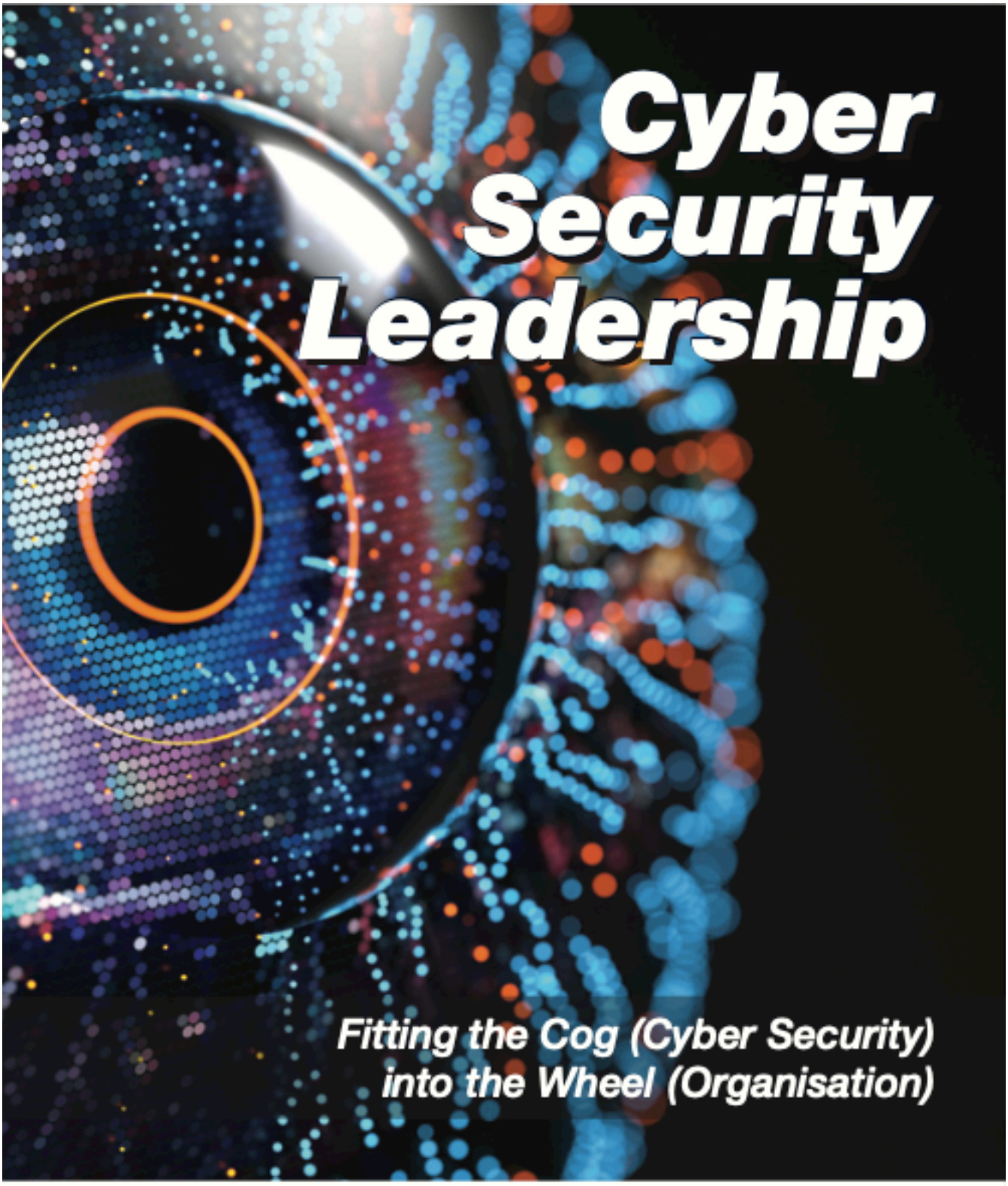

Cyber Security Leadership

Fitting the Cog (Cyber Security) into the Wheel (Organisation)

VOLUME 2
AMPA PUBLICATIONS SERIES

Dr Monjur Ahmed

AMPA
ACADEMY OF MUSIC AND PERFORMING ARTS

Cyber Security Leadership

FITTING THE COG (CYBER SECURITY) INTO THE WHEEL (ORGANISATION)

Dr Monjur Ahmed

Melbourne, Australia

AMPA Publications/- Intertype Publish and Print
U45, 125 Highbury Road
BURWOOD VIC 3125
www.intertype.com.au

Ordering Information:
Quantity sales. Special discounts are available on quantity purchases by corporations, associations, and others. For details, contact the "Special Sales Department" at the address above.

Cyber Security Leadership / GJW Consulting. —1st ed.
ISBN 978-1-7640856-4-9

Contents

CHAPTER 1

Introduction

Cyber Security Leadership is crucial to understand the importance of thoughtfulness in Cyber Security practice.

Prelude

This book delves into the realm of Cyber Security leadership within organisations, aligning with its subtitle's focus on seamlessly integrating Cyber Security into the organisational structure. Its primary objective is to present leadership principles in Cyber Security in a clear and straightforward manner. Serving as a practical checklist, the discussion in this book covers essential aspects that Cyber Security leaders should consider. The term 'Cyber Security Leader' encompasses individuals responsible for guiding Cyber Security efforts within an organisation, such as the Chief Information Security Officer (CISO), Head of Cyber Security or Cyber Security Lead.

Motivation

Cyber Security isn't just an IS/IT concern; it's fundamentally a business matter. Responsibility for Cyber Security doesn't

solely rest with the Cyber Security team; it's a shared responsibility [1] across the entire organisation. Cybersecurity extends beyond merely installing firewalls or antivirus soft- ware. The roles and responsibilities related to cybersecurity aren't globally standardised yet, and there may be a lack of clear definitions of Cyber Security roles within a Cyber Security team. The interconnectedness between an organisation and its Cyber Security might not be fully appreciated or understood to date, leading organisations to grapple with the aftermath of cyberattacks. These factors motivate the writing of this book - its aim is to address these issues and present a clear, concise understanding of what cybersecurity leadership means within an organisation.

Target Audience

This book could prove advantageous for individuals in leadership roles within an organisation's Cyber Security domain. Those aspiring to become Cyber Security leaders or currently progressing along that path, driven by passion and ambition, could also derive value from its contents. Consultants guiding organisations in enhancing their Cyber posture may also find this book to be a valuable resource. Additionally, students enrolled in Cyber Security programmes, especially those emphasising strategic and leadership dimensions, could enhance their understanding through the insights offered in this book.

What this book is (and is not) about?

This book is (to some extent) a non-exhaustive checklist for a Cyber Security leader. This book helps one to understand what the role of a Cyber Security leader is. This book is not about how to do what needs to be done by a Cyber Security leader. Thus, this book is on 'what' of Cyber Security leadership, not 'how'. As an example, this book recommends 'risk

management' to be part of a Cyber Security leader's dish, but this book does not suggest how to carry out risk management practices by using what kind of risk management framework.

This book does not elaborate on technical and Cyber Security jargons; the expectation is that the readers are already familiar with or motivated to familiarise (through other resources) with the technical and Cyber Security jargons used in this book. For example, this book mentions 'Patch Management' as one of the 'menu items', but does not explain what a patch management is, to avoid deviating from the focus and scope of this book.

Structure of this Book

This book is divided into four parts - each of these parts form a chapter in this book. The four parts are the domains that a Cyber Security leader does not afford to avoid, these are:

- Strategy
- People
- Governance, Risk and Compliance (GRC)
- Technology

Figure 1.1 provides a birds-eye view of the structure of this book.

Cyber Security Leader

This book is for aspiring Cyber Security leaders. This book may be considered as a starting point and overview of checklist for a Cyber Security leader. Before we close this chapter, let's define Cyber Security leader. In this book, the term 'Cyber Security leader' refer to the role(s) that is/oversee the Cyber Security unit of an organisation and thus a bridge between the organisation and the Cyber Security team. A Cyber Security leader speaks three organisational languages - Business, IS/IT, and of course, Cyber Security. A Cyber Security leader ensures

the Cyber Security becomes and remains an effective business enabler.

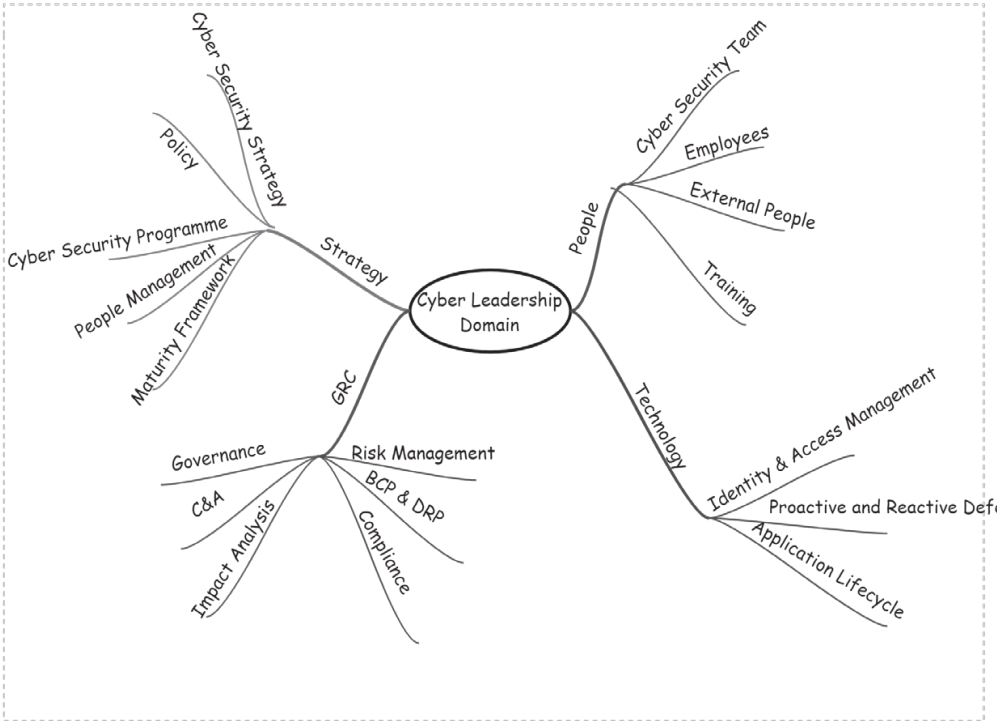

Figure 1.1: Cyber Leadership Domains - Structure of this Book

CHAPTER 2

Strategy

Cyber Security is a Business issue, not IT/IS issue; everyone in an organisation is responsible for Cyber Security, the Cyber Security team is there to (mostly) prescribe best practices.

Prelude

In this chapter, we look into the Cyber Security strategy for an organisation followed by the ins and out of a Cyber Security programme. Cyber Security related policy as well as their importance and space within the context of Cyber Security is also explored.

Readiness Maturity

Even before we move into talking about Cyber Security, we first need to take a look into an overlooked pre-requisite of successful Cyber posture - that is, Readiness Maturity of an organisation to embrace a culture of fostering and improving Cyber posture in course of time. The author proposes the concept of Cyber Security Readiness Maturity (CSRM) in this chapter.

What is Readiness Maturity?

If an organisation cares about Cyber Security, it should dream of putting Cyber Security best practices in place, improve Cyber posture and be Cyber resilient. But, without certain level of assurance, quality, commitment and preparation, trying to implement Cyber initiatives is nothing more than playing with fireballs while considering the fireball as a snowball. CSRM means whether an organisation is prepared and is a good ground to flourish Cyber Security best practices. The level of readiness defines the level of maturity.

Why CSRM?

If an organisation does not have readiness maturity, it may create more chaos than resilience when it tries out 'Cyber Security'. An organisation without CSRM is just like a car driver without any driving experience and without a driver's license. Without CSRM, trying out Cyber initiatives may in fact make an organisation more vulnerable to Cyber-attacks and breaches. Trying to improve Cyber posture without considering CSRM is like trying an activity at home that is labelled as 'do not try at home'.

Elements of CSRM

How do we measure an organisation's CSRM? To the best of the author's knowledge, there is no established model on this to date. However, there are some factors and aspects that, upon exploring, an organisation may be able to determine its Cyber Security readiness maturity level. The following is a non-exhaustive list of factors that may help determine an organisation's Cyber Security Readiness Maturity:

- Governance: If an organisation does not have good and clear governance in place, Cyber Security practice cannot be standardised within an organisation.

- Sponsorship: Senior Management sponsorship is a defining factor for an organisation's Cyber readiness maturity. If such sponsorship is not in place, or not in place properly, Cyber maturity initiatives are highly likely to mess up.
- Budget: Enough budget is crucial, if an organisation does not have enough budget or does not have the mindset to spend enough money for Cyber Security, it then has low readiness maturity.
- Team Size: Cyber Security is an umbrella topic. A Cyber Security team needs diverse skillset and all skillsets may not be expected from a couple of personnel.
- Cyber Realisation: The less the realisation the lower the maturity - it's the realisation on the importance of Cyber Security within an organisation.
- Cyber Team Realisation: Cyber Security team is not solely responsible to protect an organisation - they are merely there to prescribe best practices. The closer an organisation in acknowledging the above theme, the better readiness maturity that organisation has.
- Reporting Line: The Cyber Security reporting line plays a crucial role in Cyber Security practices within an organisation. The reporting structure of the Cyber Security to the business/organisation is an indicator of the level of Cyber Security maturity, as well as on the transparency and whether Cyber Security is prone to subjective bias and/or C-level corruption - Figure 2.1 is a self-explanatory illustration on this.

The above is a suggested list of elements of CSRM, not a quantified CSRM framework. An organisation needs to develop or adopt a CSRM framework to determine its CSRM level.

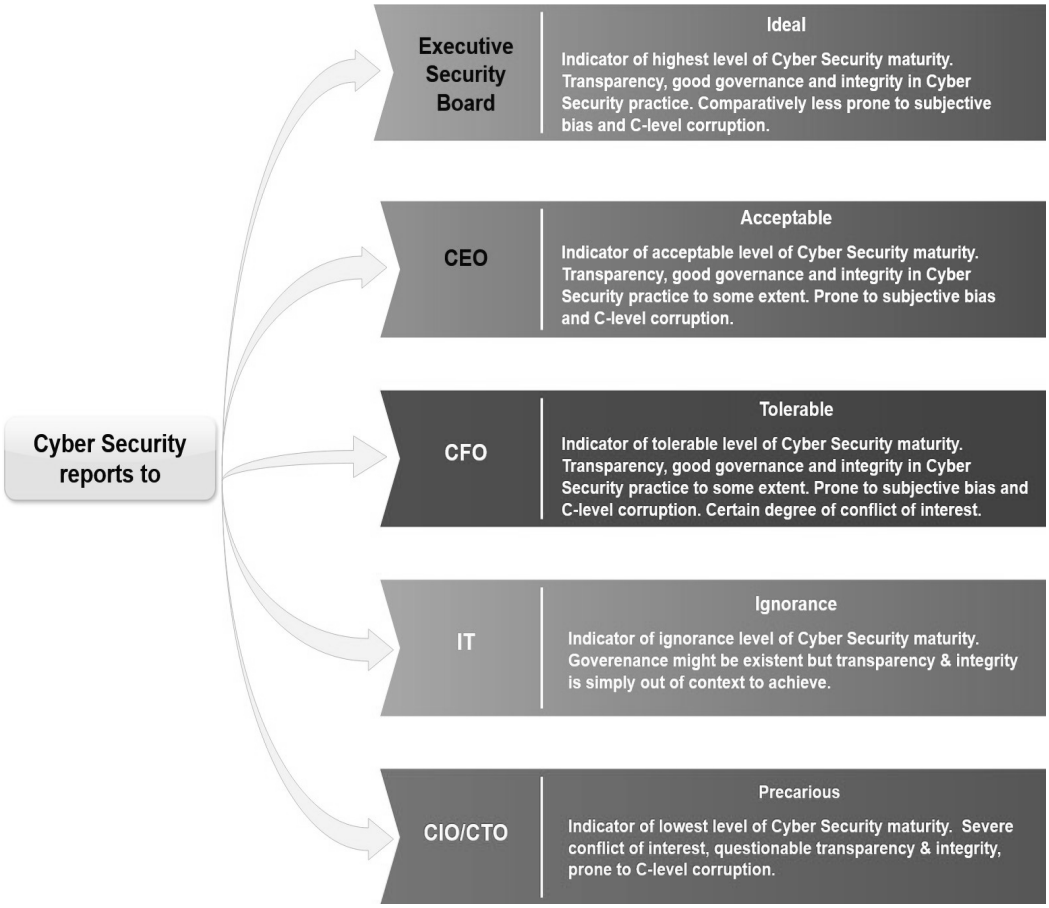

Figure 2.1: Cyber Security Maturity vs. Reporting Line

Cyber Security Strategy

The starting point of a Cyber Security journey for an organization, is to start with having a Cyber Security strategy. Cyber Security strategy is a crucial component as evident from research for example [2], [3] and [4]. It is an overarching document that outlines how an organization is going to deal with Cyber Security, what are the overarching strategies that the organization is going to follow, and how people, GRC, and technology part of Cyber Security are to be implemented within the organisation. When we talk about Cyber Security strategy, we mean what an organization is aiming to achieve from both Cyber Security perspective and Cyber Security maturity perspective. A Cyber Security strategy answers ‘what’ rather

than 'how'. For example, a Cyber Security strategy informs the organisation on how it visions to achieve Cyber maturity over a specific course of time and using technologies by implementing governance, for example having proper risk management Practices in place. It is very crucial to have a Cyber Security strategy for an organisation.

Since a Cyber Security strategy is an overarching document, it does not necessarily need to be specific. For example, a Cyber Security strategy mentions what will be monitored but not how they will be monitored, not specifically mentioning any tool. However, in strategy it might talk about specific frameworks, to give a reference point when it comes to achieving Cyber Security maturity. Example of such frameworks are ISO27001 [5], NIST [6], OCTAVE [7] just to name a few.

Policy

A Cyber Security leader needs to ensure the relevant policies are in place and enforced. The depth, breadth and importance of Cyber security policies are evident in practice, one such example is [8]. It is crucial to distinguish between IT policies and Cyber Security policies yet marry these together to ensure any IT aspects do not fall outside the radar of Cyber Security. Policies should be simple to read, and without excessive technical jargons - policies are written for everyone in the organisation, not just for IS/IT and Cyber Security department.

Project & Programme Management

To improve Cyber posture or the Cyber Security maturity, an organisation needs to have a specific goal with timeline which we call the Cyber Security programme. A Cyber Security leader needs to be aware on the requirements and importance of a Cyber Security Programme to actualise the identified Cyber Security project. Once an organisation has its Cyber Se-

curity strategy formulated, it's time to focus on developing a Cyber Security program. A Cyber Security program outlines the projects that needs to be carried out for an organisation to be Cyber mature. To develop a Cyber Security programme, it is important for an organisation to know its current state of maturity which could be 'zero' to 'some'; an organisation may have some maturity or may have no maturity at all. Whatever is the scenario, an organisation needs to know the current level of maturity as the starting point to design and develop a Cyber Security program. And to do that. The first activity that needs to be done for to develop a Cyber Security program is a gap analysis. A gap analysis simply means this: what is the target maturity (point B) and what is the current maturity level (point A), and how to go from point A to point B. So, when a gap analysis is carried out, an organisation knows its level of maturity whether it's low or high, and then it can realise what needs to be done to reach to the targeted level of maturity. The output from a gap analysis is what we can call the requirements of the projects that needs to be done as part of Cyber Security programme.

Referring to [9], [10] and [11], Cyber Security programme and project identification, development and management requires proper and strategic approach and planning.

People Management

A Cyber Security leader is to lead a team of people who are Cyber Security professionals. This fact makes it imperative that a Cyber Security leader has people management skills. This is no different than any other team where people management is required. Subject matter expertise alone is far from total requirement to succeed in a Cyber Security leadership role. People management skill is a generic skill that is required by any leader, and this is no exception for a Cyber Security leader too.

Cyber Maturity Framework

One of the aims of such Cyber Security programme that we have discussed earlier is to have a vision of in improving Cyber maturity over time. Now the question comes: which Cyber Security maturity framework to use? There are two options: the first is to use any specific framework and the second is to use a customised ad-hoc framework adopted to suit for the organisation. I would vote for an ad-hoc framework instead of using a specific framework blindly and regardless.

Any Cyber Security maturity framework that is readily available maybe too narrow or too broad for the specific context of an organisation. For ex- ample, an off-the-shelf framework may not address Cyber Physical Systems (CPS) security, but if an organisation deals with CPS then an off-the-shelf framework may not be adequate improve Cyber Security maturity of that organisation; it may be required to look into multiple frameworks to customise one framework capable of addressing specific needs of the organisation to help achieve Cyber maturity.

Risk-based Maturity

As discussed earlier, an ad hoc framework could be the best solution for an organisation to follow. The author recommends adopting a risk-based maturity approach. In a risk-based maturity approach, an organisation tends to find all the risks associated/incorporated from Cyber Security point-of- view and builds a programme that includes projects to mitigate the risks identified, resulting in improving maturity or Cyber posture of an organisation over time. A risk-based approach helps to improve Cyber maturity faster by focusing only on the aspects within the organisation that requires attention. On the other hand, following a generic framework might be over ambitious. At the same time, a generic framework might include redun-

dant components not applicable/required for an organisation that, if adopted, may lead to wasting time, effort and resources after aspects that are not crucial for the organisation to improve its Cyber posture.

Risk-based approach to Cyber Security maturity is highlighted in research and discussions for example in [12, 13, 14, 15] .

Cyber Security Maturity Life Cycle

The aim of achieving improved Cyber Security maturity cannot succeed either with no planning or with ad-hoc, on-demand silo-style implementation. The process of Cyber Security maturity is not one-off; it must be considered as iterative and ongoing. Thus, it needs proper planning, implementation, monitoring, review and continuous improvement. Figure 2.2 presents a framework on Cyber Security maturity life cycle - which is self-explanatory from the illustration in addition to discussion incorporated throughout this book.

Figure 2.2: Cyber Security Maturity Life Cycle

Takeaways

Strategic planning is at the core of Cyber Security success. The technological operational part will be a mess if not built on a solid strategic foundation. For this part, reflecting to the discussion in this chapter, the key points as takeaways are:

- Cyber Security is a business issue, not just an IS/IT issue.
- Readiness maturity analysis is a crucial pre-Cyber step for an organisation.

- Cyber Security strategy and policy are the starting steps into the journey of Cyber Security maturity.
- Gap Analysis helps to determine the path towards Cyber Security maturity.
- People management framework is more crucial for a Cyber Security leader than subject matter expertise.
- A risk-based maturity approach helps an organisation to focus only on the crucial and required elements resulting in a faster improvement in Cyber posture.

CHAPTER 3

People

People are probably the most crucial, most sensitive and weakest element in Cyber Security.

Prelude

This chapter looks into people that are related to or tied into the context of Cyber Security in an organisation. Within the context of Cyber Security for any organisation, people play a very crucial and important role either directly or indirectly. The Cyber Security perspective of People includes not only the Cyber Security team but also all other people who are directly or indirectly connected to the organisation. Every single person directly/indirectly tied to an organisation has the potential to be an attack vector for security breaches. A Cyber Security team in an organisation must identify all the people that are directly or indirectly connected to an organisation – both internal and external people. People aspects in the Cyber Security domain has been given great attention to date, some of such examples are [16, 17, 18, 19, 20, 22].

People

Figure 3.1 illustrates the people that a Cyber Security team needs to take into account. Both external and internal people fall within the scope of Cyber Security. Referring to Figure 3.1, we mostly focus on the Cyber Security Team in this chapter.

Cyber Security Team

There may be two different perspectives to look at the Cyber Security team – the whole Cyber Security unit/department as the Cyber Security team or considering the Cyber Security unit as a department and outlining teams of the units based on work functions. We follow the latter approach in this book. The depth and breadth of a Cyber Security team is illustrated in Figure 3.2. The illustration in Figure 3.2 defines roles, not number of people. Depending on the size of an organisation, multiple roles may be carried out by one person, or one role might be occupied by multiple people. Figure 3.2 is to be considered as a non-exhaustive solution for guideline purpose only; and a Cyber Security Leader need to come up with the team structure suited for the organisation.

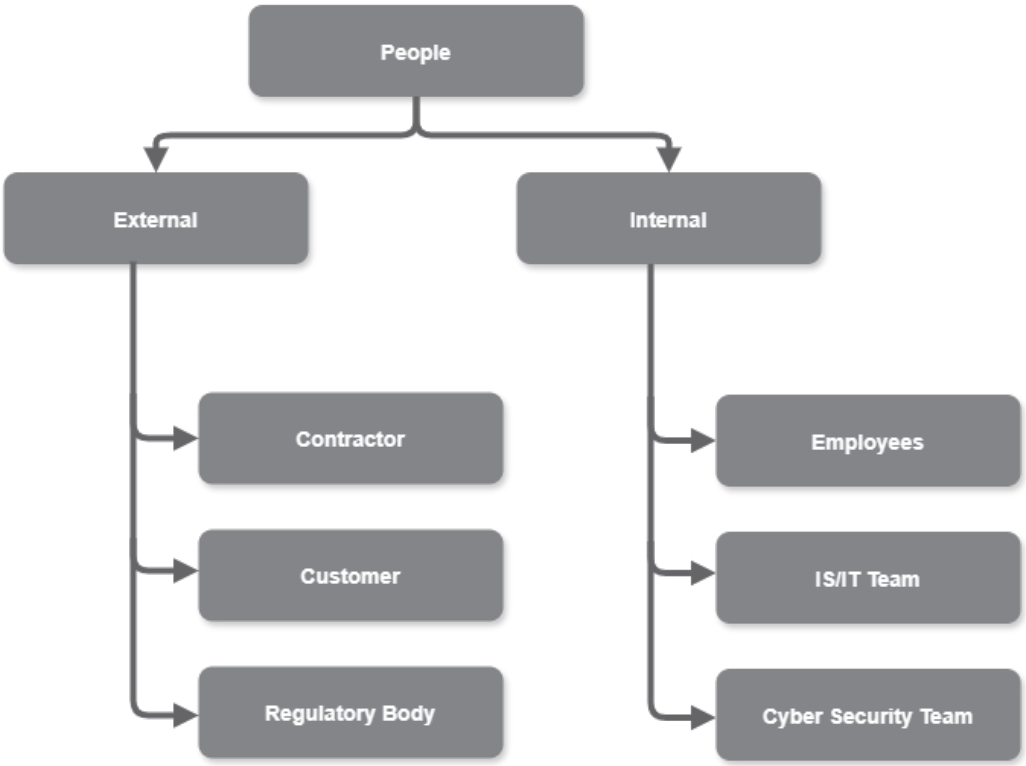

Figure 3.1: People within Cyber Security Context

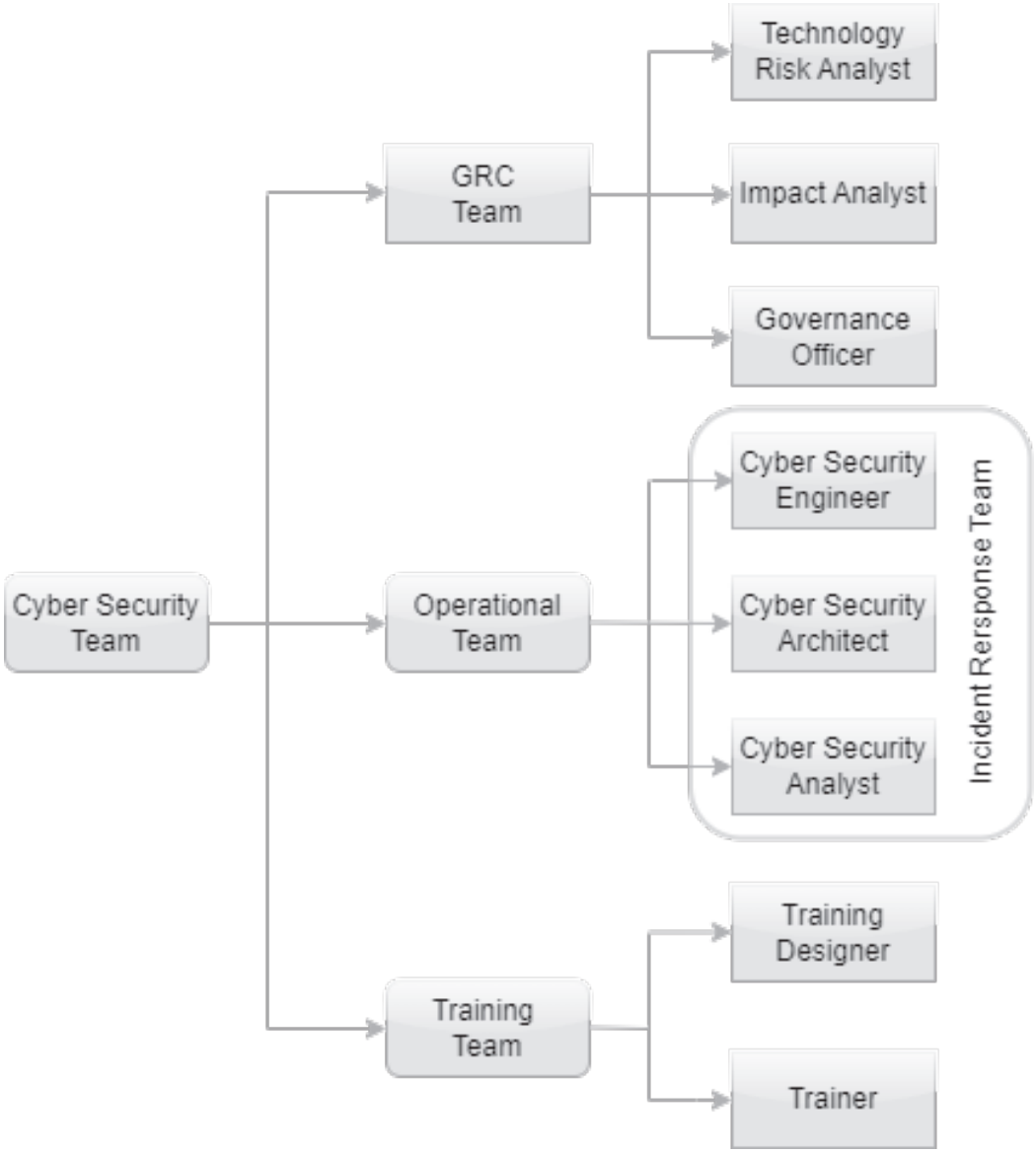

Figure 3.2: Cyber Security Team

For example, the role 'Privacy Officer' is not included in the above illustration but is a role that steps across Cyber Security realm. Whether this role should be part of the Cyber Security team is at discretion and organisation specific. While a small organisation may not have a dedicated Privacy Officer, large organisations may have an organisation wide Privacy Officer, not just for IT/IS and Cyber Security.

GRC Team

The main roles that a GRC team is made up of are Technology Risk Analyst, Impact Analyst and Governance Officer.

Technology Risk Analyst

Technology Risk Analysts look into the technologies used within organisation to ascertain the risks associated. This also applies when acquiring new system. The output from this role is input to risk management and governance.

Impact Analyst

Involves in various impact analysis, e.g., security impact analysis, business impact analysis, privacy impact analysis. The output from this role is input into governance, risk management as well as to the Operational Team.

Governance Officer

Governance Officer manages the governance of all Cyber Security aspects to ensure compliance. This is a rather complex role touching all aspects of Cyber Security and works closely with virtually the whole Cyber Security Team as well as the IS/IT team. Governance Officer may act as the representative of the Cyber Security Team to the Cyber Security Governance Committee.

Operational Team

The operational team looks after the real-time operational part of Cyber Security, guarding the doors! Typical roles in this team are Cyber Security Engineer, Cyber Security Architect, and Cyber Security Analyst. The operational team has a distinct feature that makes them another virtual team within the team - the Incident Response Team (IRT). We avoid exploring the anatomy of an Incident Response team to stick to the scope of this book. However, it is worth noting that the IRT may request

inclusion of any other role (from other sub-team of the Cyber Security team) into IRT either on an ad-hoc or ongoing basis.

Training Team

This is the team responsible for the training and awareness of Cyber Security for the entire organisation. This team looks after the Cyber Security Training & Awareness programme. This is the team that still probably does not exist in a lot of (if not most of) the cases; this is probably due to the lack of awareness of the importance (and the nature and aspects) of Cyber Security training and awareness. In our another book, we have discussed on Cyber Security Training and Awareness Programme [23].

Training Team is responsible for training Cyber Security awareness within the organisation – for both internal and external people. it is important to note that the training team is not necessarily part of Cyber Security team or subject matter expertise in Cyber Security. Rather, they are learning designers and trainers with expertise in instructional design and educating people. Thus, this team requires the subject matter expertise of other roles in a Cyber Security Team. It's crucial for any Cyber Security leader to note that the Cyber Security professionals maybe subject matter expert's but they are not necessarily trainers. It's crucial to seek expertise of instructional designers and qualified trainers who know the arts and science of training people.

Training Designer

Training Designers are instructional designers who define the logical lay- out and flow of the training materials of a Cyber Security Training & Aware- ness Programme. An expert to reflect the art and science of effective training design.

Trainer

Being a subject matter expert and teaching that subject matter are two very different things. A subject matter expert is not necessarily an expert trainer on the subject matter. A qualified and/or experienced Trainer finds the right approach to effectively train and educate people. They are expert in the art and science of pedagogy and training people effectively.

Employees

All employees of an organisation need to be taken into consideration by the Cyber Security team from two broad perspectives. All the employees of an organisation working in different departments needs to be identified and need to be trained on Cyber Security awareness. The reason is that, there are different types of Cyber-attacks applicable to different teams. For example, the People & Culture team may be targeted for one type of Cyber- attack where the Accounts department may be targeted for different kinds of scams or Cyber-attack. One important aspect not to miss is the employee on-boarding and off-boarding is done through Cyber Security filter. For example, when an employee leaves and an efficient & adequate off-boarding is not in place, the employee may be left with having access to organisational system even after they leave the organisation.

External People

It is crucial to identify external people who are not part of the organisation as employees, rather come from out of the organisation either as a customer or service providers. One prime example in this regard could be the external contractors. Let's consider a scenario where contractors from an external IT company have access to the system of a client's organisation,

and the level of access is a privileged one (e.g., admin level access). As we know high privilege access rights come with high risk, the activity of all external parties that interface with the organisation must be monitored and activities logged.

Training

All people connected to an organisation (whether internal employees or external contractors or customers) falls within the context of Cyber Security awareness training. A Cyber Security team needs to look into all peoples' Cyber literacy and put a proper Cyber Security awareness training pro- gramme in place. Cyber Security awareness training is not just about providing with some training tools or training video; it's about understanding structured training methods and developing training & teaching materials and activities in such a way so that people can be trained easily. It must be noted that such training is an extra load for people as this is in addition to their BAU workload. A Cyber Security training programme needs to be well-planned and well-structured following pedagogic strategies to effectively teach people.

Takeaways

The most qualitative part of Cyber Security is People part. Thus, this is the most challenging part of a Cyber Security leader. The followings are key points to note from the discussion in this chapter:

- People in Cyber Security realm include both internal and external people.
- People is the most crucial and probably the weakest part in Cyber Security context.
- Proper understanding of an ideal and required Cyber Security team and roles within it required.

- People with the Cyber Security team, the employees and people ex- ternal to organisation - all must be given adequate importance.
- Training for all people is undeniably important.

CHAPTER 4

Governance, Risk & Compliance

At least fifty percent (if not more) of Cyber Security is GRC.

Prelude

This chapter focuses on GRC. We explore how Governance significantly impacts Cyber Security and the roadmap of Cyber Security maturity. Major topics addressed in this part are Business Impact Analysis (BIA), Business Continuity Planning (BCP), Disaster Recovery Plan (DRP), Risk Management, Security & Privacy by Design, and Compliance.

Governance

Proper understanding and implementation of governance is not only crucial but also a must have prerequisite for successful Cyber Security initiatives. Governance and its related aspects must be clearly defined. One of the historical challenges related to governance is that, if an organisation does not have a holistic maturity and good practices in governance, then achieving

good governance in isolation becomes a not-so-constructive challenge for the Cyber Security team.

Good Governance practice for a Cyber Security team starts with a Cyber Security Governance Board. However, there could be two different types of Security Board - they are explained below to avoid any confusion.

Executive Security Board

Referring to Figure 2.1, in an ideal scenario, Cyber Security reports to the Executive Security Board. The member of the executive security board must include a mix of C-level, non-C-level and external members. External members are from outside of the organisation and with no conflict of interest.

Cyber Security Governance Board

The internal governance board to overlook the governance within the Cyber Security department/unit. Members of this board must have representative from Cyber Security, IS/IT and risk office (organisational, not the Cyber Secu- rity technology risk team). Forming Cyber Security Governance Board with members onyl from the Cyber Security may incorporate conflict-of-interest. Any Cyber Security related decisions that are not BAU must be approved by the security governance board. Non-BAU tasks and initiatives refers to those that generally change the current state of an organisation from a Cyber Security point-of-view. For example, the commissioning of a new tool or changing the configuration of an existing tool could be a crucial a decision which should be taken by the security governance board. To expand with further example, a Cyber Security leader may decide that a new application should be commissions – approval for such commissioning must be done through security governance board. Establishment of security governance board increases the transparency of an organisa-

tion and does helps to maximise the Cyber Security maturity of an organisation.

To sum up, it is mandatory for an organisation to realise Governance and its importance, and why Cyber Security operations must be operated within a robust governance framework.

Certification & Accreditation (CnA)

A clear and verified process to CnA (or lack of CnA thereof) tells a lot about the level of governance maturity. The existence of CnA, the existence of CnA that is integrated and exhibits good governance, and an expert of can - all these three are in the 'must have' list for a Cyber Security leader.

Impact Analysis

Various 'impact analysis' are part of governance related decision-making and this is not optional. Any changes (e.g. adding new element, decom missioning or modifying any existing element, demonstrative e.g., acquiring a new IT system, configuration changes to an existing system, or decom- missioning an existing IT system) to any context within the scope of Cyber Security must be done with clear understanding and realisation of the following impact analyses:

- Business Impact Analysis (BIA): aims to understand the impact on the business due to the proposed change.
- Security Impact Analysis (SIA): aims to understand how and whether Cyber Security might be impacted due to the proposed change.
- Privacy Impact Analysis (PIA): aims to understand the impact on various privacy aspects due to the proposed change.

Security & Privacy by Design

Proactive Cyber Security leadership considers security and privacy from the grounds up. That is, for any change introduced and any development occurred, the security and privacy is given ample consideration to embed right from the early planning and design. A bad approach is to think about security and privacy at later stages. For example, when acquiring an IS/IT system, conducting SIA and PIA before commissioning the IS/IT system to decide whether to go forward with the acquisition is feasible from security and privacy point-of-view. Another classic example in this regard is DevSecOps.

Risk Management

Risk management is an integral part of overall Cyber Security portfolio of an organisation. A robust risk management framework must be adopted to identify risk and manage the risks. Without a robust risk management framework implemented within the Cyber Security context, an organisation will have little ability to improve its Cyber Security maturity. Without proper risk management in place, an organisation simply has no intelligence on the inherent risks and thus has (knowingly or unknowingly) little or no capability to mitigate the risks, resulting in low or no Cyber Security maturity.

We discussed and recommended risk-based maturity in chapter 2. Without a robust risk management framework implemented, a risk-based maturity cannot be thought of. The identified risk mitigation approaches – referring to step 5 of the Figure 2.2 – becomes projects that are put into the Cyber Security Programme.

BCP & DRP

An organisation should have a holistic BCP of which Cyber Security DRP is a part. Non-existence of a DRP is not only an indicator of very low level of Cyber Security maturity for an organisation, but also a catalyst to create confusion of responsibilities among various IS/IT and Cyber Security roles during the time of a disaster. Thus, it's needless to say that a poor DRP or a non-existential one poses the risk of detrimental effect on business as part of the aftermath of a breach or Cyber-attack.

Compliance

Compliance is an indicator and the outcome of Governance and Risk Management. Compliance comes from both internal and external point-of-view of an organisation. External compliance often means adhering to the legal framework and internal compliance refers to conforming to internal policies. Good level of compliance is an ambitious one without good governance and robust Risk Management.

Takeaways

GRC cannot be undermined unless an organisation sets itself up for failure. GRC is at the heart of integrated and matured Cyber Security practices. Some examples research and discussion where the spotlight is on GRC are [24, 25, 26, 27, 28, 29, 30].

To connect dots between GRC and Cyber Security, some key takeaways are:

- Good GRC is crucial; no GRC is probably better than bad GRC.
- GRC is simple and straightforward to understand. Thus, the root cause of bad GRC may be an indicator of incompetence or mindset (towards GRC) of an or-

ganisation. If GRC is done just to tick the GRC box, the consequence is bad GRC that leads to scenario worse than no GRC.

- Cyber Security governance board - the heart of the pumping heart of good GRC.
- GRC with no BCP, DRP, Impact Analysis and CnA may sound paradoxical.

CHAPTER 5

Technology

Inadvertent or poor management of technology will bring successful failure to the strategic part of Cyber Security.

Prelude

This chapter suggests types of technologies required to complement strategic part of Cyber Security. Discussions in this chapter explores possible 'genre' of tools & technologies required, as opposed to mentioning any specific tool(s) or solution(s). Topics considered in this chapter consists of a non-exhaustive list, as expected when it comes to ever emerging computing technologies.

Cyber Threat Intelligence (CTI)

The Cyber Security maturity of an organisation demands CTI to be one of the defining matrices. Good governance and good maturity are exhibited by having a robust and established CTI process. That is, how to maintain, review, enhance and enrich CTI through an iterative loop and as an ongoing practice.

This short paragraph is no justice either to the importance or to the complexity of CTI.

IS/IT & System Portfolio

Technology Portfolio, a superset of configuration management, must be maintained for seamless operation. This may not be a task of the Cyber Security team as such, as it falls under the hood of IS/IT team, but importance of its integrity and maintenance to the Cyber Security team is undeniable, which makes it imperative that there be a strong coalition between the Cyber Security and the IS/IT team. For example, the Cyber Security team would require full access to the Technology Portfolio to understand what applications are being used in an organisation. The above (i.e., access to tech portfolio) is also required to understand the applications' life-cycle – this is crucial as outdated applications and tools may pose severe Cyber threat.

One Bird in Two Stone?

With poor governance, organisations may end up using multiple applications or solutions to achieve one thing. With proper governance and maintenance of technology portfolio, an organisation may avoid the above scenario. An example could be using a software for network monitoring and using another as firewall while the latter is a subset feature of the former. The above not only lacks business feasibility, but also may incorporate additional attack vectors into the attack surface of an organisation; the more the tools, the more the possibility of security loopholes!

Proactive vs Reactive

It is important for a Cyber Security leader to understand the difference between proactive and reactive approaches. Proac-

tive approaches refer to the measures and preparations for a risk before it happens, and reactive approaches 'react' once the risk occurs. Reactive approaches are not only hardly acceptable for Cyber Security but also is an indicator of low Cyber Security maturity of an organisation.

Identity & Access Management (IAM)

IAM must be integrated into the overall digital practice of an organisation. The bottom-line is to maintain Accounting, Authentication and Authorisation (AAA) integrity. IAM is much more than AAA. While AAA is mostly technical implementation, IAM is rather a strategic approach that requires thoughtful planning to achieve IAM maturity over time.

Application Blacklist/Whitelist

Does the Cyber Security team know the complete list of applications that are being used within the organisation? Is there a whitelist of allowed applications? Is there a blacklist of the applications there are prohibited? Is there a clear process to whitelist or blacklist an application? A Cyber Security leader would not want to learn one morning for the first time that their organisation has already started a social media channel!

Shadow IT

Everything ties back to good governance! Shadow IT is when employ- ees in the organisation starts using tools/systems/software that are not ap- proved, and often without anyone's knowledge. Example: employees using online PDF converter to upload confidential documents to convert to PDF and neither the IS/IT team, nor the Cyber Security team has any knowledge whatsoever on such practice. The Cyber risk of the above practice hardly requires any explanation to a Cyber Security professional.

Patch Management

Is there a clear policy on patch management? Is there a periodic patch management process in place? Is there an emergency patch management process in place? How does the organisation collect intelligence and updates on patches and updates?

State-of-the-art

How does the Cyber Security team learn about developments in local and global Cyber Security landscape and Cyber threat landscape? Does the organisation connect to the government CERTs to learn about new threats? Does the organisation report any novel threat discoveries to the relevant national authority? The author personally believes in this bottom-line when it comes to technology: always be state-of-the-art in strategies and tactics, but practice extreme caution to be state-of-the-art when it comes to adopt to technologies.

Takeaways

Technology is ever evolving; strategy in place is required to harness the rapid evolvement for goodness. There will always be new technologies, prob- ably with more unknowns incorporated than the 'knowns'. Good governance and sound strategy are the key to both leveraging new technologies and minimising technology risks. As mentioned in [31], thought process as well as a structured approach must be in place to select right tools and technologies for Cyber Security.

Technologies may be quantitative in a lot of ways, but their management is qualitative. Lack of good governance in leveraging technology may impact the strategic part of Cyber Security. For example, despite of having all precautions and strategic

soundness, choosing a technology residing in an undesired geographic location may lead to severe consequences.

CHAPTER 6

Concluding Remarks

Cyber Security Leader is rather a business leadership role, not a technical role - a CISO is not necessarily a CTO.

Cyber Security leadership is just like all other leadership roles - only subject matter or domain expertise would not see someone excel in this role. Leadership in organisations is rather more about people management and complementing business mission and vision. A Cyber Security leader establishes the value proposition of Cyber Security within an organisation. A Cyber Security leader is the translator between the business and the Cyber Security team.

Cyber Security leadership is a strategic role where strategic decision making and people skill is more crucial than technical expertise in Cyber Security. Hands-on experience in computer networks or in Cyber Security tools are by no means a requirement for a Cyber Security Leader.

Having said the above, and albeit neither required not a crucial component, technical expertise in Cyber Security always complements the portfolio of a Cyber Security leader.

Bibliography

[1] Niki Panteli, Boineelo R Nthubu, and Konstantinos Mersinas. Being responsible in cybersecurity: A multi-layered perspective. Information Systems Frontiers, pages 1–19, 2025.

[2] Eric Luiijf, Kim Besseling, and Patrick De Graaf. Nineteen national cyber security strategies. International Journal of Critical Infrastructures 6, 9(1-2):3–31, 2013.

[3] László Kovács. Cyber security policy and strategy in the european union and nato. Land Forces Academy Review, 23(1):16–24, 2018.

[4] Aleksandar Klaic. A method for the development of cyber security strate- gies. Information & Security, 34(1):37–55, 2016.

[5] Jule Hintzbergen and Kees Hintzbergen. Foundations of Information Security Based on ISO27001 and ISO27002. Van Haren, 2015.

[6] Lei Shen. The nist cybersecurity framework: Overview and potential impacts. Scitech Lawyer, 10(4):16, 2014.

[7] Christopher J Alberts and Audrey J Dorofee. Managing information se- curity risks: the OCTAVE approach. Addison-Wesley Professional, 2003.

[8] Jennifer L Bayuk, Jason Healey, Paul Rohmeyer, Marcus H Sachs, Jeffrey Schmidt, and Joseph Weiss. Cyber security policy guidebook. John Wiley & Sons, 2012.

[9] Brian K Payne, Lisa Mayes, Tisha Paredes, Elizabeth Smith, Hongyi Wu, and ChunSheng Xin. Applying high

impact practices in an inter- disciplinary cybersecurity program. Journal of Cybersecurity Education, Research and Practice, 2020(2):4, 2021.

[10] Issa Atoum, Ahmed Otoom, and Amer Abu Ali. A holistic cyber secu- rity implementation framework. Information Management & Computer Security, 22(3):251–264, 2014.

[11] Tari Schreider. Building an effective cybersecurity program. Rothstein Publishing, 2019.

[12] Francois Rheaume. Risk-based cyber mission assurance model, process and metrics. In The 24th International Command and Control Research Symposium (ICCRTS) Conference, 2019.

[13] Donald A McKeown. Building a risk-based information security culture.

ISSA Journal, 17(4):14–21, 2019.

[14] Afnan Alfaadhel, Iman Almomani, and Mohanned Ahmed. Risk-based cybersecurity compliance assessment system (rc2as). Applied Sciences, 13(10):6145, 2023.

[15] Jim Boehm, Nick Curcio, Peter Merrath, Lucy Shenton, and Tobias Stähle. The risk-based approach to cybersecurity. McKinsey, New York, 2019.

[16] RC Dodge, Daniel J Ragsdale, and Charles Reynolds. Organization and training of a cyber security team. In SMC'03 Conference Proceed- ings. 2003 IEEE International Conference on Systems, Man and Cy- bernetics. Conference Theme-System Security and Assurance (Cat. No. 03CH37483), volume 5, pages 4311–4316. IEEE, 2003.

[17] Harrison Stewart and Jan Jürjens. Information security management and the human aspect in organizations. Information & Computer Security, 25(5):494–534, 2017.

[18] Ayşe Asiltürk. The role of top management and it team interaction on the success of cyber security strategies. Adv Soc Sci, 267, 2022.

[19] David Lacey. Managing the Human Factor in Information Security: How to win over staff and influence business managers. John Wiley & Sons, 2011.

[20] Stephen J Zaccaro, Reeshad S Dalal, Lois E Tetrick, and Julie A Steinke. Psychosocial dynamics of cyber security. Routledge, Taylor & Francis Group, 2016.

[21] Amy Ertan, Georgia Crossland, Claude Heath, David Denny, and Rikke Jensen. Cyber security behaviour in organisations. arXiv preprint arXiv:2004.11768, 2020.

[22] Rick Van der Kleij, Geert Kleinhuis, and Heather Young. Computer secu- rity incident response team effectiveness: A needs assessment. Frontiers in psychology, 8:2179, 2017.

[23] Monjur Ahmed and Farkhondeh Hassandoust. Cyber security awareness training: A practical guide. 2024.

[24] Ashish Batra. Cyber security management: Creating governance, risk, and compliance framework. i-Manager's Journal on Software Engineer- ing, 14(4), 2020.

[25] Ishwor Thapa Chhetri. Cybersecurity and governance, risk and compli- ance (grc). Australian Journal of Wireless Technologies, Mobility and Security, 1, 2022.

[26] Adebayo Adeyinka Victor, Mubarak A Moronkunbi, Oyetunde Christian Oyedeji, Popoola Olusegun Victor, and Shodunke Ajani Samuel. The role of it governance risk and compliance (it grc) in modern organizations. International Journal of Latest Technology in Engineering, Management & Applied Science, 13(6):44–50, 2024.

[27] Yudistira Asnar and Fabio Massacci. A method for security governance, risk, and compliance (grc): A goal-process approach. In International School on Foundations of Security Analysis and Design, pages 152–184. Springer, 2011.

[28] Mr V Karthick, J Prabhakaran, Mrs P Banu, and US Senthil Kumar. Systematic literature review on grc-a study on best practices and im- plementation strategy in grc.

[29] Jason Edwards and Griffin Weaver. The Cybersecurity Guide to Gover- nance, Risk, and Compliance. John Wiley & Sons, 2024.

[30] Clarence Goh, Yuanto Kusnadi, Gary Pan, and Poh Sun Seow. Gov- ernance, risk and compliance (grc) in digital transformation: Investor views. Accountancy Business and the Public Interest, 21:200, 2022.

[31] Abbas Moallem. Understanding Cybersecurity Technologies: A Guide to Selecting the Right Cybersecurity Tools. CRC Press, 2021.

Dr Monjur Ahmed is a Cyber Security strategist and leader with extensive experience spanning academia and industry. With a proven track record in senior leadership roles in both Academia and Industry, he specializes in guiding organisations through the complexities of Cyber risk management, strategic security planning, and enterprise-wide cyber resilience.

Dr Monjur earned his PhD in Cyber Security from Auckland University of Technology, New Zealand. He complements his academic credentials with a suite of industry certifications in Cyber Security leadership, Enterprise Architecture and Project Management. His expertise encompasses a broad spectrum of Cyber Security domains, including Cyber Security Programme development, Cyber Maturity Analysis, Cyber Threat Intelligence (CTI), Incident Response, Governance Risk & Compliance (GRC).

9 781764 085649

intertype.com.au