If developed in-house, this can be adopted through different technology solutions to integrate with the application. If purchased, ensure that the product comes with access controls.

   Employ multi-factor authentication (MFA) to add an extra layer of security for users. This can be within the applications or have digital solutions to control access.

3. **Data Protection** (Ensure both developed and bought applications have this)

   Encrypt sensitive data both at rest and in transit.

   Mask data in non-production environments to protect it during development and testing.

4. **Regular Patch Management**

   Keep applications up to date with the latest security patches and updates to address known vulnerabilities.

5. **Least Privilege Principle**

   Limit application permissions to only what is necessary for their functionality.

   This is linked to RBAC, because you cannot achieve the least privilege principle without it.

Key Technologies for Application Security

1. **Web Application Firewalls (WAFs)**

   Protect web applications by filtering and monitoring HTTP traffic.

   Detect and block common attack vectors such as SQL injection, cross-site scripting (XSS), and other examples from the OWASP Top 10.

2. **Runtime Application Self-Protection (RASP)**

   Embed security into the application itself to detect and block threats in real-time during runtime.

   This is often managed by the vendor, or if your organisation has a team implementing it, it can greatly improve the security of the application.

3. **Application Programming Interface (API) Security**

   Secure APIs, which often serve as the bridge between applications and systems, by:

   Implementing strong authentication and authorisation.

   Enforcing input validation and rate limiting to prevent abuse.

   Monitor API activity for anomalous behaviour.

Penetration Testing and Vulnerability Scanning

Conduct regular penetration tests to simulate real-world attack scenarios and identify vulnerabilities.

Use automated vulnerability scanners to continuously monitor application security.

Best Practices for Application Security

(For in-house development)

1. **Shift Left in Security**

   Incorporate security into the earliest stages of the software development lifecycle (SDLC). This is through SCA, SAST and DAST as part of the process.

   Train developers on secure coding practices and provide tools for real-time code analysis.

2. **DevSecOps Integration**

   Integrate security into DevOps practices, creating a DevSecOps culture where security is an integral part of development and deployment workflows.

3. **Zero Trust Principles for Applications**

   Assume that every interaction with an application could be malicious. Require continuous validation of user and device authenticity.

   Segment application environments to prevent lateral movement in case of a breach.

Application Security when Purchasing

1. **Third-Party Risk Assessment and Audit**

   Many applications might have certain certifications such as SOC 2 Type 2, ISO27001, or PCI-DSS. However, doing due diligence to understand if their applications are well-managed and secured.

   Regularly audit these applications and ensure they are updated to their latest secure versions based on any risk that has been identified for that application or third party.

For lower risk applications that do not contain sensitive information, ensure that the login credentials and authentication methods are not repeated.

2. **Cloud-Native Applications**

   There are many SaaS applications that require cloud connections or internet access for the users to gain access to the applications.

   Use tools like Cloud Workload Protection Platforms (CWPPs) and ensure compliance with cloud security standards.

   Whitelist those domains and create unique access for these SaaS applications.

   Ensure computer software applications and cloud-based applications are being monitored regularly for their behaviours as they can also be space for attacks to take place.

3. **Mobile and Remote Access**

   Secure applications accessed through mobile devices with Mobile Device Management (MDM) and robust authentication measures.

   Protect remote access applications with ZTNA.

4. **Evolving Threats**

   Stay informed about emerging threats like supply chain attacks and advanced persistent threats (APTs) targeting applications.

   Implement threat intelligence feeds to proactively identify and mitigate risks.

Measuring Success in Application Security

To assess the effectiveness of your application security measures, track these key metrics for development:

- **Vulnerability Remediation Time:** How quickly vulnerabilities are identified and fixed for in-house solutions.

- **Number of Attempted Unauthorised Access:** How many times the applications have been attempted at access and how many were thwarted.

- **Attack Surface Reduction:** The number of open vulnerabilities and exposed APIs over time. This is especially important for any implemented solutions in the organisation.

- **Incident Response Time:** How quickly incidents affecting applications are detected and mitigated.

Applications are the interface of your business's data, processes, and customer interactions. Securing them is not just a technical imperative—it's a business necessity.

By implementing robust security measures, adopting best practices, and leveraging advanced technologies, you can protect your applications against evolving threats.

The next step in this journey is securing the **data** these applications process, ensuring that sensitive information remains protected regardless of where it resides or how it is accessed.

CHAPTER

04E

Data

Protecting Data: Securing the Lifeblood of your Business

In today's digital economy, **data is the most valuable asset** for any organisation. It powers decision-making, fuels innovation, and serves as the foundation of trust between businesses and their stakeholders.

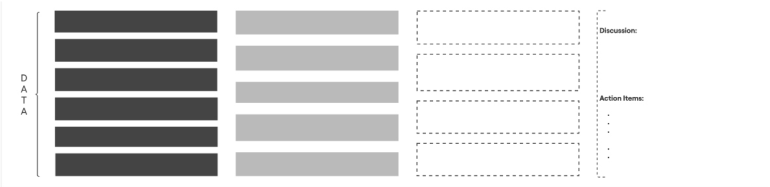
Moreover, in the age of artificial intelligence (AI), it is the new black gold. However, its value also makes it one of the most targeted assets by cybercriminals.

Protecting your organisation's data—wherever it resides or however it is accessed—is paramount to ensuring operational continuity, compliance, and reputational integrity.

Why Data Security Matters

Data breaches and leaks can lead to devastating consequences, including:

- **Regulatory Penalties:** Non-compliance with regulations like GDPR, PDPA, HIPAA, or PCI-DSS can result in substantial fines.
- **Reputational Damage:** Compromised customer or partner data erodes trust and can drive business away.
- **Operational Disruption:** Data loss or corruption can bring business processes to a halt.
- **Financial Loss:** Intellectual property theft, fraud, and legal costs can significantly impact profitability.



Core Principles of Data Security

1. Data Classification

Understand what data you have, its sensitivity, and its value to your organisation.

Categorise data as public, internal, confidential, or sensitive and apply appropriate protection levels to each category. This data classification also supports ensuring that the efforts in securing are optimised.

Categorisation and identification of the data is a key requirement for business impact assessments and the level of mitigation required for preparedness.

2. Data Encryption

In Transit: Use secure protocols like HTTPS, TLS, or VPNs to encrypt data being transmitted across networks.

At Rest: Encrypt stored data, including on local devices, servers, and cloud environments.

3. Access Control

As explained in identity, implement strict access policies to ensure that only authorised individuals or systems can access sensitive data.

Use role-based access control (RBAC) or attribute-based access control (ABAC) to align permissions with business needs.

4. Data Integrity

Ensure data remains accurate and unaltered during storage, processing, and transfer.

Use checksums, hashing, and validation mechanisms to detect unauthorised changes.

5. Data Minimisation

Only collect and store data that is necessary for business operations.

Regularly review and delete data that is no longer needed, reducing exposure in case of a breach.

Key Technologies for Data Security

1. Data Loss Prevention (DLP)

DLP tools monitor and control data transfers to prevent unauthorised sharing or exfiltration.

They can flag suspicious activity, such as sending sensitive information to personal email accounts or external cloud storage.

2. Encryption and Key Management

Use robust encryption algorithms (e.g., AES-256) and manage encryption keys securely. Today, it is helpful to utilise quantum-resistant algorithms, which AES-256 is one of them.

Consider hardware security modules (HSMs) for high-security environments. These are physical devices that store and manage cryptographic keys and perform cryptographic processing, which allows for increased security of encryption while not impacting performance.

3. Cloud Security Tools

Employ Cloud Access Security Brokers (CASBs) to monitor and secure data in cloud environments. They monitor and enforce security policies for cloud applications and services.

Use data discovery tools to identify and secure sensitive data stored in cloud services. They help to both gain insights and classify the data such that your organisation's sensitive data is properly identified.

4. **Data Masking and Tokenisation**

   Protect sensitive data by replacing it with anonymised or tokenised versions in non-production environments. There are several techniques to this and are more pressing for high-risk organisations.

5. **Backup and Recovery Solutions**

   Regularly backup critical data and test recovery procedures to ensure continuity in case of data loss or ransomware attacks.

   This is also part of IT resiliency for any technological outages or difficulties, together with disaster recovery procedures.

Best Practices for Data Security

1. **Develop a Data Protection Policy**

   Create a policy that defines how data is classified, stored, transmitted, and shared across your organisation.

   Ensure the policy aligns with regulatory requirements and industry standards. Again, this aligns with your organisation's threat profile as well.

2. **Regularly Audit and Monitor Data**

   Conduct regular audits to ensure compliance with data security policies and regulations.

   Monitor data access and usage for anomalies that could indicate a breach.

3. **Integrate Data Security into Application Design**

   Build security into the development lifecycle of applications that handle sensitive data.

   Ensure applications adhere to principles like privacy by design and secure data handling.

   This topic deserves a book on its own.

4. **Train Employees on Data Handling**

   Educate staff on the importance of data security and best practices for handling sensitive information. One of the biggest gaps in the staff's understanding would be how to understand if the data is classified sensitive, and that education is key.

   Include phishing simulations and social engineering awareness to address common attack vectors, especially regarding sensitive data.

Adapting Data Security for Modern Challenge

1. **Remote Work and BYOD**

   Ensure data security policies extend to remote workers and personal devices.

   Use secure access methods, such as VPNs and ZTNA, to protect remote data flows.

2. **Hybrid and Multi-Cloud Environments**

   Implement consistent data security measures across on-premises, hybrid, and cloud environments.

   Leverage CASBs and encryption for end-to-end protection.

3. **Evolving Regulatory Landscape**

   Stay informed about new and emerging data privacy laws and adapt your policies accordingly.

   Focus on meeting compliance standards proactively to avoid fines and reputational risks.

Measuring Success in Data Security

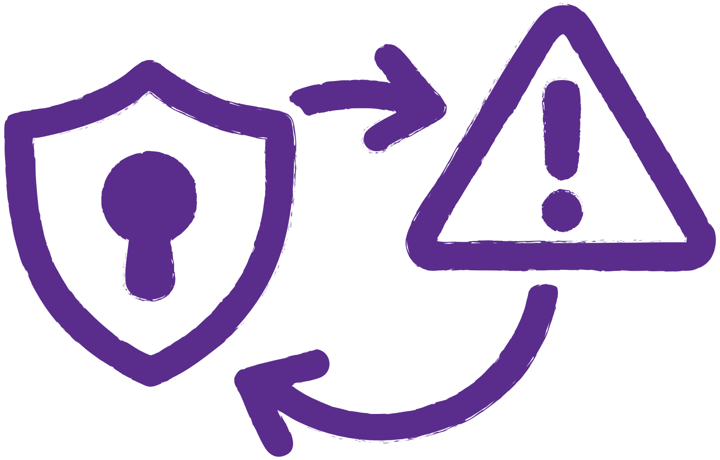
To ensure your data security efforts are effective, monitor key performance indicators (KPIs), such as:

- **Data Breach Incidents:** Number and severity of data breaches over a specific period. While you aim for zero, limiting the impact of a breach is also a great win.
- **Encryption Coverage:** Percentage of sensitive data encrypted at rest and in transit. This is to ensure that your sensitive data is much harder to access.
- **Access Violations:** Frequency of unauthorised access attempts detected and blocked.
- **Backup Success Rate:** Percentage of successful data backup and restoration processes. Testing this regularly would be helpful in ensuring that should real incidents happen; the systems are still intact.

As mentioned, data is the lifeblood of your business, and its protection must be a top priority.

By implementing strong data security measures, leveraging advanced technologies, and fostering a culture of accountability, you can mitigate risks and ensure that your organisation remains resilient in the face of evolving threats.

As you build and refine your cybersecurity strategy, remember that data security is not just about compliance or technology—it's about protecting the trust that forms the foundation of your relationships with customers, partners, and employees.



CHAPTER

05

Navigating Cyber Security Incident Notification in Malaysia

A Leader's Duty: Navigating Cyber Security Incident Notification in Malaysia

In our interconnected digital economy, a single cyber security incident is not a localised problem; it is a potential threat to our collective national cyber resilience. The "Crown Jewels" we identified in Chapter 2—your most critical data, computer systems, and processes —are often the very assets our adversaries target to disrupt operations and undermine trust. True cyber resilience, therefore, is demonstrated not just in the strength of our defences, but in the clarity, speed, and effectiveness of our response.

This chapter provides actionable guidance for all business leaders on their duties and best practices under the Malaysian Cyber Security Act 2024 [Act 854]. Its purpose is to equip you with the knowledge to lead with confidence during a crisis, ensuring you not only protect your organisation but also contribute to the security and stability of Malaysia's wider digital ecosystem.

The Legal Landscape: Your Core Responsibilities

The Cyber Security Act 2024 [Act 854] is a landmark piece of legislation designed to strengthen Malaysia's overall cyber-resilience. For business leaders, understanding its core tenets is no longer optional—it is a fundamental aspect of corporate governance.

- **National Critical Information Infrastructure (NCII)**
  Act 854 protects our nation's most vital computer systems, which are defined as National Critical Information Infrastructure (NCII).

  An NCII means a computer or computer system which the disruption to or destruction of the computer or computer system would have a detrimental impact on the delivery of any service essential to the security, defence, foreign relations, economy, public health, public safety or public order of Malaysia, or on the ability of the Federal Government or any of the State Governments to carry out its functions effectively;

  The organisations that own or operate these computer or computer systems are designated as **NCII entities by the respective NCII sector lead in respect of the NCII sector for which it is appointed.** Once an organisation is designated as NCII entity by the NCII sector lead, the duties of NCII entities enumerated under Act 854 would apply to that NCII entity including the duty to give notification on cyber security incident.

  They are stewards of services vital to the nation, covering eleven sectors:
  - Government
  - Banking and finance
  - Transportation
  - Defence and national security
  - Information, communication and digital
  - Healthcare services
  - Water, sewerage and waste management
  - Energy
  - Agriculture and plantation
  - Trade, industry and economy
  - Science, technology and innovation

- **The Reporting Authority: Your Partner in Resilience**
  The Cyber Security Act 2024 (Act 854) empowers the National Cyber Security Agency (NACSA) as the central coordinating authority for national cyber security. The duty to notify under the Act is a crucial, collaborative effort involving both the central agency and sector-specific regulators.

  Under **Section 23 of the Act,** when an NCII entity discovers a cyber security incident, it must notify both the **Chief Executive of NACSA** and its respective **national critical information infrastructure sector lead.** This dual notification ensures that both the national coordinating body and the specific sector authority are alerted, allowing for a more effective and tailored response. This reporting mechanism is not intended to be punitive; it is a function designed to protect the entire business community by preventing the spread of threats.

- **The Cost of Inaction: The Business "So What?"**
  The responsibilities under Act 854 carry significant weight. For designated NCII entities, a failure to notify a cyber security incident as required under Section 23 of the Act commits an offence and, on conviction, is liable to a fine not exceeding five hundred thousand ringgit (500,000RM), to imprisonment for a term not exceeding ten years, or to both. This potential liability transforms a legal duty into a direct and material business risk that every leader must manage proactively.

Identifying a Reportable Incident

A leader's responsibility is to discern between a minor IT issue and any cyber security incident that threatens the business. A "cyber security incident" is defined as an act or activity carried out on or through a computer or computer system, without lawful authority, that jeopardises or adversely affects the cyber security of that computer or computer system or another computer or computer system. From a business perspective, this includes:

- **Ransomware Attacks:**
  When malicious actors encrypt your critical files and demand payment, directly halting your operations.

- **Significant Data Leaks:**
  When sensitive or confidential information, such as customer personal data or corporate intellectual property, is exfiltrated or exposed.

- **System Intrusions:**
  When an unauthorised party gains access to your secure networks or protected computer systems.

- **Major Service Disruptions:**
  When a cyberattack, such as a Distributed Denial of Service (DDoS) attack, renders your key services unavailable to your customers or stakeholders.

- **Any other incident** that seriously harms or has the potential to harm services vital to Malaysia's national security, economy, or public health and safety.

A Culture of Proactive Reporting

In the face of an evolving threat landscape, it is always better to err on the side of caution. Leaders should foster a culture where potential incidents are reported promptly. There is no penalty for a report made in good faith that later turns out to be a false alarm. Early notification allows for rapid assessment and is a hallmark of a mature and responsible organisation. Hesitation can cost valuable time; proactive communication strengthens our collective defence.

The Leader's Action Protocol: The Critical First Hours

The **Cyber Security (Notification of Cyber Security Incident) Regulations 2024 [P.U.(A) 220/2024]** mandates a three-stage notification period for NCII entities. In a crisis, this structure provides clarity and ensures a response that is both swift and thorough.

Stage 1: Immediate Notification

Upon detecting a potential cyber security incident, your first action is to notify **NACSA immediately** by electronic means. This can be done via e-mail to **cert@nc4.gov.my** or through the official NACSA portal at https://www.nc4.gov.my. This first alert triggers the national response mechanism.

Stage 2: The 6-Hour Detailed Report

Within six hours of the initial discovery, a more detailed report must be submitted to NACSA. This report is critical for initial situational awareness. Use the following checklist to ensure you provide all legally required information:

Initial Notification Action Checklist (To Be Completed Within 6 Hours of Discovery)

[ ] Identify the Reporting Officer:
Provide the particulars of the authorized person making the report.

[ ] Identify Your Entity:
Provide the particulars of your NCII entity, its NCII sector, and the relevant NCII sector lead.

[ ] Describe the Incident:

- State the type and description of the incident (e.g., Ransomware, Data Leak).
- State the severity of the cyber security incident.
- Note the date and time the cyber security incident was known to have occurred.
- Note the method of discovery of the cyber security incident.

Stage 3: The 14-Day Supplementary Report
Within fourteen days of the **initial notification, a comprehensive supplementary report** is required. This report must provide to the fullest extent practicable the following supplementary information:

(a) the particulars of the NCII affected by the cyber security incident;
(b) the estimated number of host affected by the cyber security incident;
(c) the particulars of the cyber security threat actor;
(d) the artifacts related to the cyber security incident;
(e) the information on any incident relating to, and the manner in which such incident relates to, the cyber security incident;
(f) the particulars of the tactics, techniques and procedures of the cyber security incident;
(g) the impact of the cyber security incident on the NCII or any computer or interconnected computer system; and
(h) the action taken.

Proactive Readiness: A Universal Business Imperative

While Act 854 places specific legal mandates on NCII entities, the principles of proactive readiness are universal. For any business, including SMEs, preparing for a cyber security incident before it occurs is the most effective way to protect your profits, reputation, and customer trust. A well-prepared organisation can significantly reduce the financial and operational impact of an attack.

Leadership Accountability, Not Just an IT Task

Ultimate responsibility for cybersecurity rests with the organisation's leadership. Act 854, under **Section 58,** stipulates that where any person who commits an offence under Act 854 is a company, limited liability partnership, firm, society, or other body of persons, a person who at the time of the commission of the offence was a director, compliance officer, partner manager, secretary and other similar officer of the company, limited liability partnership, firm, society, or other body of persons or was purporting to act in the capacity or was in any manner or to any extent responsible for the management of any of the affairs of the company, limited liability partnership, firm, society, or other body of persons can be held personally liable for offences committed by the entity.

This provision underscores a critical point: cyber security oversight is a core function of corporate governance.

Assessing Your Readiness: Applying the Rose, Bud, Thorn Framework

To translate this responsibility into action, leaders of any organisation can use the **Rose, Bud, Thorn** methodology from Chapter 3 to assess their incident response capabilities. This simple, practical exercise helps identify strengths and weaknesses in your current plan.

- **Rose (What is going well?):**
  "We conduct regular backups of our critical data."
  "Our employees know who to report a suspicious email to."

- **Bud (What are the areas for improvement?):**
  "We could formalise our incident response plan in writing."
  "Our team could be better trained on the specific reporting window to ensure we can meet the deadline."

- **Thorn (What are our limitations or challenges?):**
  "We lack the in-house expertise to conduct a detailed forensic investigation after a breach."
  "The potential cost of business interruption is high, and we have not quantified it."

Mandatory Proactive Duties for NCIIs

Beyond best practices, NCII entities have legally mandated proactive duties under the **Cyber Security (Period for Cyber Security Risk Assessment and Audit) Regulations 2024 [P.U. (A) 219/2024].** These NCII entities are required to:

- Conduct a comprehensive cyber security risk assessment at least **once a year.**

- Carry out a cyber security audit at least **once every two years,** or at a higher frequency if directed by the Chief Executive of NACSA.

Conclusion: A Unified Effort for a Resilient Nation

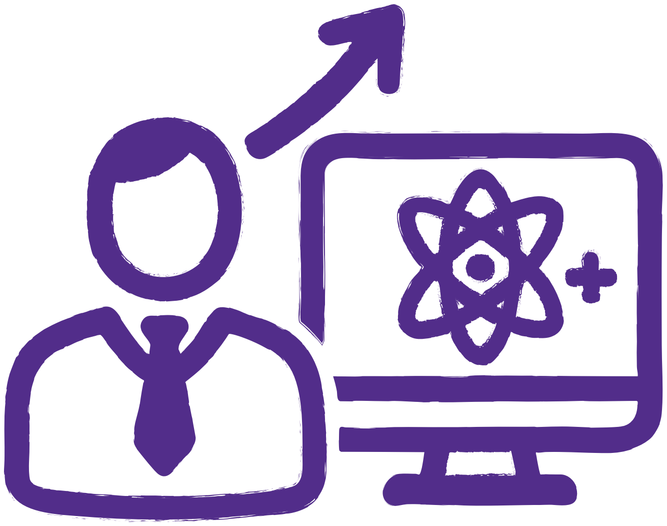
Navigating Malaysia's Cyber Security Act 2024 is more than a compliance exercise; it is an act of corporate responsibility and a vital contribution to our nation's security.

A swift, structured, and compliant response to a cyber security incident protects your organisation while enabling a coordinated, national effort to defend against cyber security threats.

This is the essence of the **unified whole-of-government, whole-of-nation, and internationally coordinated approach, built on strong public-private partnership** that we must foster.

By understanding your duties and preparing your response protocols, every business leader—from the largest NCII entity to the smallest enterprise—plays a role in strengthening our collective digital ecosystem.

The guidance in this book is a key part of that effort, and it is a precursor to the full national strategy, **Malaysia Cyber Security Strategy (MCSS) 2025-2030.**



CHAPTER

06

A Leader's Guide to the Post-Quantum Era

Future-Proofing Our Digital Sovereignty: A Leader's Guide to the Post-Quantum Era

By: Professor Dr. Muhammad Rezal Bin Kamel Ariffin

Introduction: The Urgent Journey

Embarking on the study of a new technology is much like being an explorer preparing for a journey into an unknown region. It requires a disciplined mind, an understanding of the landscape, and the right set of tools. The transition to Post-Quantum Cryptography (PQC) is such a journey, and for today's leaders, it is no longer optional—it is an urgent and necessary expedition.

The urgency is driven by a clear and present threat known as a **"Harvest Now, Decrypt Later" (HNDL)** attack. Sophisticated adversaries are actively infiltrating systems today to steal encrypted data. They cannot break the encryption now, but they are stockpiling this information with the expectation that a sufficiently powerful quantum computer will be able to decrypt it in the future.

This threat is not limited to **the National Critical Information Infrastructure (NCII) entities** that protect our most vital services. It is a direct risk to **any enterprise with "evergreen data"**—information that must remain confidential for many years. This includes your long-term intellectual property, trade secrets, financial models, research data, and strategic plans. The security protecting your most valuable "Crown Jewels" has an expiration date, and the journey to a secure future must begin today.

The Quantum Threat Explained

For decades, we have relied on two main families of cryptography. First, **asymmetric cryptography,** such as RSA and Elliptic Curve Cryptography (ECC), which uses the public-private key approach. It is designed for public functions such as digital signatures and key exchange. On the other hand, **symmetric**

cryptography, like the Advanced Encryption Standard (AES), uses a single secret key for encrypting data. The security of asymmetric cryptography is based on mathematical problems that are practically impossible for even the most powerful classical computers to solve. While the security of symmetric cryptography (among others) hinges upon the length of the secret key that is sufficient to ensure confusion and diffusion of the ciphertext produced from the plaintext.

A quantum computer, however, operates on entirely different principles and is armed with specific algorithms that target the foundations of our current security:

- **Shor's Algorithm:**
  This is the most significant threat to our public-key infrastructure. Shor's Algorithm is specifically designed to solve the two core mathematical problems that underpin asymmetric cryptography: factoring large numbers (which breaks RSA) and calculating discrete logarithms (which breaks ECC). A sufficiently powerful quantum computer running this algorithm will render our current methods for digital signatures and secure key exchange obsolete.

- **Grover's Algorithm:**
  This algorithm targets symmetric encryption. While it does not "break" it in the same way Shor's does, it dramatically speeds up brute-force attacks used to guess a secret key. It effectively halves the security strength, meaning a 128-bit AES key becomes as vulnerable as a 64-bit key, and a 256-bit key offers the protection of a 128-bit key. While the immediate defence is to double key lengths (e.g., using AES-256), it demonstrates that no part of our cryptographic toolkit is unaffected.

The combined power of these algorithms means the encrypted data harvested today will become an open book tomorrow. This fundamental shift requires a new generation of defensive tools.

The Solution: Post-Quantum Cryptography (PQC)

Post-Quantum Cryptography is the development of new cryptographic algorithms that are secure against attacks from both classical and future quantum computers. The global cryptography community, led by institutions like the U.S. National Institute of Standards and Technology (NIST), has been working for years to develop and standardize these new methods.

The goal is not simply to create theoretically secure algorithms, but to produce a set of tools that are practical, efficient, and can be implemented in the real world. This requires a deep focus on creating solutions that meet the demanding needs of modern digital systems.

A Malaysian Innovation: The Practical Value of KAZ family of algorithms

As part of this global effort, academicians in Malaysia aspires to put forward ideas for the potential usage for ensuring digital security in the quantum computer era. Understanding the need for seamless replacement and not to interrupt current user experience, the KAZ (Kriptografi Atasi Zarah – Cryptography Overcoming the Particles) family of algorithms are put forward. KAZ family of algorithms, has not been fully analyzed (even in Malaysia).

At the time of printing, it has been submitted to Malaysia's National Trusted Cryptography Algorithm List (MySEAL) exercise for evaluation.

KAZ family of algorithms are the:

- KAZ Key Encapsulation (KAZ-KEM)
- KAZ Key Agreement (KAZ-KA)
- KAZ Digital Signature (KAZ-SIGN)

Innovations within KAZ family of algorithms are:

Efficiency: Short Keys and Ciphertexts and Signatures.
A major challenge in PQC is that many algorithms require very large keys or signatures, making them impractical for systems with limited memory or bandwidth like smart cards, passports, and IoT devices. The KAZ family of algorithms is designed to provide robust PQC security with key and ciphertext or signature sizes that are significantly smaller than many alternatives, making it more efficient and versatile.

Performance: Speed and Simplicity.
The underlying mathematics of the KAZ family of algorithms are designed for high performance, allowing for fast key generation, encapsulation, decapsulation, signing, and verification. This is essential for high-throughput systems, such as financial transaction networks, where speed cannot be compromised.

Ease of Integration: A "Drop-in" Replacement.
Acknowledging that migration is a significant business cost, KAZ family of algorithms is designed as a potential "seamless drop-in replacement" for currently used encryption/signature schemes. This focus on ease of integration aims to lower the barrier to adoption for businesses and government agencies, reducing the need for radical and expensive re-engineering of their systems.

Proposed Security Foundation:
To use "simple" mathematics to achieve maximum simplicity in design, such that even practitioners with limited mathematical background will be able to understand the arithmetic

A Leader's Call to Action: The Journey's First Steps

Preparing for the quantum era is not merely a future technical upgrade; it is a strategic business decision that must be integrated into the **business goals** you identified in Chapter 2. Your PQC migration plan is itself a critical **IT asset** that must be developed and protected. As we established in Chapter 4E, protecting your **Data** is paramount, and PQC is the next frontier of that responsibility.

The transition to PQC is a marathon, not a sprint. As a leader, you can begin this essential journey today with three practical steps:

1. **Inventory Your "Evergreen" Data.**
   The most critical first step is to understand what you need to protect. As part of your data classification efforts, ask the question: "What data, if decrypted in 10 or 20 years, would cause significant harm to our business or national security?" This inventory of your most sensitive long-term assets defines the scope and priority of your PQC migration.

2. **Engage with Your Technology Partners.**
   Begin a dialogue with your key software and hardware vendors. Ask them about their PQC roadmaps and their plans for crypto-agility—the ability for their systems to be updated with new cryptographic standards as they become available. This is a crucial aspect of managing the risk within your supply chain.

3. **Champion National Innovation.**
   Support the development of a sovereign PQC ecosystem. By embracing homegrown solutions and fostering local expertise, you not only secure your own organisation but also contribute to Malaysia's long-term digital sovereignty.

By starting this journey now, with a clear understanding of the threats and a methodical plan, you can ensure your organisation's resilience and play a vital role in securing our nation's digital future.

CHAPTER

07

Creating the Bridge between Business and Cybersecurity

Creating the Bridge between Business and Cybersecurity

This book has been written with a simple, practical mission: **to bridge the gap between business goals and cybersecurity practices.** We recognise that for many business leaders and operators, cybersecurity can seem like a daunting, highly technical field filled with jargon, complex frameworks, and endless product pitches. Similarly, cybersecurity practitioners often struggle to communicate the value and urgency of their work in terms that resonate with business priorities.

However, the truth is that business goals and cybersecurity goals are never mutually exclusive – at the end of the day, **cybersecurity is here to protect your business and ensure that your business goals are achieved with little to no worries.**

Our goal with the **Practical Cyber Framework** and this book is to make cybersecurity accessible and actionable for both sides of this equation—**to help business leaders better understand the impact of cybersecurity on their operations and goals, and to help cybersecurity professionals align their efforts with business objectives.**

In short, this framework aims to build a shared language, a common ground where decisions can be made with clarity, purpose, and mutual understanding.

It is a long-term project where this book and the Practical Cyber Framework are but the first of the series and we would love to have the support of anyone who is interested in utilising and expanding on it!

An Invitation to Use, Adapt, and Share

Cybersecurity is not a one-size-fits-all solution. Every business faces unique risks and challenges based on its size, industry, and digital footprint.

That's why we designed the **Practical Cyber Framework** to be flexible, scalable, and adaptable. We encourage you to **use**

it in your organisation, or for your clients, adapt it to fit your specific needs, and share your experiences with us.

If you choose to use the framework, we simply ask that you **credit the Practical Cyber Framework** and **link back to our GitHub** so that others can benefit from it too.

Our goal is to make cybersecurity **as easy to understand and apply as possible,** and we want to continuously improve the framework based on real-world experiences.

Learning from Your Stories: Successes and Failures

We believe that the best way to improve this framework is by learning from those who use it. We want to hear your stories**—both successes and failures—**about how the **Practical Cyber Framework** has impacted your cybersecurity posture.

- **What worked well for you?**
- **Where did you encounter challenges?**
- **How did the framework help you align cybersecurity with your business goals?**
- **What improvements would you suggest?**

Your stories can help us refine and evolve the framework to better meet the needs of organisations across industries and regions. Cybersecurity is a continuously evolving field, and we are committed to keeping this framework relevant, practical, and impactful.

Building a More Secure Future, Together

The world is becoming more connected, and with that connectivity comes increased risk.

Cybersecurity is not just a technical problem—it's a business challenge that affects **profitability, sustainability, and reputation.**

By adopting the principles outlined in this book, we hope you'll see that **cybersecurity can be a driver of business resilience and growth**, not just a cost centre or compliance checklist.

Ultimately, **cybersecurity is about people.** It's about protecting your employees, customers, partners, and the communities you serve. It's about ensuring that your business can continue to thrive in an ever-evolving digital landscape.

Together, let's build a more secure future—**one conversation, one business, one framework at a time.**

Thank you for being part of this journey.

We look forward to hearing your stories and continuing to improve the Practical Cyber Framework with your insights and experiences. **Let's work together to make cybersecurity practical, achievable, and sustainable for all.**

Join the conversation:

- **Credit us:**
  Practical Cyber Framework

- **GitHub:**
  https://github.com/practicalcyber/practical-cyber-security-decisions

- **Reach out:**
  We are always eager to engage, learn, and grow with you. Share your feedback, stories, and insights at book@practical-cyber.com

  Let us improve cybersecurity together.

About the First Edition Co-Authors

The first edition of this book was made possible through the collaborative effort of several industry experts,

Daniel Goh

Daniel Goh is a seasoned cybersecurity professional and the founder of ATET Security, established in 2019 with the mission to make cybersecurity practical and affordable for all companies. He began his cybersecurity career with the Singapore Infocomm Technology Security Authority (SITSA), focusing on safeguarding the nation's information infrastructure.

In 2013, Daniel joined the Civil Aviation Authority of Singapore (CAAS), where he played a pivotal role in developing the Aviation Sector's cybersecurity strategy. He integrated cyber elements into the aviation regulator's crisis management plan and co-authored the article "Aviation Cyber Security: A New Security Landscape" in the Journal of Aviation Management in 2014.

Daniel also contributed to the Critical Information Infrastructure Protection (CIIP) programme, conducting inaugural Operational Technology Security assessments across various industries. Additionally, he spent several years with ST Electronics, integrating and securing large-scale military systems.

Courtney Guss

Courtney Guss is a seasoned cybersecurity leader with deep expertise in Governance, Risk, and Compliance (GRC) and cyber risk quantification.

As the Director of Strategic Alliances at Immersive Labs, she helps organizations fortify their cyber resilience through innovative upskilling strategies and crisis preparedness exercising. Previously, she served as a Senior Consultant at IBM Security, where she guided enterprises in applying the FAIR framework to quantify and prioritize cybersecurity risks.

Courtney's insights into risk management and cybersecurity maturity models have made her a sought-after speaker, including at industry events like FAIRCON21. With a proven track record in helping organizations navigate complex security landscapes, she is a trusted voice in cyber risk and resilience strategy.

Umesh Patel

Umesh Patel, a seasoned Cybersecurity Leader with a proven global track record in delivering robust IT risk management and security solutions across Compliance, Governance, Technology Risk Management and Data Privacy. Currently working for an online Travel Start-up specializing in securing enterprise technology systems, establishing end-to-end frameworks like Third-Party Risk Management. He has experience with ETRM and Finance systems, complex infrastructure and cloud environments, with expertise in ISO27001, PCI DSS and NIST SP 800-53.

Experienced in managing globally dispersed, agile delivery teams and leading organizational change within fast-paced, hyperscale environments. A proven track record in building security frameworks, cultivating stakeholder buy-in at the senior leadership level, and fostering partnerships with delivery teams to create a results-driven culture.

Deepak Talwar

Deepak Talwar is a distinguished leader with 24 years of expertise in cybersecurity, Artificial Intelligence, and national security. At Microsoft, he collaborated with governments, customers, and partners to build trust in cloud adoption and secure critical infrastructure.

At Dell, he drove AI and cyber readiness initiatives for partners, fostering an ecosystem of innovation and resilience.

At Symantec, he scaled the cloud security business, and at EY, he led business development by integrating advanced technologies with strategic solutions for global challenges.

As a recognized cybersecurity leader, AI visionary, and author, Deepak's work reflects a deep understanding of practical applications in the field. His extensive experience played a pivotal role in shaping his contributions to the book Practical Cyber, where he bridges the gap between strategy and execution in cybersecurity. With a unique ability to align technology with business goals, he is celebrated for delivering innovation, resilience, and sustainable growth in an increasingly digital world.

Donavan Cheah

Donavan Cheah has had more than eight years of experience in cybersecurity after successfully pivoting from an undergraduate degree in Physics.

He currently consults for a wide range of customers for advisory services such as governance, risk and compliance, threat modelling as well as penetration testing services. He has also built up a threat modelling practice in his previous role and has built a cybersecurity gamification experience where players can understand cybersecurity through role-play.

He has spoken at numerous conferences regionally, such as Japan's largest CTF, SECCON. He has also been on the advisory board of a conference in India, VulnCon, since 2024.

Donavan also volunteers with Division Zero (Div0) and ISACA. He contributes to the next generation through training as well, such as through his threat modelling workshops at the Global Cybersecurity Camp 2025 in Taiwan, Seasides Goa as well as OT Security workshops with Div0.

He also has an active mentorship practice, mentoring younger generations of cybersecurity professionals from all around the world.

Prologue by
Emil Tan

Emil Tan is the founder and leader of Division Zero (Div0)—Singapore's largest techno-centric cybersecurity community—dedicated to fostering collaboration among professionals, researchers, and enthusiasts. He is also a Cyber Strategist and Market Lead in Critical Infrastructure at Booz Allen Hamilton, where he drives strategic cybersecurity initiatives.

Beyond Div0, he founded Infosec In the City, SINCON, Singapore's international techno-centric cybersecurity conference, and leads the Singapore Chapter of The Honeynet Project. He also serves on the CREST Asia Council, and the Singapore Computer Society (SCS) Cybersecurity Chapter.

With over a decade of experience across cybersecurity R&D, operations, governance, policy and regulation, and consultancy, he has received accolades including the inaugural Cybersecurity Awards (Professional Category) in 2018 and the Ministry of Communications and Information (MCI)'s Special Recognition Award in 2023. In 2024, he was named among Tatler's Gen.T Leaders of Tomorrow.

Published by:
Verixiom Pte. Ltd.

National Cyber Security Agency
(NACSA)

Malaysia Cryptology Technology
and Management Centre