

# Building a Cyber Resilient Business

**A cyber handbook for executives and boards**

Dr. Magda Lilia Chelly

Shamane Tan

Hai Tran



# Building a Cyber Resilient Business

A cyber handbook for executives  
and boards

**Dr. Magda Lilia Chelly**

**Shamane Tan**

**Hai Tran**

**<packt>**

BIRMINGHAM—MUMBAI

# Building a Cyber Resilient Business

Copyright © 2022 Packt Publishing

*All rights reserved.* No part of this book may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, without the prior written permission of the publisher, except in the case of brief quotations embedded in critical articles or reviews.

Every effort has been made in the preparation of this book to ensure the accuracy of the information presented. However, the information contained in this book is sold without warranty, either express or implied. Neither the authors, nor Packt Publishing or its dealers and distributors, will be held liable for any damages caused or alleged to have been caused directly or indirectly by this book.

Packt Publishing has endeavored to provide trademark information about all of the companies and products mentioned in this book by the appropriate use of capitals. However, Packt Publishing cannot guarantee the accuracy of this information.

**Group Product Manager:** Vijin Boricha

**Publishing Product Manager:** Mohd Riyan Khan

**Senior Editor:** Shazeen Iqbal

**Content Development Editor:** Romy Dias

**Technical Editor:** Nithik Cheruvakodan

**Copy Editor:** Julie Kerr

**Language Support Editor:** Safis Editing

**Project Coordinator:** Neil Dmello

**Proofreader:** Safis Editing

**Indexer:** Manju Arasan

**Production Designer:** Nilesh Mohite

**Marketing Coordinator:** Ankita Bhonsle

First published: October 2022

Production reference: 1051022

Published by Packt Publishing Ltd.

Livery Place

35 Livery Street

Birmingham

B3 2PB, UK.

ISBN 978-1-80324-648-2

[www.packt.com](http://www.packt.com)

*To the Chelly and Laaksonen families ... To my most fabulous husband, whom I cherish beyond words.*

*– Dr. Magda Lilia Chelly*

*To my dearest husband, your love and encouragement mean the world to me. I'm also thankful for my family and dear friends who're always cheering me on—this is for you. Finally, to my trusted circle and community who have grown together with me, I'm grateful for your support.*

*– Shamane Tan*

*To Hai Tran, who passed away while this book was being finalized.*

*He'd love to have seen his idea for this book, of helping as many organizations as possible derive the best value from cybersecurity functions, come to fruition.*

*Rest in peace now, my love, knowing that your legacy and unparalleled passion for the industry will be carried on by the many professionals who will find value insights from this book.*

*– Natallia Tran (Hai Tran's wife)*

# Contributors

## About the authors

**Dr. Magda Lilia Chelly** is an award-winning global cybersecurity leader. She has been named one of the top 20 most influential cybersecurity personalities in 2017 and 2021 by ISFEC Global.

In her career, Magda has worn several hats, including Information Security Officer for multiple organizations. Magda co-founded a cybersecurity start-up in Singapore called Responsible Cyber Pte. Ltd.

Magda's speaking engagements address topics on cyber risk quantification, bridging the gap between business and cybersecurity, cyber awareness, diversity and inclusion in the cybersecurity industry, and cybersecurity investments and entrepreneurship. Magda's research around cybersecurity has been featured by IEEE, the RSA Conference, and the CYBER RISK LEADERS magazine.

*I want to thank my husband for giving me the space and support I've needed to write this book, even while the COVID-19 global pandemic was raging around us. I'd also like to thank the Packt team for their support and patience for granting me the opportunity and time to complete this journey.*

*Many thanks for my Responsible Cyber team, and all my supporters throughout this journey.*

**Shamane Tan** is the Chief Growth Officer at Sekuro, leading the security outreach strategy with the C-Suite and executives. Recognized by IFSEC as a Global Top 20 Cybersecurity Influencer and awarded ASEAN Top 30 Women in Security, the Cyber Risk Leaders and Cyber Mayday and the Day After author was listed in the 40 under 40 Most Influential Asian-Australians.

Awarded ARN Shining Star 2021 and AiSP Singapore's Cybersecurity Professional, the TEDx speaker regularly chairs CxO thought leadership roundtables and serves on the Advisory Board for Black Hat Asia Executive Summit. Featured in World's Leaders World's 10 Most Influential Business Leaders in Cyber Security, Shamane is the founder of Cyber Risk Meetup, an international community and platform for cyber risk executives.

*To God, my source of inspiration, vision, and passion—Psalm 106:1. To my dear husband, who constantly cheers me on; thank you for your joy, encouragement, and celebration of my passion and vision. Thank you to my family, who have always been so understanding and supportive. You are so precious to me. Thank you Sekuro for being an amazing company that aspires to lead by example and challenges boundaries of what is possible and what is excellence. Thank you to my industry friends for your mentorship, for your contributions, and for shaping our industry for the benefit of everyone's growth and development. Finally, to my co-authors Magda and Hai, it has been such a journey the last few years bringing this together. We finally got there, although it is mixed with sadness to realize that this book has become a legacy that Hai leaves behind. To the whole Packt publishing team, it has been such a pleasure working together on this incredibly meaningful project. Thank you!*

A business-oriented and accomplished CISO, **Hai Tran** sought to leverage his exceptional governance, stakeholder engagement, and project management skills to manage risk by aligning mitigation strategies with business objectives. Hai had extensive leadership experience across a broad range of industries, including five years as the inaugural CISO for the Western Australia Police Force. Hai's strong focus on communication and transparency gained him respect and an outstanding reputation. He had a pragmatic and business-led approach to security in that it should be an enabler, company-wide, and frictionless. He was a strong, visible, and effective leader, keen to share his knowledge and empower industry professionals to reach their potential.

## About the reviewers

**Faisal Hussain (Syd)** is a veteran in the field of cybersecurity engineering and threat hunting. Currently, Syd is managing a cybersecurity program for Microsoft customer protection in the United Kingdom and EMEA as a **Microsoft Security Response Center (MSRC)** partner.

Syd works for Microsoft Corporation as a cybersecurity expert, specializing in cloud and enterprise security, advising C-level executives and field experts in detecting and preventing threats and response strategies across the industry.

Syd has peer-reviewed and developed IPs for Microsoft field security teams and presented at various conferences as a speaker. Syd is a regular presenter on security briefing calls hosted by Microsoft.

*I would like to say thank you to Madiha (my wife), Mohib (my son), and Maheen (my daughter) for supporting me in reviewing this book during my uber-busy life at Microsoft. I would also like to congratulate the authors on producing this book at a time when the industry needs this knowledge the most.*

**Kevin Tham** is a CISO leader in the Australian digital banking sector and a seasoned information security veteran in the financial services industry. Kevin's practical approach to cyber security is often seen as pushing the boundaries and balance between user-centric design and effective controls.

Kevin began his career as an academic researcher in the late 90s, an educator, and a security engineer, developing and implementing security controls, when many organizations did not regard information security as a risk. Today, Kevin is the CISO of a fintech organization, which aims to make a difference to individuals through well-thought-out banking solutions and products.

During his spare time, Kevin devotes his time to volunteering and giving his time back to the security industry through his involvement with the ISACA Sydney Chapter. He served on the board for 8 years and is also a former President, dedicated to serving its over 1,600 chapter members.



# Global Expert Takeaways

“Cybersecurity is perhaps the most challenging issue facing the modern boardroom – every organization has or will deal with a potentially devastating cyber incident, malicious or unintentional, and yet directors still find themselves struggling to understand whether their organization is effectively managing that risk. It doesn’t help that the constantly evolving threat landscape and the highly technical nature of cyber discussions can further alienate the board from understanding the right questions to ask. The result is often a sidelining of cyber risk to technical experts – the IT department and the CISO – which can lead to a potentially critical failure of effective cyber risk management.

Shamane, Magda, and Hai take a robust, straightforward response to this challenge, laying out a clear set of questions for both directors and C-suite executives. These go to the heart of effective cybersecurity risk management – are you communicating cybersecurity risk clearly, comprehensively, and effectively amongst the C-suite and to the board, and are you regularly monitoring your performance as an enterprise? Cyber is not an IT issue, it’s a business issue, which requires the whole business to be aligned and equipped to respond to, and that starts at the very top. As one director put it recently, *“No one thinks a cyber-attack will happen to them until it does, and that’s when robust cyber governance shows its merit.”* I would highly encourage any prospective and current board members or C-suite executives to read the chapter for boards in depth, and ask those very questions of their organization without delay.”

*Nicholas Chilton, Head of Board Advisory – South  
Pacific, Nasdaq Center for Board Excellence*

“Cyber risk is a live and dynamic topic in today’s boardroom discussions and decisions. The authors have presented a clear pathway for engagement with boards on cyber risk identification and management. Shamane’s six success criteria provide a useful checklist for boards in considering and discussing cyber risks. In the chapter for boards, the authors’ message to CISOs and other executives about how boards operate and how best to engage with boards is a valuable framework for ensuring the best outcomes for all businesses.”

*Teresa Dyson, Non Executive Director and Audit & Risk  
Committee Chair on boards of listed companies and  
government entities across media, financial services,  
energy, legal and government sectors*

“In my past career I’ve been a CIO for more than 20 years, a CISO for 3 years, and most recently, a Global Head of Technology and Cyber Risk, providing 2 Line oversight. As such, my perspective on the CIO and CISO is *unique*, as I understand their roles and responsibilities at a first-person level.

The CIO can be a powerful ally for the CISO. To understand this dynamic and harness this positively can be the key to an effective cybersecurity defense. Each leader has a critical role to play, and the chapter on CIOs provides some great insights into the potential challenges.

If we take a 10,000-foot view, then we can see the CIO has some conflicting requirements. They need to both innovate and drive digital change but do so in a manner that supports the customer experience. Conversely, the CISO passionately wants to protect the foundations, but they are aware that change can introduce new threats and vulnerabilities.

This book is a good guide for managers that want to understand and engage in protecting your enterprise.”

*David Gee, former CISO at HSBC, current Global Head  
Technology (Cyber & Data Risk) at an Australian global  
financial services group, with more than two decades in  
the CIO field*

“*The World of the Board* is an excellent chapter! Cybersecurity in any organization is the responsibility of the board and its members. Good cybersecurity protects the business’s ability to function, and ensures organizations can exploit the opportunities that technology brings. Cybersecurity is therefore central to an organization’s health and resilience, enabling its competitive advantage, and this places it firmly within the responsibility of the board.

It is important for board members to understand the right questions to ask their CISO/cybersecurity experts to have a strategic conversation. Ideally, the board structure should have a board member with CISO/cybersecurity expertise and credentials, and have an operational CISO reporting directly to them, and not to an intermediate C-suite executive.

The book gives an excellent insight into the traditional significance of the board's role versus the executive C-suite role, classifying the individual responsibilities within "Regulatory Governance" peripheries. The reader concludes that the common sense approach to good governance, risk, and compliance for the sake of the organization, is for the board and the C-suite to ensure they have a good line of communication and professional trust, and that recommendations or advice conveyed can be understood.

*Clr. Jeff Whitton, FAICD, CDPSE, local Government  
Councilor, Orange City Council, and industry veteran of  
forty years in the IT and cybersecurity domain as a CEO,  
Chair and board member*

"Congratulations on producing a publication that is resourceful for all of us! I must stress that cybersecurity is not merely an IT issue; it is everyone's responsibility. The board of directors, top management, and all employees must step forward to take full responsibility to overcome issues the at stake, and ensure collective and significant decisions.

As emerging threats are now highly sophisticated and disastrous, and have the potential to cause severe risks and challenges, cybersecurity risk management strives to enhance cyber-resiliency to prevent and detect threats, and to minimize business disruption and financial losses.

The implementation of a holistic approach is critical as it involves people, processes, and technology in order to decrease the risk of cyber-attacks and prohibit the unauthorized exploitation of systems, networks, and technologies."

*Dato' Ts. Dr Haji Amirudin Abdul Wahab, CEO of  
CyberSecurity Malaysia*

"Very well done! There is so much good stuff in this book. I enjoy the clarity of the explanations and the straightforward guidance that will serve many CEOs, COOs, and the rest of the executive team very well. I love the fact that Shamane, Magda, and Hai's advice stresses the importance of the CEO as the champion of creating the culture which considers cyber risk the risk

to the business operation. These days, investors as well as customer are less likely invest or put their money into a company that does not put cyber risk at the top priority. Cybersecurity (or “data care”) no longer applies to experts, it belongs to us all– including CEOs. I love the questions posed to the executives in the chapters, as they prompt us to check whether the right security measures are in place.

Also mentioned in the chapter for COOs is that it is absolutely critical to test both the *business continuity plan* and *disaster recovery plan*, because assuming that they will work can put the company in a very difficult situation, and even put it out of business. I worked for the “California Earthquake Authority”, where both plans were considered a high priority because of the unpredictability of earthquakes, which can not only ruin businesses but also cause the loss of life if not smoothly executed.

I remember us testing both business continuity and incident recovery by running thorough a mock test from A to Z every 6 months. There were many manual procedures, but at least we knew we could complete them both. In real life, there are no do-overs when a disaster strikes. From the continuous process improvement perspective, it is important to do what you call the PIR or Post-Implementation Review, because it is our best chance to learn from what has gone well, and what we must improve before the next incident. Continuous improvement is the key to having a great cyber risk plan, and post-mortems are where the suggestions come from.”

*Carmen Marsh, CEO, United Cybersecurity Alliance |  
Intelligence, Board Member*

“This is a good book and I liked it a lot. The overall articulation is a great way to convey the differences between the CIO and CISO roles, but also how they complement each other in enabling important business outcomes for the organization. The priorities may differ and the authors call out the need for clear communication and common goals. I particularly like the section where the authors articulated the role of a CIO in supporting cyber resilience. I found the narrative quite practical and of great value to everyone who reads it.”

*Abhishek Singh, Chief Information Officer, UNICEF*

“Reputation risk is an intangible balance sheet that’s hard to quantify. But a data breach can be devastating, and it’s going to fall on the CMO to manage and recover brand trust. I highly recommend all CMOs read the chapter

on the CMO and CPO – *Convergence between Privacy and Security*. It's in a simple and easy to digest form, but raises issues of utmost importance.”

*Brent Annells, Chief Marketing Officer, Smart Token  
Labs, formerly with Uber and Facebook*

“This is a book that I would highly recommend for cybersecurity leaders navigating a complex business environment. I especially enjoyed the chapter on building a strong security culture. It is important to understand that cybersecurity is not a pure technical issue; shaping human behavior is one of the important elements of a cyber-resilient organization. Empowering employees to be first defense and to share the same values, philosophy, and behavior is extremely important to sustain a good cybersecurity posture in any organization.

This book provides a holistic view of different perspectives, from technical, business, to cultural aspects, which will build up your business to be more cyber-resilient through partnership and collaboration.”

*Christopher Lek, Director, Cyber Security, Centre for  
IT Services, Nanyang Technological University,  
Singapore (NTU)*

“Cybersecurity is a real-world challenge, and we all must have a fair understanding of the *what and how* at each level of the organization to manage a crisis when it erupts. This book outlines the areas for each group of executives to know the challenges and potential ways to deal with them.

In one of the chapters, it was great to see a fair comparison of a CIO versus CISO's roles and responsibilities; it's commendable how both perspectives were stitched in to demonstrate that both leaders need to collaborate to deliver the *customer* objective. The debate on *who should report to who* will continue, but it's vital that both executives play a collaborative role in working together to deliver the same best customer experience, and keep the organization safe, which is a win for everyone.

The authors have produced thought-provoking work, and while reading this book you will find yourself changing your hats to gain both sides' perspective.”

*Amit Chaubey, Chair, Australian Information Security  
Association (AISA), Sydney*

“Shamane, Magda, and Hai have a gift for demystifying the role of the CISO with context, logic, and meaningful illustrations. The role of the CISO is greatly misunderstood by many organizations, as reflected in their own corporate structure reporting lines, responsibilities, and accountabilities. The emphasis made on using business risk language to engage non-technical audiences is correctly put into perspective for continued success. Cybersecurity is highly dynamic and therefore never stops nor goes to sleep at night. *Chapter 5* provides excellent tips for cyber risk quantification and board interaction for CISOs.

The chapter on *The World of the Board* also presents great insights, including the need for business acumen and financial understanding to successfully articulate the enterprise cyber risk exposure to the board of directors. Speaking the board’s language is presented as a critical skill for building rapport and for getting the voice of the CISO heard with authority, trust, and respect. The insights that the authors bring in this chapter makes this book a must have for any cyber practitioner’s professional library.”

*Marco Figueroa, former Group CISO for New South Wales  
Department of Customer Service cluster and current  
Senior Manager for Cyber Security, Risk and Compliance  
at the Australian Institute of Company Directors*

“Shamane, Magda, and Hai have aptly put across key business digital concerns at the board, CEO, and CISO/CSO levels, and key risk governance approaches to adopt. The approaches, illuminated through the experiences of the authors and experts interviewed in the book, resonate well with ISACA’s Risk IT Framework. The chapters are a real pleasure to read, succinct, and practical for anyone in these key business roles to follow. Without a doubt, I would recommend any aspiring board director, CEO, or CISO/CSO to pick this up early and have a good read, avoid major mindset pitfalls, and save yourself and your business future heartaches!”

*Steven Sim Kok Leong, President, ISACA Singapore  
Chapter; Chair, OT-ISAC Executive Committee and  
Global CISO, Global Logistics Multinational Corporation*

“Cybersecurity is often seen as a technology issue. Given that this perspective has been transitioning to being seen as a business issue, this book brings across many key factors in very basic terms to the reader. There are many relevant principles that are more management, board, and CEO-focused, which is exactly how it should be to truly make a business cyber-resilient. I really like how the book touches upon various regional aspects; from different

areas of focus to some of the shortcomings, and this is helpful to any level of reader – board, CEO, and the rest of the C-suite. The chapter for boards is also an excellent read and simple to understand. I like that it provides key emphasis on how both the directors and management should be cyber aware, from their role in cybersecurity to helping board and non-cyber management understand cyber risk, to providing strategic direction in ensuring the organization is cyber-resilient. This is crucial, especially in light of the release from the U.S. Securities and Exchange Commission on their proposed new rules requiring U.S. public company boardroom disclosure of corporate directors with cybersecurity expertise, which happens to also align nicely with one of the topics highlighted in the book, *The CISO's Seat at the Table*. Well done Shamane, Magda, and Hai!”

*Prashant Haldankar, Co-Founder and CISO, Sekuro |  
Privasec Asia | Co-Founder, DroneSec*

“The roles of the executive team are well established in every organization, but to know what motivates them and how to use this motivation to spearhead cybersecurity goals and outcomes can be tricky. This book works almost like a cheat sheet for any new or established CISO to better understand their executive team and colleagues. This book contains invaluable insights that will accelerate the execution of any security strategy.”

*Kevin Tham, CISO, Avenue Bank, ISACA Sydney  
Chapter Past President*

“Great work, authors! I especially enjoyed the chapter on the secret recipe and building security culture. I liked the idea of all the questions that were included at the end of the chapters, as well as how a CISO should engage at all levels of the organization. Asking the right kind of questions is something I’m pretty passionate about. It’s only through asking the right provocative questions that we can identify the problems worth solving, and invite thought leadership and discussion.”

*Tim Wenzel, Head of Global Security Protective  
Intelligence, Fortune 50 Technology Company |  
Co-Founder, The Kindness Games*

# Table of Contents

Preface

xxi

---

## 1

<b>The CEO Cyber Manual</b>			<b>1</b>
<b>Why cybersecurity should be a CEO's priority</b>	3	Beyond technology—cyber risk is a business risk	12
Dependency on technology—a critical business failure blindspot	5	Demystifying data breaches and cyberattacks	13
Cybersecurity is a critical environmental, social, and governance pillar	6	<b>Quantifying cyber costs versus return on investment</b>	14
<b>Understanding cyber risks and their implications for businesses</b>	7	<b>Building a culture of cybersecurity</b>	17
<b>Understanding cybersecurity challenges, organization, and reporting</b>	9	<b>Preparing a business for cyberattacks</b>	20
Cybersecurity and information technology—similar skills but with a different focus	11	Cybersecurity considerations for a CEO's first month	21
		<b>Questions to ask yourself as a CEO when considering your cyber risk coverage</b>	22
		<b>Summary</b>	23



## 2

### **A Modern Cyber-Responsible CFO 25**

---

<b>Why the CFO should care about cybersecurity</b>	<b>26</b>	Benchmarking cybersecurity budgets	34
The role of the CFO in cybersecurity	27	Defining cybersecurity spending	35
<b>The CFO's understanding of cybersecurity</b>	<b>28</b>	Supporting cyber-risk quantification	35
<b>The aspects of cybersecurity the CFO should consider</b>	<b>30</b>	Purchasing cyber insurance	36
A CFO's perspective	32	Assessing third-party risks	37
Addressing cyber risk from a complex financial view	33	<b>Communicating with the CFO about cyber risks</b>	<b>37</b>
Defining the CFO's role in building cyber resilience	34	Economic costs	39
		Mindset	40
		<b>Questions to ask your CFO</b>	<b>40</b>
		Summary	41

## 3

### **The Role of the CRO in Cyber Resilience 43**

---

<b>Understanding the role of the CRO and its key focus areas</b>	<b>45</b>	<b>Developing the right mindset as a CRO</b>	<b>52</b>
Analyzing the CRO's key priorities	46	Understanding the collaboration potential between the CRO and CISO	54
<b>Identifying the CRO's challenges</b>	<b>47</b>	<b>Questions to ask your CRO</b>	<b>56</b>
Strategies, systems, frameworks to manage cyber risk	50	Summary	57
Connecting the dots	52		

## 4

**Your CIO—Your Cyber Enabler 59**

Understanding the CIO's role and the impacts their decisions have on cybersecurity	61	Differences and commonalities between the CIO and CISO roles	65
Rapid technology adoption	62	Getting ahead of cybercriminals	67
Balancing digital transformation	63	How the CIO supports your security	68
Complex regulatory landscape	65	Questions to ask your CIO	70
Third-party risks	65	Summary	71

## 5

**Working with Your CISO 73**

Understanding the role of the CISO	74	Questions to ask your CISO	88
Your CISO's understanding of your business	77	A Bonus Segment for Our CISOs—Decoding Your CxOs' Expectations	89
Priorities for a new CISO	78	Key Communication Non-negotiables	90
Addressing cybersecurity challenges	78	Cyber Risk Quantification—the Holy Grail for Your Success	92
Cyber risk identification and quantification	80	A Bonus Segment for Our CISOs—Purchasing Cyber Insurance	95
The different approaches to handling your cyber risk	82	A Bonus Segment for Our CISOs—Reporting to the Board of Directors	98
Cyber risk management strategy	84	Summary	99
Cybersecurity metrics	87		
Indicators for dashboarding/reporting	88		

## 6

### **The Role of the CHRO in Reducing Cyber Risk 101**

---

Why the CHRO should care about cybersecurity	102	The challenges CHROs face with cybersecurity	111
The transitioning role of the CHRO	105	Questions to ask your CHRO	112
How the CHRO supports cyber resilience	107	A bonus segment for our CISOs—recruiting and building your cybersecurity team	113
The tools HR uses	109	Summary	116
Recruiting qualified cybersecurity team members	109		

## 7

### **The COO and Their Critical Role in Cyber Resilience 117**

---

Understanding the role of the COO	118	Business continuity plan management—the dos and don'ts	122
Why the COO should care about cybersecurity	119	Business continuity and disaster recovery must not fail!	123
Where the line is between the COO and the CISO in terms of responsibility for business continuity	120	What does a good BCP look like?	124
Operational technology and cybersecurity—a necessity in today's world	121	The methodology	124
		Disaster recovery planning	127
		Test, test, test. Did we mention your plan must be tested?	128
		Questions to ask your COO	128
		Summary	129

## 8

**The CTO and Security by Design 131**

<b>The role of the CTO</b>	132	<b>Secure coding and secure software development</b>	137
The difference between a CDO and CTO	133	<b>Conflicts of interest and collaboration between the CTO and the CISO</b>	139
<b>Why the CTO should care about cybersecurity</b>	134	<b>Questions to ask your CTO</b>	141
<b>How the CTO becomes a security ally</b>	136	<b>Summary</b>	142

## 9

**The CMO and CPO—Convergence Between Privacy and Security 143**

<b>What the CMO and CPO roles have in common</b>	144	<b>The role of marketing and communication following a cyber incident</b>	152
<b>The role of marketing and privacy in cybersecurity</b>	146	<b>Questions to ask your CMO and CPO</b>	154
Risk mitigation	147	<b>Summary</b>	155
<b>The intersection of privacy and security</b>	150		

## 10

**The World of the Board 157**

<b>Understanding the world of the board</b>	158	<b>The board's interests in cybersecurity</b>	162
<b>The board's structure</b>	160	Business ownership	163
		Appropriate investment	164

---

Rightly equipped	164	Reporting to the board	
Risk transfer options	165	(an add-on for CISOs and	
Maintaining foresight	165	a reference for CEOs)	171
Industry resilience	165	Boards and mergers and	
The CISO's seat at the table	166	acquisitions	172
Speaking the board's language	167	Asking the board the right	
What <i>not</i> to do in the		questions and setting up	
boardroom	170	your CISO for success	173
		Summary	174

## 11

### **The Recipe for Building a Strong Security Culture—Bringing It All Together** **177**

---

Building a robust security culture	178	A hands-on cyber-awareness program	188
Bringing it all together	179	What kind of community are you building?	190
CISO add-on—building a cybersecurity culture	181	Questions to ask yourself about building a culture	191
The different building blocks	183	Summary	192
Varying your training	185		
Cloud-sharing responsibility	187		

### **Index** **193**

---

### **Other Books You May Enjoy** **202**

---

# Preface

Executive leadership is essential in creating a culture of cybersecurity and business resilience within an organization. Therefore, every executive has a role to play in cybersecurity and their organization's cyber resilience. Executives must be aware of the risks their organization faces, and they must collaborate to put in place the right strategy to protect the company's data and infrastructure.

In addition, executive team members can play a critical role in responding to a cyber incident. They can provide direction during the response phase, help ensure all stakeholders are kept informed, and make decisions about how to best restore systems and services. Finally, executives must also continue to work toward increasing the organization's overall cybersecurity posture, even when there is not an active incident.

This book provides an in-depth view of each executive's role in the cyber-resilience journey and provides practical insights, with lessons learned, supporting a mindset change to address the new digitization era.

## Who this book is for

This book is for you—the executive who is curious about cyber resilience and cyber risk and is ready to understand the importance of everyone's role in achieving it.

## What this book covers

*Chapter 1, The CEO Cyber Manual*, starts by laying out the fundamentals of building a cyber-resilient business in a digitized world. The Chief Executive Officer has a critical role in cybersecurity and cyber resilience, as they are ultimately responsible for the overall security of the company and its data.

*Chapter 2, A Modern Cyber-Responsible CFO*, lines up the fundamentals for a CFO's success in supporting cyber resilience. The Chief Financial Officer has a critical role in cybersecurity and cyber resilience. One of their key functions is to ensure the organization has accurate data to make decisions. The CFO is also responsible for ensuring there is a process in place to quantify the losses associated with a cyberattack, in collaboration with the Chief Information Security Officer. This includes quantifying the financial loss but also the cost of downtime, loss of customer data, and loss of employee productivity.

*Chapter 3, The Role of the CRO in Cyber Resilience*, looks at the Chief Risk Officer's perspectives, challenges, and how cyber risk is integrated into an enterprise's risk management strategy. The CRO is responsible for making sure the company is managing all types of risks, and when it comes to cyber, they need to collaborate closely with the CISO to achieve a balanced risk posture.

*Chapter 4, Your CIO—Your Cyber Enabler*, explores the Chief Information Officer's role in cyber resilience, which is to ensure an organization has a technology infrastructure while protecting its digital assets and that these assets are accessible to the appropriate stakeholders when needed. It is the CIO's responsibility to keep up with new technologies and to develop policies and procedures for incorporating these technologies into the organization's infrastructure, including security and privacy concerns. This can be a challenging task, as it often requires balancing security needs with business needs. This chapter presents examples of conflict of interest inherent in the CIO's responsibilities and how to address them while continuing to innovate.

*Chapter 5, Working with Your CISO*, is a thorough overview of the Chief Information Security Officer's world, challenges, lessons learned, and practical insights on cyber-risk quantification and risk transfer. The CISO is responsible for risk management within an organization. They work with senior leadership to ensure the company is protected from cyber threats and business processes can continue in the event of a cyber incident. The CISO is also responsible for usability while maintaining a balance with security. They work with departments across the company to ensure employees have access only to data they need to do their jobs, and that information is accessible in a way that makes sense for the business.

*Chapter 6, The Role of the CHRO in Reducing Cyber Risk*, delves into the Chief Human Resources Officer's role in cybersecurity, which is to ensure the company has the proper HR policies and procedures in place to protect employees' personal data and mitigate the risk of a cyberattack. The CHRO,

together with the CISO, is responsible for developing and implementing a security awareness program that educates employees about how to protect themselves online, how to spot phishing emails, and what to do if they suspect they've been compromised. As well, the CHRO must work with the CISO to establish a cultural change and cyber awareness adoption.

*Chapter 7, The COO and Their Critical Role in Cyber Resilience*, examines the role of the Chief Operating Officer in cybersecurity, which is to help develop and execute an organization's **Business Continuity Plan (BCP)**. The BCP outlines how the company will continue to function in the event of a major disruption, such as a cyberattack. The COO is responsible for ensuring the BCP is up to date and comprehensive and all departments are aware of their roles and responsibilities in relation to it. Collaboration between the COO and the CISO is critical in achieving a successful resilient journey.

*Chapter 8, The CTO and Security by Design*, specifically addresses the responsibilities of the Chief Technology Officer in supporting cyber resilience. The role of the CTO in cybersecurity is to ensure software development processes are secure and compliant with industry standards. This includes overseeing the **Secure Development Life Cycle (SDLC)**, which encompasses code review, testing, and other activities designed to ensure applications are free of vulnerabilities. In addition, the CTO works closely with other parts of the organization to ensure security is embedded into every facet of the business, which necessitates strong collaboration with the CISO.

*Chapter 9, The CMO and CPO—Convergence Between Privacy and Security*, explores how, in recent years, the roles of Chief Marketing Officer and Chief Privacy Officer have become increasingly important in cybersecurity. As the world becomes more connected, businesses are collecting and storing more data than ever before. And with the **General Data Protection Regulation (GDPR)** recently coming into effect, companies must be extra careful about how they collect, process, and store customer data. That's where the CMO and CPO come in. The CMO is responsible for overseeing all marketing activities within a company. This includes developing marketing strategies, planning and executing marketing campaigns, and analyzing market trends. The CPO, on the other hand, is responsible for ensuring a company's privacy policy complies with all applicable laws and regulations. This chapter provides good insights on how those two roles support cyber resilience.



*Chapter 10, The World of the Board*, looks at business priorities and clarifies a board of directors' role in achieving business resilience while supporting the CISO. The role of the board in cybersecurity is to ensure an organization has adequate defenses in place to protect its digital assets and management has put in place processes and protocols to mitigate risk and respond to incidents. The board should also ensure the organization has a risk management framework in place, which includes assessing vulnerabilities and threats, determining acceptable levels of risk, and implementing mitigating controls. Finally, the board should review incident response plans to make sure they are adequate and enable the organization to quickly restore normal operations after an incident.

*Chapter 11, The Recipe for Building a Strong Security Culture – Bringing It All Together*, brings together everything we have learned and provides a holistic overview of how a team effort leads to a resilient business. An organization's cyber-awareness culture is a collection of values, policies, and norms governing how its employees use personal data and information technology. A strong cyber-awareness culture helps an organization protect itself from cyber threats by educating and empowering its employees to be security conscious in their daily work routines.

## Download the color images

We also provide a PDF file that has color images of the screenshots and diagrams used in this book. You can download it here: <https://packt.link/xgNMw>.

## Get in touch

Feedback from our readers is always welcome.

**General feedback:** If you have questions about any aspect of this book, email us at [customercare@packtpub.com](mailto:customercare@packtpub.com) and mention the book title in the subject line of your message.

**Errata:** Although we have taken every care to ensure the accuracy of our content, mistakes do happen. If you find a mistake in this book, we would be grateful if you would report this to us. Please visit [www.packtpub.com/support/errata](http://www.packtpub.com/support/errata) and fill in the form.

**Piracy:** If you come across any illegal copies of our works in any form on the internet, we would be grateful if you would provide us with the location address or website name. Please contact us at [copyright@packt.com](mailto:copyright@packt.com) with a link to the material.

**If you are interested in becoming an author:** If there is a topic that you have expertise in and you are interested in either writing or contributing to a book, please visit [authors.packtpub.com](http://authors.packtpub.com).

## Share your thoughts

Once you've read *Building a Cyber Resilient Business*, we'd love to hear your thoughts! Please [share your thoughts](#) for this book and share your feedback.

Your review is important to us and the tech community and will help us make sure we're delivering excellent quality content.



# 1

# The CEO Cyber Manual

If we could travel back in time even just a few years, no one could have imagined a global pandemic would strike, causing massive social upheaval and affecting almost every sector. The COVID-19 pandemic that swiftly transmitted to almost every nation in early 2020 impacted life as we know it, including how we work, interact with each other, and, essentially, how we live.

Businesses and educational institutions shut down, employees were forced to work from home or remotely from other locations, supply chains were disrupted, individuals were compelled to self-isolate, most travel was prohibited, and in-person meetings and conferences transitioned to virtual gatherings. When we started writing this book, these interruptions had already been going on for several months. Even as we put our pens down, nearly two years later, the times we live in have changed drastically, and the economic, commercial, and social consequences will be felt for years.

Nonetheless, businesses need to operate in this new environment. Livelihoods depend on it. Corporate operations and services need to keep running smoothly and efficiently. Technology has been a viable solution, used in both conventional and creative ways.

With more businesses adopting digital technologies in their bid to improve efficiency, value, and the pace of innovation, we have found ourselves in the age of digital transformation. Many processes and services are continuously moving online, and technologies such as cloud computing, robotics, drones, artificial intelligence, chatbots, virtual realities, augmented reality, autonomous systems, and the *Internet of Things* is shaping the future of the workplace.

Technology plays a vital role in all activities, from operations in healthcare, business, education, government, the legal system, and community services to consumer-connected houses. Recent technological advancements have altered significantly how we conduct our everyday personal and business activities.

While many C-level executives are excited about how technology can enable businesses and individuals, its adoption comes with drawbacks, such as increased interconnectivity and dependency on third parties. This dependency also raises concerns about emerging cyber risks.

As boards of directors are frequently seeing cyberattacks (from advanced nation-state attackers all the way down to average malicious threats) and cyber warfare in the headlines, it is natural for them to be increasingly concerned and wary about businesses falling victim. At the same time, business stakeholders have found themselves overwhelmed by the technical jargon and misalignment between business and cybersecurity. In this handbook, we will describe each executive position's responsibilities in achieving a cyber-resilient business.

In this first chapter, we're going to answer the main business stakeholders' most frequent questions by addressing the following topics:

- Why cybersecurity should be a CEO's priority
- Understanding cyber risks and their implications on a business
- Understanding cybersecurity challenges, organization, and reporting
- Quantifying cyber costs versus return on investment
- Building a culture of cybersecurity
- Preparing a business for cyberattacks
- Cybersecurity considerations for a CEO's first month
- Questions to ask yourself as a CEO when considering your cyber risk coverage

## Why cybersecurity should be a CEO's priority

As a **Chief Executive Officer (CEO)**, chief administrator, or just **Chief Executive (CE)** in charge of managing an organization, four goals are critical for businesses in the *new normal*:

- Cloud and digital transformation, which has accelerated due to long-term remote working.
- Increasing the pace of automation, supported by technology adoption.
- Placing sustainability at the heart of all initiatives.
- Skills development and talent retention, which gets harder by the day due to changing job market demand.

We live in a globally connected world, where information is the lifeblood of an organization, and technology the blood vessels. Traditionally, companies build trust through physical files and locks, protecting their customers' interests with manual security processes. As businesses evolve and the nature of how they deliver products and services to customers changes, their reliance on technology also increases, whether they realize it or not.

Today, customers interact with businesses through digital channels, creating a plethora of digital data and avoiding any form of physical paper and files. Through this change in customer expectations, businesses try to keep up, and sometimes even try to stay ahead of the curve, by adopting new technologies, including cloud networks, the **Internet of Things (IoT)**, **artificial intelligence**, and **blockchain**, at a fast rate. The year 2020 specifically saw an explosion of digitization, driven by people who were forced to work from home. Quarantine requirements meant customers could no longer just walk into any physical store. Due to the threats posed by COVID-19, companies were forced to adopt more technology-driven business models to remain competitive.

These changes are beneficial for businesses as they increase revenue by providing automation and better customer service, with everything at the customers' fingertips. However, the intangibility of data and assets stored in digital form in the cloud and other technology systems has created a false sense of security.

These transformational changes, including the increasingly complex ecosystems in which companies operate, have inevitably increased organizations’ risk exposures and, therefore, their cyber risk. Due to the intangibility of data and digital platforms, CEOs historically haven’t seen a clear value in investing in cybersecurity and the emerging risks technology adoption brings: “*I am not a target, and I have an information technology team working on the problem. I am safe.*” Such is the typical feedback we have heard regularly from leaders of organizations.

For many other businesses, cybersecurity is still seen as *nice to have*, a nonfunctional requirement driven only by customer demands. It is, therefore, unfortunate it has taken businesses falling victim to cybercrime before they start seeing cyber risk as a tangible business risk.

It is ultimately the CEO’s responsibility to create, institute, and maintain a cybersecurity strategy. In a May 2022 AICD survey on Board’s Cyber Resilience Practices Report, of the 856 board directors in Australia, the majority indicated the CEO as the executive primarily responsible for building cyber resilience in the organization. *Figure 1.1* shows the results of that survey.

### Responsibility for Cyber Security

Q. Who is primarily responsible for: (a) building cyber resilience in your organisation; and (b) reporting to the board on issues related to cybersecurity? Please select maximum 3 options in each row.

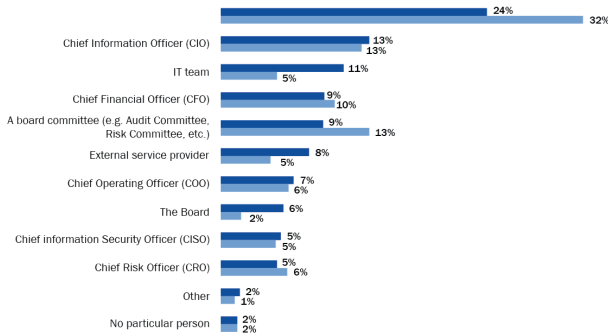


Figure 1.1 – Survey of who is responsible for building cyber resilience in their organization

With businesses becoming more dependent on technology to provide services to customers, and with new changes to their operating model, CEOs need to re-evaluate the ways they are going to retain, and after a cyberattack, regain trust with their customers.

## Dependency on technology—a critical business failure blind spot

Businesses now have more flexibility, automation options, and mobile capabilities thanks to technology. It's unsurprising to see how reliant company owners are on technology and how technology aids the growth of businesses. According to a recent study, over 48 percent of company owners say the ability to operate their firm from a mobile device is critical. This statistic is supported by the fact that a typical company owner uses their mobile device at least twenty-one times every day.

The mass digitization of core business processes, from sales to accounts receivable, business analytics, production lines, cost optimization, and productivity improvement, has increased the potential impact a technological failure can have on a business. Every business process depends on technology, from a simple spreadsheet to a complete technology platform.

**Cyber risk** is defined as any risk of financial loss, disruption, or damage to an organization from a failure of its information technology systems due to a cyber threat. This risk extends to technology disruption, data loss, theft or disclosure of data, and product recalls as examples of plausible business risks.

Every organization (and indeed every individual) is a target. The dependence on information and technology has exponentially exposed all to cyber risk, regardless of industry, size, or geography. It is simply not realistic to claim, “*We will never be attacked*” or “*It won't happen to us*.” It is widely acknowledged that companies fall into two categories—the ones that have been hacked and those that do not yet know they have been hacked.

The more tech-savvy and cyber-aware CEOs know that changing business models and growing technological dependencies lead to newly emerging cyber risks that can have a tangible impact on their businesses. This is a starting point for organizations to address those cyber challenges and decide on adequate and cost-effective cyber initiatives. Building security into a new technology platform early on will often be cheaper than having to rework a solution at a later stage. We cover this in more detail later in the chapter.



## Cybersecurity is a critical environmental, social, and governance pillar

Investors today are just as concerned about a firm's cybersecurity posture as they are about system capability and operational stability. They often review data protection and information security policies to assess a firm's cyber risks. As our digital economy continues to flourish and evolve, executive management and global investors are also rapidly becoming more cognizant of the widespread business and social impact of a cyber breach (such as financial or reputational damage). Cybersecurity, which was once primarily a technological problem, is now recognized as a critical **Environmental, Social, and Governance (ESG)** concern—in particular, a key metric of the **social** pillar.

ESG frameworks are a practical way to assess business behavior. By including cybersecurity as one of its concerns, a new dimension is introduced, providing insight into how an organization approaches cyber risks and employees' online behaviors, both of which are vital elements of the overall ESG picture.

As the global workforce has shifted to working from home, more employees are placed outside the security protections offered by their office IT systems and environments. This has resulted in an increased vulnerability in organizations' security defenses (perhaps caused by insecure habits due to lack of awareness or security apathy), leading to more frequent cyber incidents and, naturally, focusing more attention to the area of cybersecurity. If companies do not sufficiently safeguard their information networks, they risk being fined in the event of a breach and/or damaging their reputation. We have seen this become increasingly common in the IT sectors and financial and communications services, along with sectors that traditionally haven't invested as much money in cybersecurity.

Cybersecurity has become a social concern, and a global perspective needs to be factored in, taking into consideration geographical and geopolitical data when analyzing cyberattacks. It is also a growing industry, with core security spending estimated to reach \$1.75 trillion over a five-year period from 2021 to 2025, according to Cybersecurity Ventures.

Increasing investment in a company's systems, products, and services to boost protection against cyberattacks can benefit many businesses across different industry sectors, which means organizations, investors, and the general public increasingly are aware of the need for cybersecurity protection. Although including cybersecurity as an ESG metric is still a relatively new

concept, there is an undeniable increase and continued interest in this across industries. In a discussion Shamane (co-author of this book) had with a group of board directors, they highlighted with great enthusiasm that the current two hot topics constantly brought up in the boardroom are *ESG* and *cybersecurity*. That cybersecurity becomes a concern of ESG, therefore, makes perfect sense.

Cybersecurity is no longer just a technical problem; it's not only here to stay as an ESG concern but will also expand to other segments of a business with time as recognition of its necessity becomes commonplace.

Now that we've unpacked the role and future of cybersecurity and why it must be a priority for all CEOs, in the next section, we will dive further into understanding the business fundamentals concerning cyber risk. We will demonstrate how cybersecurity can be aligned to business goals and priorities, and help translate the technical jargon into business risks.

## Understanding cyber risks and their implications for businesses

Cybersecurity is often an afterthought, a contractual requirement, a compliance checkbox, or a tender requirement mixed in with other functional requirements. Rarely is it included as an embedded strategy within a business. As a cyber risk is perceived as complex and intangible (until a company is victimized by a cyberattack), many executives are challenged to understand and evaluate the need to incorporate it into their business plan and instead approach it as enterprise risk in general.

The following list details some questions executive leaders should ask about the cybersecurity strategy at their company:

- “*What is my cyber ROI?*”
- “*What is my exposure?*”
- “*What are my losses in the event of a cyberattack?*”
- “*Will a cyber event cause physical damage to our systems?*”
- “*How much should I spend on cybersecurity, and what should I prioritize?*”
- “*How ready would we be if a significant security event occurred?*”

These questions raise and define the current challenges of tackling cyber risks. The recent race to adopt digital solutions for business coupled with a lack of cyber awareness and minimal or patchwork regulation has created the urgent need for organizations to develop awareness and understanding of their exposure to cyber risk, the general importance of cybersecurity, and their **return on investment (ROI)**.

First and foremost, it is important to align a company's cybersecurity with its business goals. Protecting a business from cyberattacks and data breaches is crucial and requires skilled resources with an adequate budget. However, it doesn't just stop at purchasing expensive tools, or getting your IT team to work with those tools. Security programs should have a long-term vision, and there is never an "end date."

Cyber risk management requires a holistic risk approach that incorporates mitigating controls across the spheres of people, processes, and technology. It needs to align with the business priorities and the company's risk appetite. Cyber risks are often inadequately addressed (if at all) by business stakeholders, probably because they lack the awareness to do so. *"It won't happen to us."* Too often, organizations tend to bury cyber risks under general technology risk, which in turn gets buried under operational risk. Cyber risks are not just malware; a cyber risk can result in business operation disruptions, data breaches, data loss, and/or reputational damage. Unfortunately, too many companies, and too many executives, have yet to start viewing a cyberattack as a risk and not only an IT problem. Too often, cybersecurity remains a problem when professionals who support cybersecurity strategies do not have the right skills, experience, and qualifications.

Cyber risk is a *business risk*. Just as any business that operates a physical office space needs to take precautions to protect against threats to property, organizations today need to protect themselves from technology risks, especially with the increasing adoption of work-from-home policies and a growing amount of business activities solely performed using technology.

Mitigating cyber risk requires cybersecurity controls to protect information and systems from unauthorized access, loss, theft, and disruption. Organizations need to ensure information, applications, and IT systems are easily accessible to staff and authorized users and, at the same time, protected from harm and disruption while ensuring their cybersecurity plans are worth the investment. Possible controls here are not limited to technical solutions but are based on a balance among people, processes, and technology controls that support the business and mitigate the risk to the business.

Lastly, local regulations influence cybersecurity strategies. Inevitably, when organizations and industries fail to meet community expectations and address consumers' safety and security, the government's role is to step in through regulation. In some countries, governments have been proactive and built regulatory frameworks to support companies in their cybersecurity journey, directing them via guidelines, laws, and regulations. In Singapore, specific grants (such as the GoSecure program) are available to businesses as co-financed cybersecurity initiatives to expedite the adoption of basic cyber hygiene throughout the country. Other examples of government-backed schemes include Cyber Essentials in the UK and the Cyber Security Skills Partnership Innovation Fund in Australia. The level of involvement and role of governments differ from country to country and there isn't a one-size-fits-all model. What is clear is that cybersecurity needs to be a priority of all governments.

A CEO or a business leader needs to understand this before discussing, starting, or hiring their business cyber capabilities. Cybersecurity is not an IT problem—it is, *in actual fact, a business risk*.

With this necessitates understanding the challenges cybersecurity faces and how it is organized. In the next section, we will demystify the current cybersecurity challenges, focusing on the critical question: *Why do companies get continuously hacked while appearing to do the "right" thing?*

## Understanding cybersecurity challenges, organization, and reporting

Cybersecurity is a young and emerging profession. That is one reason why it is not fully understood or taken seriously by many C-level executives. While many CEOs and board members have extensive cross-functional experience in accounting, finance, marketing, or HR, few have much cybersecurity experience. As a result, cyber risks are not commonly understood in boardrooms. Many companies leave cybersecurity to the organization's **Chief Information Officer (CIO)/Chief Technology Officer (CTO)**, and cyber risk management is perceived as a cost confined to the IT department where it must compete for resources/budget against new initiatives for revenue generation, profit increase, customer acquisition, and so on.

A **Chief Information Security Officer (CISO)** who is responsible for the confidentiality, integrity, and availability of data often reports to a CIO or CTO. While this structure is common, it has proven ineffective due to the CISO's objectives regarding cybersecurity and associated conflict of interest with the CIO. The CIO aims to ensure the implementation of any business technology is completed within the required timeframe and budget, but security requirements might slow this process by requiring further checks and tests before the launch. In many cases, the security elements might not even be treated as a business priority.

When Hai (co-author of this book) was the CISO at Western Australia Police Force, he suggested to a senior executive, *"If security is responsible for the availability, integrity, and confidentiality of information, then perhaps the CIO/CTO should report to the CISO, rather than having to compete for organizational resources."* This was an attempt to shift the executive's mindset about how the role of security was perceived.

The senior executive's counterview was that security was kept *"healthy"* by competing with other business facets for resources. It is a fact, however, that *cyber risk is a business problem that can only be solved through collaboration, not competition.* Cybersecurity must be seen as an integral part of achieving business goals successfully. A product or service provided without the necessary safeguards in place to protect and the company will prove costly in the end.

IBM's *Cost of a Data Breach Report 2021* (<https://www.ibm.com/au-en/security/data-breach>) revealed that 2021 saw the highest average total cost of data breaches in the seventeen-year history of the report. This cost rose from \$3.86 million in 2020 to \$4.24 million in 2021, suggesting it is becoming more costly to recover from a cyberattack than to address security by design at the initial stage of technology adoption. It also shows that it goes beyond the capabilities of an IT department and its goals.

Having worked with IT departments across law enforcement, government, academia, and the private sector, Hai adds, *"I have seen that most IT departments do not have the capability and capacity to manage cyber risks or the skill set necessary to address technical security controls."* Some of the skills may be similar but the focus is completely different.

## Cybersecurity and information technology—similar skills but with a different focus

Left to the IT department, cybersecurity is often considered a technical issue, a cost center, and a low-priority task that competes for budget resources against other IT projects, most of which demonstrate better ROI for the business.

In Asia, approximately 10 percent of the companies Magda (co-author of this book) has interacted with have hired a CISO. In her many years of experience, most of Magda's customers rely on their IT teams, rather than cybersecurity teams, to perform cybersecurity tasks. A misaligned organizational structure such as the one where cybersecurity is a component of, rather than separate from, IT often leads to operational ineffectiveness and challenges.

This shows the challenges cybersecurity professionals have to influence business leaders within their own organizations. Cybersecurity executives are just like any other executive and should have the ability to communicate effectively. Even though their skills to perform their role might be mostly technical, having communication skills at the leadership level is critical. Unfortunately, security professionals have addressed cybersecurity for years using technical jargon. This trend has driven a wedge between cybersecurity leaders and businesses. It's crucial to communicate in nontechnical language.

As well, CISOs are expected to understand what their organization does from a business perspective and be able to speak about business strategies (and, in some cases, even customer engagement). A common discussion on social media revolves around how the CISO (or equivalent security executive) should communicate with and influence executives, and failure to do so effectively should be considered a failure of the security function.

Unfortunately, cyber is sometimes a thankless job, with an average eighteen-month turnover rate for a CISO. In an interview Shamane conducted with a group of APAC CISOs, they attributed stress as a key factor in why they leave a company, originating in part from a misalignment of views in the senior leadership team, as well as the wider culture of the company. There is only so much a CISO can do if they are unable separate cybersecurity from the IT department and effectively influence the necessity of a broader cybersecurity strategy and its need for the appropriate resources. In essence, corporate success is a team effort. It is commendable progress, therefore, that

as time goes by IT and security are increasingly being recognized as critical, and separate, components to professional success. Hai's career timeline and progression is one good example:

- In 2005, when Hai was the IT security manager in a government agency, he had five levels of management above him before reaching the **chief executive**.
- In 2009, when he was the associate director of information security at a university, there were three layers of management between his position and the chief executive.
- In 2013, as CISO of a police force, there were two management layers between his position and the chief executive.
- In 2020, Hai held both the CEO and **Chief Security Officer (CSO)** positions in a not-for-profit organization.

It is notable that, while on the surface, being appointed both a **C-level executive (CxO)** and CSO or CISO might demonstrate a commitment to cyber by making a CxO accountable for cyber through a secondary appointment as the CSO or CISO, CEOs need to appreciate having a CISO in the same way they would their **Chief Financial Officer (CFO)** or CIO. In a digitally connected world fraught with cyber risk, the CISO and their team help keep their organizations running.

The CEO needs to be an organization's cybersecurity leader and role model. They need to promote a cyber-safe, -active, and -responsible culture where each team member understands their responsibility for managing cyber risks to the business and recognizes that cybersecurity is not merely an "*IT problem*." Everyone in the organization has a critical role. Once in agreement with the cybersecurity strategy and roadmap defined by the CISO, the CEO needs to back its communication, adherence, and enforcement to ensure everyone in the organization plays a critical role to achieve cyber safety for the organization.

## Beyond technology—cyber risk is a business risk

When cybersecurity fails, it affects the whole business, not just the IT department. Just look at the reporting on the cyberattacks on Garmin, Toll, MyBudget, Travelex, and Lion, to name just a few. It's crucial to think

about cyber first and make it a business-wide joint function that coordinates security, finance, HR, corporate risk, and IT.

Tackling cyber challenges requires a strong security culture, prioritizing cyber risk and addressing it accordingly to keep it within an organization's risk tolerance. An organization is led by the CEO and supported by a team promoting the same values and goals. If the CEO supports a cyber-aware culture, all stakeholders will consider cybersecurity as part of their priorities and address it.

Cyber risk, while intangible, can be identified by the CISO, who then defines the right strategy and roadmap in alignment with the company's risk tolerance. The strategy should consider the previously identified cyber challenges, the company's current security control landscape, any gaps identified, and the roles and responsibilities of its workforce while maintaining alignment with the organization's business strategy, trajectory, and stakeholders. Everyone within an organization has a role. This handbook describes all business executives' responsibilities and expectations to achieve a resilient cyber-secure business.

The bottom line: cybersecurity professionals must be encouraged to avoid using technical jargon and align their thinking toward business impacts. Part of that includes taking technical language and terms and explaining it clearly and deliberately.

## Demystifying data breaches and cyberattacks

Let's examine two commonly interchangeable terms—**data breach** and **cyberattack**:

- A data breach occurs when personal information is accessed without authority. Data breaches, in general, are also personal data breaches, and they may be either unintentional or purposeful.
- A cyberattack is more severe than a data breach since it is likely to impact the organization more directly. It is a deliberate, intentional act.

Data breaches are just one of many different types of cyber risks businesses of all sizes and industries face daily. A data breach might happen without a cyberattack when there is a misconfiguration and unauthorized parties manage to access data.



The size and scope of a security event or data breach vary from one instance to another. A data breach or security event may have a significant financial and reputational effect on a business.

Although a security event may be mitigated by a timely, deliberate, and well-organized response, without sufficient preparedness, companies can undoubtedly be subjected to severe consequences from which they may never completely recover. The CEO needs to understand the impacts and financial consequences for a business when a cyber incident occurs and communicate it effectively to all stakeholders.

## Quantifying cyber costs versus return on investment

While some organizations have well-developed cybersecurity strategies and programs, most think they have adequate processes in place, and many more still believe they are not a target for cybercriminals. Those who think they have appropriate programs and those who think they are not targets have little to support their current comfort level, other than they have not yet experienced any discomfort. However, it may already be too late when they do encounter a cyber incident, which is inevitable. According to IBM's *Cost of a Data Breach Report 2021*, the average cost of a data breach in the United States is an alarming \$8.64 million.

Many small businesses would not survive such an expense, and larger businesses that can take on such a big expense would still feel a painful financial impact. In addition to the financial loss, other costs include direct and indirect losses following a cyberattack and/or data breach. There can be investigation or forensic costs, profit losses due to reputational damage, revenue losses due to business disruption, share value impact, incident response costs, customer notification costs, recovery costs, and so on. Everything just adds up.

As mentioned earlier, a data breach may result from a security event or incident, but it may also arise from a non-security-related event. With varying privacy and breach reporting regulations depending on a company's location, for example, the requirements and consequences of a data breach may vary.

When a security event or a data breach happens, companies must analyze a variety of criteria to determine the true financial ramifications, expenses, and losses. There can be significant expenses from a *data breach*:

- Notification costs might include fees, charges, and expenditures required to inform customers, regulatory agencies, and any other impacted parties who must be informed. Following the notice, a corporation should be prepared to respond to questions and clarify any issues that emerge as a result of the breach, as well as class action lawsuits. Those activities have a monetary cost.
- The expenses incurred as a result of a data breach may involve forensic investigations, a change in processes, improved security precautions, and compensation for losses or damages. These variables contribute to the company's financial losses after a data breach, both directly and indirectly, and are included in the cost of a data breach.

In the event of a successful cyberattack, a company might face significant interruption of essential systems, disruption to business operations, damage to the integrity of business data, and business stagnation. The different factors contributing to the financial impact of a cyberattack include:

- Direct and indirect expenses and third-party expenditures contribute to the company's financial losses following a successful cyberattack.
- Forensics costs, notification costs, and share value losses may be incurred in addition to the immediate business interruption, employee overtime, communication costs, and direct expenditures (such as recovery costs).
- On a medium timescale, the impact of a successful cyberattack might be a loss of customers, a decrease in sales, and a decrease in earnings. In addition, with time, this might lead to a reduction in market share, a decline in value, or a delay in an **initial public offering (IPO)**.
- The organization will need to assess the *overall recovery time* after a successful cyberattack. The interruption, whether days, weeks, or months, will impact a company's operations and finances, including expenditures associated with market recovery.
- In the event of a successful ransomware cyberattack, the organization may experience business disruption or operational paralysis. When a company's activities are interrupted, it suffers a financial loss. There is likely to be lower sales and higher labor costs; future income streams are lost due to possible reputational harm.

According to Comparitech, breached firms underperform in the market over time, growing 8.38 percent on average the year following the attack but still underperform the Nasdaq index by 6.5 percent. Target's data breach in 2013 is a fantastic example. Target experienced a significant data breach that exposed the personal information of about 70 million people. The cost of this data breach was estimated to be \$252 million.

For any company that is publicly traded, following a cyberattack there will be a stock price decline after a breach; it will take time for a corporation to reclaim whatever market share it may have lost due to the occurrence. Significant reputational damage as a result of the attack impacts the time it will take to recover, resulting in a greater loss of market share and more time needed to resume operations.

The 2017 WannaCry ransomware attack affected more than 200,000 computers globally across many industries. Users' files were held hostage until demands for a ransom payment in Bitcoin were met. With over 150 countries affected, this attack had an estimated cost of \$4 billion on the global economy.

All successful cyberattacks leave an impact that will affect an organization financially. Depending on the organization's sector, the extent of the damage will vary. Take, for example, a cyberattack against an **industrial control system (ICS)**—a breach of an ICS could result in property damage, such as fire or explosion, and even loss of life. Cyberattacks can have bigger ramifications than a breakdown of technology systems. Recovery from a cyber incident may not only be costly but lengthy as well, such that the business could be interrupted or stalled for a long period while the situation is being rectified.

The cost of a cyberattack is a complicated calculation that takes into account all of the ramifications that may occur. It goes well beyond the expense of restoring a server or an IT activity. In reality, it is putting a price on a business risk becoming a reality. The financial, reputational, and legal consequences of a security incident can be forecasted, with the associated financial losses also quantified. This quantification gives greater clarity and insight into the actual cost, and thus also the ROI on a cybersecurity investment. We will unpack this further in *Chapter 5, Working with Your CISO*.

Good cybersecurity enables organizations to build and protect their reputation and trust with their customers. To succeed, organizations need to ensure they have the proper risk management fundamentals, they have the appropriate structure for the cybersecurity team, and the relevant staff feel empowered to protect the organization. While the trend to elevate cybersecurity to the

C-suite is a step in the right direction, making it a secondary responsibility of another CxO is counterproductive. The CISO should have a seat at the main table.

With a clearer picture of the financial and reputational costs of a cyberattack, in the following section, we address the importance of cybersecurity awareness and creating a culture that builds and nurtures a cyber-ready company.

## Building a culture of cybersecurity

The CEO needs to lead in promoting a culture that reinforces the idea that cybersecurity is an organizational capability rather than just a problem for IT to solve.

A strong cybersecurity culture drives the members of the organization to behave in unison when faced with security challenges. An established, well-thought-out cybersecurity plan approved by the board of directors is only helpful if *every* staff member understands their role and responsibilities before, during, and after an event, appreciates the significance of cyber threats, complies with security measures and guidelines, and understands what it means to remain cyber-vigilant.

A cybersecurity plan needs to be approached holistically to be successful. Every part of the organization must understand that processes and technology play a critical role in developing and maintaining a robust cybersecurity culture. Cyber risk must be taken as seriously as risks such as natural disasters or acute illnesses. Most importantly, we must test, audit, practice, and rehearse cyber threats, keeping in mind the goal isn't to be 100 percent secure; there's no way to ensure that. Rather, cyber resilience is about understanding security threats, maintaining effective security controls, and having a swift and focused cyber-incident response prepared to reduce the impact of any incident.

Regardless of an organization's cyber maturity, the main cyber-resilience goal of any company should be the preservation of business operations, protecting the confidentiality of its data, and, in the event of a cyberattack, recovering as quickly as possible with minimal disruptions and losses. One of the biggest challenges is knowing where to start and what good cybersecurity practices and processes look like. It does not start with IT and cannot be left to the CIO or CTO.

Understanding cybersecurity at the board level does not require an understanding of security jargon or technical terminology. It comes down to defining the business risks that might materialize following a cyber event, such as a data breach, business disruption, or data theft.

When the board and management are aligned and clearly understand its cyber risks, their risk tolerance needs to be defined and agreed upon before building or discussing the cyber strategy.

Table 1.1 is an example of **risk considerations** for a business. The board and the CEO must acknowledge and consider cyber risks at the same level of priority as other risks for the organization:

Global top ten risks for doing business	
1	Unemployment or underemployment
2	Failure of national governance
3	Energy price shock
4	Fiscal crises
5	Cyber-attacks
6	Profound social instability
7	Failure of financial mechanism or institution
8	Failure of critical infrastructure
9	Failure of regional and global governance
10	Terrorist attacks

Table 1.1 – An example of high-level risk considerations

According to a study conducted by Allianz, 2,700 risk management experts surveyed in over 100 countries identified cyber incidents as the “*most important business risk*” in 2020, a vast difference from 2013 when it ranked 15th place (see <https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/allianz-risk-barometer-2020-business-risks.html>).

Table 1.2 lists the negative impacts of cyberattacks. Business stakeholders are more and more concerned about the implications for their companies and have started prioritizing cyber risk in their risk management process.

Rank	Business risk
1	Cyber incidents
2	Business interruption
3	Changes in legislation
4	Natural catastrophes
5	Market developments
6	Fire and explosions
7	Climate change and the increasing volatility of weather
8	Loss of reputation or brand value
9	New technologies
10	Macroeconomic developments

Table 1.2 – Types of risk by priority

The CISO is an invaluable resource and leader in helping an organization develop the most appropriate cybersecurity strategy, but they cannot do this alone. Once the board and CEO are aligned in their risk tolerance and a cyber strategy has been created and approved, it must include a plan to create a culture of cybersecurity and embed it within the organization. All staff must understand the fundamentals of cybersecurity instead of merely complying with policies and following technical guidelines. Senior management must lead by example. Cybersecurity strategies must align with business goals, be assessed against an organization's risk tolerance, be planned and executed accordingly through collaboration between business units, and not be in competition with other departments for resources.

Once an organization has established solid cybersecurity fundamentals across the board, once it is part of the culture, the business can operate effectively and without major disruptions or regulatory implications if a cybersecurity incident occurs.

The organization's cybersecurity strategy is a collaborative strategy that requires everyone's involvement, especially when the organization is undergoing a cyberattack or is suffering from a disaster caused by a cyberattack. Everyone in the organization, not just the CEO and the board, needs to understand that it isn't a question of whether their organization is breached but a matter of being prepared for *when it is*. The following section explores this in detail.

## Preparing a business for cyberattacks

Cyberattacks are generally targeted and very well defined, designed to cause maximum impact and disruption to business operations.

The CEO needs to prepare their business for such situations. Often, organizations wrongly believe that because they have an extensive security team, a cyberattack will never succeed. Or that because they have made a substantial investment to protect against attacks, a cyberattack will never be successful. Those are myths—100 percent security should not be a goal, nor is it a realistic target.

Securing your organization is about ensuring that if an attack does prevail, the business will be able to continue its operations. Resilience is about keeping your information assets accessible to the organization as much as keeping them safe. Such resilience builds trust among your customers and protects your reputation in the event of an attack. Hence, it is crucial to plan for failure, including security control failures. Preparing for failure ensures your organization can survive and continue to operate while other preventive measures are built over time. This will help you cope with the threat of a cyber incident and prepare your business to deal with other disasters.

Gillian Findlay, board member and former CEO at Vamp, a global branded content platform, and former **Chief Operating Officer (COO)** at Australian **Software as a Service (SaaS)** unicorn SafetyCulture, shared a typical CEO's concerns: *“There are so many cybersecurity issues that should be front of mind for any CEO, but ransomware has become the most front of mind. We cannot expect end users to protect their company from this threat, so companies must secure end-user devices while enabling the employees to work efficiently and effectively. Otherwise, ransomware breaches will continue to blight our lives.”*

While many CEOs and boards might consider the risk of becoming a victim of ransomware is minimal, or might think their IT department will restore from backups while the business reverts to manual processes, very few organizations have put that to the test. Those that have done so were forced to because of a real crisis, and they quickly discovered that reverting to manual processes or restoring backups was easier said than done. We will discuss **business continuity plan (BCP)** further in *Chapter 7, The COO and Their Critical Role in Cyber Resilience*.

Preparing a company in the event of a cyberattack must be a top priority for any CEO. A CEO should make a security strategy a focus upon assuming the role. Next, we discuss cybersecurity considerations as part of a CEO's leadership assignment and risk assessment for the first month of their tenure.

## Cybersecurity considerations for a CEO's first month

With so many pressing issues requiring their attention, many newly appointed CEOs overlook the importance of cybersecurity in their first month or even first year on the job. That is a mistake.

A newly appointed CEO needs to ensure a CISO and their team are in place and working effectively while becoming familiar with the organization's cyber risk posture, from its cyber risks and risk appetite to risk tolerance. Unfortunately, threat actors and cyber risks will not wait until a CEO is ready. Some cyber criminals may also view a leadership change as an opportunity to attack if they believe an organization is unprepared. This also concerns mergers and acquisitions. A cyber disaster could ruin a CEO; a cyber event leading to significant data loss, data theft, or business interruption may jeopardize the CEO's reputation, position, career, revenue, and operations.

A newly appointed CEO should prioritize reviewing their **cyber incident response preparedness**, BCP and **disaster recovery plan (DRP)**, along with evidence that these plans have been regularly tested and updated. The plans must include and adequately address technology considerations and vendor support. Having a current and well-rehearsed incident response, BCP, and DRP will ensure an organization can quickly recover and resume operations in the event of a cyber disaster.

Ideally, the BCP should encompass the cyber incident response. However, Magda has also witnessed a lack of integration during her work in Asia, where the BCP remains focused on a simple IT DRP and doesn't consider a significant cyberattack. An IT DRP is unlikely to hold up against a well-planned cyberattack.

A communication plan is a key element of cybersecurity planning. The CEO must consider their visibility in an organization's crisis communication plan. To this end, templates and guidelines for communication from the CEO to staff, media, customers, and the public should be included in the



BCP. Communication in the event of a cyberattack is critical for reputation management and maintaining customers' trust. A mismanaged cyber communication plan will undoubtedly impact the share value of a business.

The communication plan is merely one element. The CEO must address tactical issues of ensuring an appropriate incident response, effective business continuity, and disaster recovery with a sound **security strategy**.

If an organization does not have an established cybersecurity strategy or team, within the first month, the CEO needs to prioritize establishing one immediately. This begins with understanding and communicating that cyber risk is a major concern to the company's board of directors and seeking approval for a cyber budget. If there is no internal expertise available to identify and lead discussions to address and define the organization's current cyber exposure, residual risk, and risk tolerance, the CEO may engage an external cybersecurity consultant while hiring a CISO to build internal capabilities.

A cyber-resilient business identifies its cyber risks beyond the IT department, defines its risk appetite and tolerance, and builds its cybersecurity strategy, which is then embedded into the business's operations and activities as a fundamental must-have and not an afterthought. It's not an easy task, but it's a necessary one for any CEO to take at the outset. Fortunately, there are some specific questions that can be asked to assess an organization's cyber risk coverage.

## Questions to ask yourself as a CEO when considering your cyber risk coverage

How does a CEO determine what the organization's cyber risk coverage should be? A challenge for non-cyber executives is knowing the right questions to ask, such as:

- Does my organization consider cyber risk within the enterprise risk management process, or is it still considered an IT problem?
- Are all in the C-suite held accountable for cyber risk, or has it been left to the CIO or CISO/CSO?
- Do I understand the organization's assets, including intangible ones?

- Do I understand that my organization's cyber strategy should be based on identifying risks, mitigation/transfer/approval of cyber risks, response, and recovery?
- Does my organization recognize residual cyber risks and understand its risk appetite and tolerance?
- Has the organization quantified cyber risks, and does it understand the impact and likelihood of such events?
- What is my current security risk posture, and how do I know the controls are working effectively?
- Have I considered the damage to the brand, reputation, and trust of the organization resulting from a cyber event?
- Does the organization have an effective BCP/DRP, and when was it last tested?
- Is my organization ready to respond and recover?
- Is my organization able to prove due diligence and due care following a cyber incident or could the shareholders/regulators consider my inaction negligent?
- Does my organization understand that 100 percent security does not exist?

These questions are not mere one-time questions a CEO or board of directors should ask. Such questions should be asked repeated and addressed as part of a company's security strategy and processes adjusted based on the answers.

## Summary

In a digitally connected world, organizations are dependent on information and technology now more than ever before. This state of affairs exposes organizations to global threats, some even sponsored by nation-states. Cybersecurity not only ensures your organization continues to operate in these challenging circumstances, but good cybersecurity increases customer trust and brand reputation, too.

CEOs and boards of directors should develop a healthy cybersecurity culture that encourages an entire organization to embed cybersecurity into all aspects of people, processes, and technology. These are some of the essential fundamentals you've learned from this chapter. Finally, cybersecurity needs

to be considered a business need, complementary to business functions instead of competing with them.

The following chapters will examine what roles other CxOs play in cybersecurity, starting with the CFO.

# 2

## A Modern Cyber-Responsible CFO

A **Chief Financial Officer (CFO)** is the senior executive in charge of a company's financial operations. A traditional CFO will typically act as a **financial controller**, which is more detail-oriented, and even if they are not from a financial background, they manage just the numbers and focus on transactions. A more modern CFO will be very forward-thinking. *They manage risks and the future of the business.*

While the **Chief Executive Officer (CEO)** sets the direction, culture, and budget for the company, the CFO is the agent of change, supporting that direction, implementing the company culture, and preparing the budget for the CEO.

**Enterprise Risk Management (ERM)** is a strategy across an enterprise, designed to identify potential events that may affect the company's finances, operations, and objectives and keep risk within the parameters of the company's risk appetite. The CEO's commitment and that of every management team member, including the CFO, are critical to the success of ERM adoption and execution.

The executive team's contributions, particularly in risk management, are required to meet the organization's strategic goals. Nowadays, this requires considering cyber risk and integrating it into ERM.

The CFO's job description is straightforward: cash flow management, financial planning, and financial reporting. Furthermore, their responsibilities include determining the firm's financial capability and taking remedial actions to effectively and efficiently manage the firm's risk. Each company has its own set of financial modules, and ERM is implemented using these modules. ERM can be an important tool for the CFO in helping them understand the potential impact of business risks on the business's financial standing. This means that if cyber threats pose a risk to the business, then the CFO needs to understand what this means and how it can impact the organization's financial position.

CFOs have a big say in implementing enterprise risk management, which should include cyber risk; they control the implementation of the ERM strategy. The adoption of ERM requires financial and operational resources and a thorough assessment of the likelihood of success.

This chapter discusses the main priorities for a CEO to consider when talking about the CFO's financial strategy and involvement in ERM. In this chapter, we're going to cover the following topics:

- Why the CFO should care about cybersecurity
- The CFO's understanding of cybersecurity
- The aspects of cybersecurity the CFO should consider
- Defining the CFO's role in building cyber resilience
- Communicating with the CFO about cyber risks
- Questions to ask your CFO

The following section provides further details on specific areas where the CFO remains an indispensable stakeholder in cyber risk management.

## **Why the CFO should care about cybersecurity**

As the senior executive and virtually the top-level financial controller responsible for managing the business's economic actions and financial risks, the CFO should care about any risk that may impact the organization's financial position, including cyber risk. They should play a crucial role in supporting an adequate cyber budget that enables building cyber resilience across the organization. If done right, the management of cyber risk can

also aid in the growth of an organization as well. There is a compelling need for CFOs to have a more active role in critical business decisions beyond financial performance disclosure and to play an active role in cyber risk management is growing.

## The role of the CFO in cybersecurity

There is a difference between a CFO who loves transactions, modeling, and details, and one who focuses on driving strategy and the story behind the numbers. The modern-day CFO does not just add up the numbers. They are meant to support the CEO, even when most CEOs are often more eager to take risks or find new business opportunities. The CEO is usually the one driving change, and they will want the CFO to be in their camp. The CFO is the person overseeing mergers and acquisitions and has the inspiration and motivation to take a business to the next step. They serve on the board of directors and participate in decision-making as a member of the senior executive team. As well, most organizations rank CFOs second to the CEO in any public involvement. Your CFO is your *communicator*.

For organizations that do not have a **Chief Risk Officer (CRO)**, the CFO is often the one to take on that role as well. The CFO can play the role of the CRO in tackling ERM and making decisions about risk treatment, transfer, and mitigations. Therefore, in a digitally connected world with increasing levels of inherent cyber risk, the CFO is integral to building business cyber resilience.

Integrating cyber risk into ERM is gaining traction among firms; businesses are using it to detect and manage cyber risk. ERM takes a holistic approach to risk management rather than a siloed one. It necessitates the integration of various processes to quantify an organization's exposure to uncertainties that may interfere with the business's goals and development capabilities.

These days, cybersecurity is typically in the top five risks for a corporation. A key aspect of the CFO role is to help manage that risk. Viewing cyber risk through the lens of ERM equips the CFO to position the company to manage the strategy and plan for cybersecurity. This is a practical way to align cyber risk with how the company perceives risk in general and provides a familiar environment for the CFO to get educated about the dialog on cybersecurity in a business context.

Cyberattacks present a serious economic concern for companies and business stakeholders. While awareness is increasing around the topic, there is a risk this perspective may be misinterpreted throughout an organization if a **Chief Information Security Officer (CISO)** and a CFO do not communicate and discuss cyber risk effectively with every member of the organization. The lack of communication about the organization's cyber resilience means the business may not be prepared to face cyberattacks effectively and resulting financial losses might be substantial. Those economic losses ultimately need to be quantified to support an informed decision-making process between mitigation and transfer.

Despite not being cybersecurity experts, CFOs are not in a position today to ignore the topic or continue writing it off as an IT problem. The CFO has the expertise and supervision to look at the impact of an attack on the business's financial position in a much broader and long-term manner, going beyond the immediate concerns of data loss and operational disruption to reputational and regulatory losses, as well as the impact on share prices. At the same time, if done well, having a strong cyber posture can also aid the organization in its rapid growth as well. A company that is cyber resilient will only serve to strengthen the business and give employees the peace of mind to flourish and perform to scale.

In the next section, we explore further how a CFO's cybersecurity understanding can support cyber resilience.

## The CFO's understanding of cybersecurity

Shamane Tan, chief growth officer at Sekuro and founder of Cyber Risk Meetup, a global community for prolific cybersecurity conversations and exchanges, and co-author of this book, commented on a discussion with the CFOs that she was involved in: *“Even amongst the CFOs, they recall that the conversation about cybersecurity only started to come up a decade ago when the insurers asked corporate CFOs what the company was doing about cybersecurity.”*

When insurers began asking about cybersecurity over ten years ago, it was likely one of the first times CFOs would have heard about cybersecurity. It's worth noting that these first conversations did not begin within an organization but were driven by those asking from outside the organization. Within an organization, it has not been a concern generally. Magda (co-author of this

book) had a CFO mention to her that he trusted his security team and so wasn't going to purchase cyber insurance.

With the increase in cyber risk and inevitability of cyberattacks, it is critical to understand that foolproof security does not exist. Within such a complex and interconnected environment, cybercriminals nowadays can find weaknesses within people, processes, and technology. A cyberattack can also happen through a supplier or vendor. It is just a matter of time.

A group of hackers known as "London Blue" targeted more than 50,000 finance executives, including 35,000 CFOs, with bogus requests to transfer money. The scams were estimated in an Agari report (<https://www.agari.com/cyber-intelligence-research/whitepapers/london-blue-report.pdf>) to have caused hundreds of thousands of dollars in damage. CFOs and the finance executives within an organization are not immune to being targeted and are not necessarily cyber-savvy to such scams. That must change.

In today's world, insurers take cyber risks into consideration and provide cyber insurance to organizations as a risk transfer option. This requires risk profiling of a company. Cyber insurance helps CFOs to become cyber aware and requires a shift in their perception of cyber risk. This switch in mindset also correlates directly with both the frequency and the cost of cyberattacks. As a result, cybersecurity is now formed as part of the risk register.

Nevertheless, for CFOs, understanding cyber risks and cybersecurity as a whole can be a lengthy and frustrating process. Cybersecurity is complex, the solutions not always enough to mitigate risk, and confusing technical jargon are just a few of the reasons CFOs find it challenging. Your organization might have cybersecurity hardware and software to protect your business against cyberattacks. However, it only takes one weakness to incur financial losses.

People, processes, and technology are not immune to cyber threats. Specific to the finance team, phishing, social engineering, and **Business Email Compromise (BEC)** have been some of the most common cybercrimes. The FBI's **Internet Crime Complaint Center (ICCC)** cybercrime report found BEC schemes to be the costliest of all cybercrimes, leading to losses of approximately \$1.8 billion in 2020 alone.

A good example is an employee processing the payment of a fake vendor invoice, which can lead to the misdirection of tens of thousands or even hundreds of thousands of dollars. Those social engineering cyberattacks work



by targeting humans and processes. This type of cybercrime has increased in recent years, and while some companies have addressed this cyber risk to prevent financial fraud/loss, others continue with their traditional approach and ignore critical cybersecurity pillars, people, and processes. “It can’t happen to us” remains the pervasive perspective.

Importantly, a CFO is not required to learn technical cybersecurity concepts. But they do need to consider cyber risks that might materialize from a weakness in people, processes, or technology. Understanding and communicating that foolproof security does not exist is among the first steps, along with increasing the budget to help address strategic initiatives. Further, it requires continuous support and the company’s readiness to respond when an attack happens.

It is also worth noting that when it comes to cyber insurance, not every single cyber event will be covered, which means that companies will not be able to transfer all of their risk through insurance. Take, for instance, a ransomware attack—insurance companies now deny insurance payouts for ransomware payments.

Yet ransomware attacks are only one cyber risk to a company. The following section outlines key aspects of cybersecurity that are helpful for CFOs to consider.

## **The aspects of cybersecurity the CFO should consider**

Cybersecurity is a conversation that needs to be had at the boardroom level, as the impact of a cyberattack can have enormous consequences on customer trust, brand loyalty, and shareholder value. When the CISO starts the conversation, the CFO must be a supporter. Just as finance authority is delegated across an organization, so must cyber resilience. However, cyber risk is more complex than financial risk; one aspect of that complexity is that there are no monetary limits you can establish for who responds to a cyberattack. In other words, everyone needs to have a role and everyone owns a piece of the protection and recovery—and financial losses.

Cybersecurity goes beyond the effectiveness of the right technical controls, such as firewalls and authentication. For too many, a security event is commonly seen as the failure of technical controls, which is why the reported cost of a security breach is often considered as just the cost of the initial impact.

Yet that's only part of the financial picture, and often a small part. What is often forgotten is the aftermath of things such as regulatory fines, lawsuits, and loss of the business's reputation.

Part of the modern-day CFO's role is to quantify risks and inspire change by using numbers to tell the story of managing cyber risk. With a focus on *data, data, data*, undoubtedly the most valuable commodity for any organization, the CFO can ensure it is leveraged and analyzed to help make more efficient business decisions. Cybersecurity is one of those business decisions.

Investments in the right security are required to help protect this data. If a business survives an initial attack, the recovery time can be very long and costly. The CFO must consider data value and cost, including data breach costs, cyberattack costs, cybersecurity **return on investment (ROI)**, prioritization of cyber initiatives, and proper vendor due diligence. The foundational mindset when it comes to cyber resilience should be *prevention first*. Baseline housekeeping includes running a tight IT function and maintaining patch currency, and basic cybersecurity hygiene can provide enormous benefits at a relatively low cost.

The good thing is that the CFO is not alone in this fight. CISO Rahul Khurana has reported to CIOs and CTOs in some of the organizations where he has worked. Now as the CISO for a global healthcare and defense technology company, he reports directly to the CFO. He shared his experience of being in this different reporting structure:

*“Our discussions are very focused on the overall business risk. CFOs have a clear understanding of the business impact of a cyber breach (whether it's financial, legal, reputation, and so on). It's all about the impact on revenue. I also have an independent cyber budget; I don't need to fight for a cyber share under a common enterprise IT budget. It's easy to talk numbers and return on investment through cost avoidance.*

*“Every dollar invested in cybersecurity (people/process/technology) that eventuates in reduction of cyber incidents or an overall impact of an incident reflects a return on investment—from a monetary, risk reduction or improved maturity and capability. It makes a big difference to have direct access to the CEO and the board. They are open to innovative ideas and approach when we have a business focus mindset.”*

The CFO needs to collaborate with the CISO to navigate investments and costs (such as security controls) and the complexities of financial protection (including reputational loss and lawsuits). It is important for the CFO to clearly understand how to achieve those outcomes to make the right decisions and produce proper financial forecasting. Budgets and investments in cybersecurity increase each year as new threats and defense technologies are created.

CFOs have a unique opportunity to approve funding for security solutions that will help protect a business or supplement (not replace) those solutions with a financial instrument, such as insurance. They also have to avoid overspending on products that prevent the business's growth in the name of security. The CFO needs to balance between overspending, which leads to a false sense of security, and under financing security initiatives, which can result in a higher risk across the broader infrastructure. CFOs must recognize cybersecurity as an investment to protect against financial losses rather than a burden or expense.

This is only achievable if the CFO understands and clarifies the financial impacts of a cyber event in dollars.

## A CFO's perspective

Wayne Andrews, CFO at the University of Sydney, revealed that his key consideration in planning and budgeting for cybersecurity is to first establish the organization's risk tolerance: "*It is infinitely costly and impossible to eliminate cyber risk entirely, (although CIOs would spend any amount in pursuit of that goal), so the question is how much risk can you tolerate and what it will cost to narrow your exposure to within the tolerable range.*"

The *risk tolerance* discussion focuses on establishing tolerance and understanding the spectrum of risk, making the expenditure level a mere consequence of the process.

Wayne finds it fanciful to attempt a cost-benefit analysis on cyber expenditure because the range of outcomes can be so broad and the consequences of an actual event so large. The absolute numbers are so asymmetrical and the probabilities are very subjective. It can only be done in a meaningful way by narrowing the range of acceptable outcomes and the cost of delivering them.

Wayne concluded, "*This is important because if your starting point is to eliminate all risk, you are doomed to fail in that regard and spend much money in the pursuit of failure.*"

It is like having an insurance policy and never needing to cash it in. Companies spend a lot of money, but they might not really know the full extent of the cost at the end of the day had they opted out of insurance.

Is there a way to demonstrate the number of near misses or quantify what we have saved ourselves from? Perhaps another way to look at it is by benchmarking against your peer companies cyber resilience and deciding you will be less affected by cyberattacks because you have a more substantial cybersecurity capability.

For most businesses, the objective is to be sustainable and ensure the company has a future. That half a million dollars you spend on cybersecurity risk management becomes your return on the objective. Although it might not necessarily translate to, “*I just saved my company \$10 million,*” efforts need to meet organizational requirements to thrive.

## Addressing cyber risk from a complex financial view

Wayne also offers this view: “*Can an organization balance some risks against a cyber insurance policy? There is no free lunch in this regard. What insurance can do for you is deliver the funds at short notice to remediate, including ransom payments; however, insurance will not restore your business and reputation, so it is a means of smoothing cash flow rather than eliminating risk. Indeed, you will find yourself uninsurable unless you have a credible cyber risk management program.*”

Regulatory compliance is one approach to building a credible cyber program. Some regulations with more comprehensive applications, such as the European **General Data Protection Regulation (GDPR)**, might require a solid focus on potential data breaches. The GDPR has steered the topic of the regulatory necessity of data protection into every business conversation and a notification process that requires a quick turnaround. The fines are massive, and companies cannot afford to be hit by a penalty of millions of dollars.

**Payment Card Industry Data Security Standard (PCI DSS)** compliance (where applicable to a company) is also another useful scheme to translate security controls into actual monetary fines. PCI DSS is technical in nature and designed to protect financial information. It is in your CFO’s interest to comply with this, as enterprises will need to meet this standard to instill confidence in customers. How is your CFO currently collaborating with

your CISO to oversee these compliance and cybersecurity requirements, spending, and potential losses?

We hope it is becoming clearer why the CFO's role in cybersecurity is important. Next, we go into further detail about the relevance of the CFO's role in building a resilient cyber-ready business.

## **Defining the CFO's role in building cyber resilience**

Cyber risks are now one of the most troublesome risks for CFOs. The CFO should be able to collaborate with the CISO and fully participate in a robust discussion about cyber risk with the board, the rest of the organization, and external stakeholders and position it as a business and commercial risk, mitigated through a variety of measures, not all of which are technological.

The CFO and the finance department are highly trusted and skilled when it comes to explaining the business reasons behind the financial limits and controls they put in place; thus, they should leverage this to promote cybersecurity. In the case of an attack, the CFO will, understandably, be one of the first to evaluate the possible harm and to lead, with the CEO, both internal and external actions and messages to essential stakeholders.

The CFO can improve an organization's cyber capabilities—and help fulfill the board and senior management expectations—in crucial ways. We will explore these in the next sections.

## **Benchmarking cybersecurity budgets**

The CFO may assist the CIO and CISO in determining the appropriate cybersecurity budget. Leading CFOs compare their company's cybersecurity budget to their industry peers. Magda has received continuous requests for benchmarking data from CFOs. The benchmarking requests extended beyond cyber risk mitigation to cover cyber risk transfer. If a CFO sees that the industry average for cybersecurity budgets is 10 percent of the IT budget, and their firm allocates just 1 percent of the IT budget to cybersecurity, it is likely underinvesting.

Benchmarking is a great starting position for the CFO and helps them determine whether they are spending too much or if they are underspending. This will then help adjust the budget before allocation.

## Defining cybersecurity spending

The CFO needs to collaborate with the CISO to define fund allocations and spending. An organization must assess whether funds are invested in the right initiatives. This assessment helps evaluate whether the business is spending the correct amount on the proper initiatives, given its cyber risk exposure. There have been situations where companies invested in costly tools while not having cybersecurity fundamentals in place, such as vulnerability management or two-factor authentication for administrative access. Even the best tools are ineffective without basic systems to support them.

“Defining spending” should be renamed “cyber spending allocation,” which talks about smart allocation and how the CFO can help spread and amortize expenditures across multiple budgets, and even allocate percentages of spending from other departments’ budgets to help with security. CFOs are in a unique position to do this because they have a holistic view of the budget. They are also able to evaluate risk and apply it to the allocation of cybersecurity resources as not every department’s needs will be equal.

## Supporting cyber-risk quantification

The CFO’s dollars-and-cents attitude is handy for analyzing cyber risks using a quantitative rather than qualitative approach, ensuring that business and risk values are quantified equally. Traditionally, cybersecurity professionals have not quantified cyber risk, presenting it instead using qualitative methods. While helpful, this approach is limited when requiring objective spending assessments and prioritization. While risk management practitioners have used these models for other types of risk for years, they are only now being applied to cybersecurity. Once presented, if the board remains unsatisfied with traditional security reporting, it may look at aligned visibility with other risk types as part of ERM. This requires financial figures and adequate forecasts to support their strategic business decisions. The CFO should provide these insights and help quantify cyber risks in collaboration with the CISO.

Magda has collaborated with forensic accounting professionals who were able to deliver incredible insights by quantifying values based on cyber risk scenarios. For example, they were able to clearly calculate possible financial losses for all types of business interruptions, including profit loss, employees' overtime, and third-party expenditures, among others. This demonstrates that the CEO and board members can only guarantee that resources are spent efficiently by measuring both the cyber risk and the organization's risk appetite as the cost of protecting against cyberattacks rises.

Risk quantification is really important and is how the finance team can help the CISO here. If the CISO can identify risks, then the finance team can quantify financial impacts, which helps with prioritization. Risk underpins all decisions made in an organization, and one way to quickly address risk is by transference.

## Purchasing cyber insurance

Traditionally, CFOs purchase corporate insurance in collaboration with insurance managers. As with any type of insurance purchased on behalf of the company, they also manage the evaluation and underwriting of cyber insurance and oversee auditing, inventory, testing, and compliance. Insurance is a contract in which an organization receives financial protection or compensation from an insurance firm guaranteed in a policy. Purchasing insurance is a supplement to risk management in terms of safeguarding your company.

As cyberattacks can lead to financial losses, cyber insurance might cover those financial losses, helping with cash flow and liquidity management. A detailed and intelligent risk management strategy considers mitigation and transfers of cyber risk. There is always a residual risk that might materialize, impacting the company's financial posture. If that risk occurs, the insurance compensates for the damages.

Insurance is an uncommon but important risk tool in the cybersecurity world that helps quickly reduce risk; it does have a direct correlation to the costs incurred by the organization. The downsides of insurance are that it does not cover everything, and insurance companies are starting to reduce the scope of insurance payments. As with the purchase of any policy, strict scrutiny of what is and is not covered must be part of the due diligence process.

Having a solid cyber program to address security hygiene issues will help to reduce insurance premiums, which offers a better ROI than spending on premiums. However, there is still a blind spot for many organizations, one that is often not covered by cyber insurance, and that is third-party risks.

## Assessing third-party risks

CFOs are often key players who defines the procurement process. Supply chain risks have increased tremendously, and thus supporting cyber risk assessment procedures undertaken on your vendors and suppliers before working with them should be a priority for the CFO. In some organizations, the CFO owns the third-party risk management function, while in others, this can be shared between the procurement team (finance), risk team (under the CRO), and also the security function (under the CISO).

Cybersecurity budgeting, spending, and risk quantification are all part of the CFO's responsibilities in building cyber resiliency. Yet identifying and recognizing cyber risk is the role of everyone in the organization. It is, therefore, incumbent upon everyone to communicate those risks effectively. The following section provides tips for communication with your CFO.

## Communicating with the CFO about cyber risks

Shamane explains, *“Language is important. Traditionally, the CFO has always been familiar with ROI. However, it can be a challenge for many to quantify the return on investment in cybersecurity.”*

Often, cybersecurity is under the surface, not recognizable or acknowledged, but protecting the company from cyber threats. There could be all this activity going on, but the CFO may not see any positives from it, as they are not aware of how many incidents were avoided or how many near misses there were. The CFO sees it for what the tools cost the company, not what it has saved the company.

As many CFOs have shared with Shamane, *“you can usually measure the cost to the organization after an attack, but if the company has not been compromised, how would one know what cost has been saved?”*



So how do others in an organization assess cybersecurity threats and needs? Measurements such as lead and lag indicators can be helpful in assessing this. Your lag indicators are your after-the-fact financial fines and the cost of responding to an incident that can be seen, for which we have available quantifiable measures.

Lead indicators, on the other hand, involve the use of loss-curve projections or **Factor Analysis of Information Risk (FAIR)**, which falls within the “traditional” risk calculation of likelihood and impact. FAIR is a known quantitative model for information security and operational risk. FAIR offers a paradigm for understanding, assessing, and measuring cyber and operational risks in financial terms.

The good news is innovative quantification methods are emerging. One way to quantify cyber risk—developing a cyber-specific **loss curve**—can help companies develop a meaningful capital risk framework for cyber and answer those difficult questions, including ROI. Additionally, scenario building can be used to understand the consequences of cyberattacks and ensure accurate modeling for cyber risk quantification.

Moving from qualitative to quantitative frameworks for cyber risk is a journey in itself. However, quantitating the risk provides the ground for a better discussion with your CFO. It takes practice and a different perspective, but it’s considerably more successful in gaining comprehension and keeping your CFO’s attention on the topic.

Magda has long practiced cyber risk quantification and firmly believes it empowers security professionals to communicate efficiently with business stakeholders and align cybersecurity strategies with business goals. After all, assessment is only one element. It must be presented to the CFO. In doing so, avoiding technical cybersecurity language when discussing or giving advice to the CFO, who doesn’t have a background of cybersecurity expertise, is critical to guarantee they understand cyber risks and can take part in a discussion. Therefore, the facts must be delivered in a language they can comprehend for them to confidently understand the topic and especially the requests, if any. This is where cyber risk quantification is used. It aligns with the CFO’s language—*financial losses*.

Thus, when starting a discussion with your CFO, it is crucial to leverage familiar topics to find a middle ground. Cybersecurity is a complex topic for a CFO, as is financial planning for cybersecurity professionals. The goal is for the CEO and CISO to collaboratively consider various factors of the

CFO's recommendations to understand the actual financial implications of costs and losses if a security incident or data breach occurs.

## Economic costs

Financial costs can be straightforward, and immediate, as penalties and fines. Then there are the notification costs, which can include necessary fees, charges, and expenses incurred to notify individuals, regulatory bodies, and other parties that require notification of a breach. Then there are cost-related activities as a result of replies to inquiries and other matters of clarification and legal consequences.

Data breach costs might include forensic investigations, with potential outcomes an apology in the form of compensation, a change in procedures, improvement of security safeguards, and/or payment of compensation for loss or damage suffered. In Japan, for example, apology money is paid to affected individuals. All these factors directly and indirectly increase the company's financial losses following a data breach and should be assessed as part of the total data breach cost.

In the case of a successful cyberattack in general, a business might suffer significant impacts, such as disruption to core systems, corruption of databases, business paralysis, and so on. Traditionally, security incident impacts are classified as financial, reputational, and legal. However, if not quantified, it might lead to a lack of accurate cost visibility.

Additional economic costs include financial losses arising from direct and indirect costs and third-party costs. Besides the immediate disruption, employee overtime, communication costs, direct costs (recovery costs), and share value loss might also arise. There is also the potential loss of customers, loss of sales, and a reduction in profits in the medium timeframe. This might result in a drop in market share, valuation, or a delay in an **initial public offering (IPO)**.

In the case of a successful cyberattack involving ransomware, the organization might face business interruption or operations paralysis, both of which have financial implications.

One of the goals of communicating with the CFO and appealing to them in language that they understand—financial losses—also serves to redirect the mindset they have when it comes to cybersecurity and resilience.

## Mindset

There has been an intentional shift in recent years to focus the needs of cybersecurity on the **return of value (ROV)** or **return on objective (ROO)**. Think about it from the perspective of a nation's defense strategy. Billions are pumped into military strategies and advanced artillery warfare equipment in a bid to be prepared to fight a war and save as many lives as possible if it ever comes to it. We never hope for war, but we still prepare for it.

This section discusses a new perspective and an innovative approach to the assessment of cyber risk into the financial function. Traditional cybersecurity frameworks did not empower security professionals to lead business discussions and created various challenges for business stakeholders to recognize the value and necessity of cybersecurity. Quantifying plausible financial losses and discussing them in terms of cyber risk scenarios are key factors in facilitating collaboration between security, finance, and ERM. Fortunately, there are questions designed to draw out your CFO's views and understanding of cyber risk and also challenge them on ways they should take a more active role in advocating for cybersecurity.

## Questions to ask your CFO

These questions will help facilitate a healthy discussion with your CFO and explore ways they can work more effectively with other executives in addressing your organization's cyber resilience gaps and uplift program.

- Have you considered cyber risk as a part of ERM?
- As a CFO who manages the financial risk within an organization, how can you become a champion of security in the boardroom?
- How can you shift your starting point from eliminating all risks to narrowing the range of acceptable outcomes?
- How do you understand the implementation of cybersecurity hygiene? Is it more than just firewalls and authentication?
- How do you ensure cyber risk quantification and financial optimization?
- Are you confident that cyber risk needs to be addressed with a balance between mitigation and transfer? Have you considered cash flow management and risk transfer through cyber insurance?

- How are you working with the CISO and CIO/CTO to adhere to regulatory requirements such as GDPR and PCI-DSS requirements?
- How much time are you spending with the CISO and CIO to do a business review of the cybersecurity environment?

## Summary

In this chapter, we addressed that CFOs must recognize that the danger to cybersecurity is constant—attacks continually test the defenses of both big and small firms. CFOs must also consider the possibility they have been already compromised and are unaware of it. A perimeter of defense doesn't exist anymore, with employees working remotely permanently or more often. This has a significant impact on business exposures and cyber risk.

CFOs and finance executives must consider cybersecurity risks and use it to reframe and reposition cybersecurity management as a strategic business risk. CFOs must assist in risk management by ensuring that an organization has appropriate resources allocated to all categories of risk management, including cyber risk.

Finance plays a critical role in risk assessment and governance throughout an organization. Cyber is one of these risks, but given the potential for monetary loss, it should be one that finance has a significant influence on.

In the next chapter, we will discuss the role of the *Chief Risk Officer*. This chapter will identify the biggest challenges and misconceptions currently faced when it comes to cyber risk and ERM.



# The Role of the CRO in Cyber Resilience

The **Chief Risk Officer (CRO)** is a senior executive responsible for the identification and assessment of business risks that may adversely impact your organization's profitability and productivity. They champion **Enterprise Risk Management (ERM)** efforts by leading risk management strategies and are responsible for the risk identification and mitigation procedures. In some organizations, the CRO heads a risk committee consisting of executives from different departments, such as finance, operations, IT, sales, and HR.

The CRO's approach to risk management has evolved with how we do business in the age of cyber threats. Risk management techniques in business have had to adapt to the fact that most companies are now technology-dependent or rely on **Information Technology (IT)** to run their business operations. The risk management role evolves as a business's scope, size, and value shifts, and each category of risk (operational, cyber, and financial, among others) necessitates its own risk frameworks and applicability.

This has resulted in a significant transformation in the understanding of the risk management process by various stakeholders, especially for cyber risk where many risk professionals appear to have a particular knowledge gap. This is illustrated by how most risk professionals still refer to the **ISO 31000** standard when discussing cyber risks, despite the fact that **ISO 27005** is more focused on cyber risk.

- ISO 31000 is the international standard for risk management. It provides a framework and guidance for managing risk throughout an organization. ISO 31000 is designed to help organizations identify and manage risk in a more systematic and proactive way. The standard can be used by any organization, regardless of size or sector.
- ISO 27005 is the international standard for information security management. It provides a framework and guidance for managing information security throughout an organization. It complements ISO 27001 and ISO 27002 by providing the best practices for managing the risks related to information security.

With widespread digital transformation and technology adoption accelerated by the COVID-19 pandemic, today's CROs need to ensure *digital risks* are included in their organization's risk registers, and update risk matrices to better reflect risk events specific to technology impacts.

In this chapter, we will look into the world of the CRO, bearing in mind that cyber risk is a new focus for many of them. The sections covered in this chapter explore the key areas CROs need to focus on, their main challenges, and ways to connect the dots and stay ahead in the management of cyber risk. CISOs will also find this chapter helpful in understanding what CROs require and expect of CISOs. The end of the chapter provides practical takeaways and questions C-level executives can discuss with their CROs, serving as a checklist for CROs to weigh their priorities and understand their position in addressing cyber risks.

This chapter covers the following key topics:

- Understanding the role of the CRO and its key focus area
- Analyzing the CRO's key priorities
- Identifying the CRO's challenges
- Developing the right mindset as a CRO
- Understanding the collaboration potential between the CRO and CISO
- Questions to ask your CRO

## Understanding the role of the CRO and its key focus areas

Risk management has grown in importance in an increasingly complicated, dynamic, and interconnected business world. Technological improvements have transformed corporate operations, but they have also created new risk management and mitigation challenges. More businesses are realizing the value and need to have a comprehensive risk management framework that enables them to better predict and identify risks, so that they can be turned into sustainable competitive advantages.

As a CEO, it is important to understand and value risk management within your organization. ERM is a **plan-based business strategy** that aims to identify, assess, and prepare the organization for any hazards and potential disasters that could interfere with its operations and objectives.

In many organizations, risk management is still at a crossroads. The best risk managers are those who look for opportunities to broaden their knowledge base, refine their skill sets, and get access to best practices, tools, and technologies, even while a culture of risk aversion or evasion still pervades large parts of their organizations. It is essential that the core leadership team fully understands the importance of risk management and develops risk-taking decisions capabilities that factor in risk.

With increasing levels of senior management buy-in, the risk function can move closer to the boardroom. Risk management teams must aim to play a more prominent role in risk governance and compliance. They should influence strategic growth choices actively by identifying and mitigating new and emerging risks.

The key to a successful risk management strategy is to foster a risk-taking culture rather than one that is risk averse. Decision makers must be empowered to focus on objectives that support this. After all, there are always risks in business, as in life.

The CRO is the **business risk custodian** across an ever-increasing array of risks, a reflection of the increasingly connected and complex world we live in. These risks include but are not limited to:

- Financial risks (including market, interest, and credit risks).
- Operational and technological risks (including cyber risks).



- Supply chain, third-party, and vendor risks.
- Compliance, conduct, people, and cultural risks.
- More recently, risks relating to **environmental, social, and corporate governance (ESG)**

An effective CRO should work with the board of directors to set an organization's risk appetite and tolerance while achieving business strategy and goals. It would be a catastrophic error for a CRO to assess risk out of context and without a clear understanding of commercial and business objectives.

## Analyzing the CRO's key priorities

In 2022, the CRO's priorities are moving toward innovative technologies that have seen significant shifts and changes. It is, therefore, essential to ensure that all your executives understand the business strategy and vision set by the CEO, toward which the board guides the company.

A key priority for the CRO is the need to recognize the importance of people in shaping a robust risk culture to complement all necessary mitigation activities, in alignment with an organization's risk appetite. An organization's risk culture drives and motivates the right behavioral outcomes from critical stakeholders. The right risk culture will also influence the right behaviors during decision-making and the ability to design and deploy effective controls. However, the aftermath of COVID-19 has also surfaced talent-related risks; large numbers of workers are choosing to leave their positions or take a step back from being “*always on*,” and replacing employees with the knowledge set has been a challenge. This directly impacts an organization's ability to maintain a healthy risk culture. CROs consistently rank talent-related risks as their most critical challenge for 2022—and the one in which they have the least confidence in their current HR strategy.

Another key priority of a CRO is in ensuring that risk-informed decisions remain a foundational cornerstone for their organization. Incorporating risk appetite into decision-making and analyzing difficult-to-quantify risks has always been a challenge, especially if not supported by the CEO and others on the leadership team. This is just as true and relevant when discussing cyber risk. While other concerns may be more pressing, CROs often lack the necessary confidence needed to speed up risk management and **governance, risk, and compliance (GRC)** technology adoption within the organization.

Lastly, despite significant interest in defining ERM's position within ESG, many CROs, unfortunately, do not regard strengthening their ESG governance/reporting as a major priority for 2022.

In a podcast hosted by Shamane (co-author of this book), Joanna Knox, the CRO of telecoms giant *Telstra*, walked through four key categories they focus on in their risk organization framework:

- **Safety risk for employees and members of the public is a priority:** Joanna prefers to focus on things more likely to have bad outcomes for their customers or communities. The team primarily organizes this around risks to safety, including security for their employees and the safety of members of the public who interact with the company's infrastructure.
- **Resilience risk for their customers:** This includes any way in which a disruption of one of Telstra's services (such as networking services) would impact their customers. This is another area where cyber is a primary concern.
- **Meeting customer commitments:** For instance, Telstra needs to ensure they sell products and serve customers in a way that meets their expectations.
- **Anything to do with regulatory compliance:** Telstra manages this risk by doing the right thing for customers, particularly with high-risk obligations, such as privacy and emergency calls.

Every C-level executive has different responsibilities, motivations, and priorities. Understanding the priorities relevant to the CRO's responsibilities and objectives helps you (whether you're a CEO or a CISO) develop more effective practices for working with your CROs. While many CROs adapt to new norms and business changes, there are always challenges with emerging risks, whether foreseen or that emerge unexpectedly.

It is for those reasons it is important to explore the challenges faced by CROs.

## Identifying the CRO's challenges

History remains the ultimate teacher; among its lessons is showing that patterns form and repeat themselves. In studying the global economy over time, a significant financial crisis seems to occur roughly every seven years (*7-year itch*). By this measure, we could infer that, pre-COVID, we were

overdue to experience a catastrophic event, given the last one, the **Global Financial Crisis (GFC)** began in mid-2007 and lasted through early 2009.

Nonetheless, anticipating risks on the horizon is complex, unpredictable, and often have massive negative consequences for companies.

Jeff McArthur, CRO at Greater Bank, shared the following on a *Mega C-Suite Stories* recording with Shamane: “*From now on, the CRO needs to have the capability to take historical, backward-looking insight, and apply intelligence to predict what the future might look like. The next CRO challenge is identifying if the organization is equipped with the ability to respond to an event, regardless of its nature, appropriately within a constantly changing risk profile. This has been one of the most significant challenges, stretching the CRO’s capabilities.*”

That’s quite the challenge for a CRO! Challenges constantly evolve within a fast-moving and changing environment. No matter how much CROs focus on their priorities, they will inevitably face roadblocks and challenges.

Unfortunately, risk appetite is not embedded continuously in the decision-making process, and this is especially true when the CRO does not have cybersecurity knowledge or does not work in collaboration with other security stakeholders. Risk is a notion that is intangible, especially when concerning technology. The difficulty in assessing and quantifying the impact of a given risk limits CROs in their ERM strategies, as well as limiting support from the board to identify and address risk appetite and risk tolerance. This is reflected in the pervasive “*It can’t happen to us*” attitude.

We see this challenge particularly among business managers, CROs, and information technology security/risk analysts or CISOs. For instance, when company management discusses the *effect* of a loss, they are not referring to the number of servers or IT operating systems that would cease to provide basic services if a cyber event was to occur. Yet such a description is how many of the stakeholders would quantify such losses. Instead, it must be communicated effectively to these stakeholders that the *effects* of a loss almost always refer to the loss of business activities that impair the company’s capacity to continue operating. Loss of servers or operating systems are a headache, but they can be replaced. No longer being able to conduct business would be catastrophic.

Business management stakeholders are concerned with providing regular transactions and adhering to relevant regulatory standards, which may cause the firm to limit or even cease trading in the face of harsh regulatory and legal penalties if a risk materializes. Similarly, corporate managers often regard losses as *threats* that may cause the firm to suffer but—more importantly in their eyes—won't jeopardize their own business positions significantly.

This leads to major challenges with reporting. Risk reporting remains woefully lackluster and most risk reporting rarely conveys the accurate and necessary information to the main stakeholders and the board. Magda (co-author of this book) notes that various risk registers handled by CROs in Asia do not include cyber risk yet but do consider technology risks, which are different. Because most CROs have limited cyber risk knowledge, they can only plan out limited scenarios based on limited expertise and knowledge. They often use a plan template or preprepared plan that is general and not necessarily specific to their company. These plans are theoretical, and in the event of an actual threat, they cannot be executed effectively. Thus, finding the right resources and capabilities to deploy risk plans as quickly as possible is a significant challenge CROs will face.

We have progressed beyond the new technologies of e-channels and e-commerce. With continued digital transformation, another key challenge for Jeff McArthur is, “*How do we deal with the risk nodes and, more importantly, how do we use some of the emergent technologies to manage risks?*”

CROs must be open to the idea of risks originating from nontraditional sources. Leveraging emerging risks and incorporating them into an organization's risk profile, CROs can identify more creatively and effectively their lead and lag risk indicators, formulate their risks, and report them.

A good CRO needs to look at the different risk classes on the table and consider the associated impacts of various events. The CRO needs to have the mindset that *something will happen, even if they do not know what it might be*.

Their thought process is constantly asking the *what-ifs*, including the following:

- What could go wrong if ...?
- What is the road to success if ...?
- What assumptions have we made in our scenarios if ...?
- What scenarios have we considered, and which ones have we omitted, if ...?

- What should we do to improve our forecasts if ...?
- Does the board know the organization's risk tolerance if ...? (Most honest boards will admit that they do not know how to define risk tolerance.)

Perhaps some of these questions strike a chord with you, and you wonder how other CROs address them. So, let's talk about the different strategies, systems, and frameworks that have aided CROs in managing their cyber risks.

## Strategies, systems, frameworks to manage cyber risk

One of the *value-adds* of a risk function is a system in which the business makes risk-informed decisions. Defining risk tolerance requires a structured approach, highlighting the **risk** and **return** scenarios that reflect and support strategic objectives and then soliciting a risk/return trade-off that the board of directors agrees on. Often, boards make choices that contradict a stated strategy, demonstrating the lack of a shared understanding of the strategy, or perhaps different motivations.

The strategy informs the risk tolerance and vice versa, so the risk tolerance must be revised to align with the strategy.

Your CRO should develop and maintain a governance framework that aligns cybersecurity risk management with your business operations. This governance framework will enable your organization to consider relevant cybersecurity risks, estimate their severity, and determine their impacts and mitigations.

Where ERM traditionally has been a function of compliance, and cybersecurity an IT problem, cybersecurity now needs to be considered a business risk. This business risk affects the whole organization and spans people, processes, and technology.

There is a school of thought that, in the overall risk taxonomy, cyber risks stand as an independent risk category. However, as cyber risk is very diverse and pervasive within an organization, elements of it often show up in all the other risk categories, creating yet another challenge for CROs today.

The CRO must have a perspective on how effectively they're managing risk. Cyber can be a challenging domain for CROs to master to get a good perspective and, as such, might create an obstacle or even a critical gap in

the process of ERM. Those obstacles and gaps must be overcome and cyber risk needs to be defined and included in your CRO's strategy, with mitigation strategies put in place. One such mitigation strategy is to link the CRO's strategy with the CISO's cybersecurity strategy.

Joanna Knox also shared details the risk effectiveness dashboard they have developed at Telstra, which assesses the effectiveness of the company's risk management activities. They have gone beyond just looking at risk ratings, residual risk, and control effectiveness and now consider Telstra's organizational risks more holistically.

When they step back and look at their risks, they ask themselves whether they are managing them effectively. Consider the following key questions they are always asking themselves:

- Is accountability clear?
- Do we have our risk appetite defined and agreed upon?
- Do we have our action plans to manage the risk in place? Are they adequate and on track?
- Have we got the right kind of assurance in place that our risk management actions are effective?

Joanna's strategy is to have an effective team managing all of Telstra's top enterprise-level risks, including cyber risks.

Similar to how Joanna manages her other risk management activities, cyber is no exception, even if it's really specialized and sometimes remains technical. She created a dedicated role within the team whose entire purpose is to understand how effectively the team can manage its cyber risk. Although the specialist is not a cyber expert compared to the CISO's team, their risk expertise is incredibly useful in assessing how everyone manages cyber risk. They then use that focus to challenge the cyber team, which in turn strengthens their strategies.

Lastly, even within the cybersecurity group itself, there's a recognition that diversity of thought and expertise is essential in building a robust security capability. It is necessary to critically and constructively challenge how things are done, given the constantly evolving nature of cyber threats.

Thus, Telstra's cyber team employs a number of staff with diverse backgrounds in nontechnical fields, including journalism, linguistics, education, and even UX and graphic design.

## Connecting the dots

In the current environment of intensified cyber risk, the CRO and the job of the central risk team is to connect the dots across all the teams and work together effectively.

The CRO should partner with the CISO and their cyber team to successfully categorize, identify, and quantify cyber risks. The cyber team also should work closely with their physical security teams, health and safety, data governance, and other responsible business teams. Collaboration is key in creating effective risk plans.

The specialist risk teams, together with the cyber specialist risk team, collaborate to ensure the efficiency of risk management across an organization. The CRO then works closely with the CISO on their frameworks, operating models, reporting, and incident management.

Together, they find opportunities to improve their work by considering other parts of the business, such as supply chain risk, physical security, privacy, and other sizable areas with shared governance.

The CISO then owns the mitigation controls and compliance for the digital/cyber risks and ensures alignment between the residual risk and your organization's risk tolerance.

The CRO, with the support of the CISO, enables discussions on cyber risk management. Such discussions should be given adequate time on a board meeting agenda.

Now that we have demonstrated the different ways the puzzle pieces of team collaboration can fit together, the next section covers the mindset that is vitally important for CROs and other C-level executives to have when managing cyber risk.

## Developing the right mindset as a CRO

In risk workshops, the CRO's focus should not be on why a new project cannot be done or why the company cannot roll something out. Instead of *"No, this is not possible,"* the CRO's mindset should be *"Yes, let's try to find options that can help achieve the goal."* There should be a greater focus on

defining the value proposition of a new project with the CEO, instead of focusing just on the risk management processes.

In building your risk management capability, *always start with the objective*. This crucial leadership principle requires proper training. When your executives are well informed of your corporate goals, combined with a structured way of considering risks, they are empowered to make informed decisions.

The CRO's job is not to help everyone avoid every potential risk threat. Their job is to build a structured approach into the decision-making process that complements the business goals. The next step is to improve the likelihood of achieving those goals, and the success of the new venture.

Besides its own business, it is even more critical for a telecommunications company to build resilience for its customers. Joanna Knox shared her team's journey over the years, building different resilience frameworks, from network and IT resilience to cyber resilience, supplier resilience, and business continuity management.

In the last two to three years, they've integrated all of these resilience frameworks into one overarching framework, covering all the different areas where resilience is vulnerable, either for their customers or their internal processes. Cyber is one of the key domains in this resilience framework.

CROs are also in charge of crisis management. The most important way to prepare for that is to do thorough post-incident reviews and run **crisis management team (CMT)** scenarios with a cyber element. Joanna shared how some of their cyber-specific scenarios involve their big enterprise customers, where they run the attack scenarios together.

They also build other scenarios that include cyber elements because cyber incidents often do not occur in isolation. These exercises are conducted with both the risk and cyber teams. They put the cyber operations through their paces to practice their response. One of the key roles of the CRO is to ensure that interactions with the board, the leadership team, and the rest of the company is smooth.

The purpose of such exercises is to help its organization be better at managing its risks if and when attacks do occur. It also demonstrates why a strong trusting relationship between the CRO and CISO is crucial and results in better outcomes.



## Understanding the collaboration potential between the CRO and CISO

Shamane shares her observation of the conversations she had with various CROs about their interactions with the board: *“They do not want us to be afraid of being contentious. In fact, they welcome an alternative view!”* Part of this alternative view is to pivot your message from one of fear of threats to one the CRO can use to better inform their risk management framework/analysis/taxonomy.

CROs have observed that CISOs can use threatening language to scare the board of directors into a decision. However, from a behavioral and psychological perspective, fear only drives irrational decisions that do not pan out well in the long term.

One such CISO reported during a management meeting that cybercrime would be the third-largest industry in the world within a few years. The CISO did not support these claims with facts nor provide an analysis of the consequences. It's then unsurprising that the CRO, and even the wider management, were left feeling dubious about the context.

Too often, CROs often work in silos, addressing cyber risk based on historical claims rather than collaborating with CISOs. Building on this challenging situation, CISOs do not usually address digital risks quantitatively, instead using a qualitative framework. This makes the risk approach unclear and insufficient to align with an enterprise risk management strategy. Without a quantitative framework that identifies the potential financial losses that may be incurred following a cyber event, you, as the CEO, your board, and your CRO cannot get into alignment, provide adequate security considerations, and identify possible investment or budget allocations for cybersecurity. This is a major challenge for your CISO, which will be further addressed in *Chapter 5, Working with Your CISO*.

CROs might, therefore, turn to claims-based evaluations for growing risk issues such as cyberattacks and data breaches. This has its limits, however, particularly in the Asia-Pacific region, due to inadequate actuarial data and a lack of data accuracy.

Cyber risk is a relatively new challenge compared to more established hazards such as floods or earthquakes. There may be minimal or no accessible historical data on cyber risk. Yet, by using a structured scenario approach,

organizations may effectively estimate cyber risk. This requires a collaboration between the CRO and the CISO. Working together, they can identify cyber risks and quantify them. The CRO needs the help of the CISO to understand the potential cyberattacks and their consequences on the business. The CISO needs the CRO to identify the business priorities and goals.

The board and executives also need to recognize that some risk scenarios may not manifest themselves for a year or two, or perhaps ever. Simultaneously, the CRO needs to educate the board on emerging risks by:

- Estimating the frequency of cyber-risk events
- Considering vectors of attack
- Supplementing the analysis with relevant data
- Considering historical cyber incidents provided by the CISO
- Their expert opinion

Together, the CRO and CISO can build structured scenarios to quantify the severity of cyber events based on loss types and loss drivers. They can then provide real added-value reporting to the board and CEO and an adequate view of cyber risks.

For CEOs, when you talk to your CROs, take the conversation beyond risk management, and start talking about effective decision-making that you and other executives can buy into. Consider the full risk management process, including insurance or risk transfer. In the case of cyber risk transfer, it can be difficult for risk managers to fully identify the effects of cyberattacks on the organization and understand the requirements for good coverage. We cover cyber insurance in further detail in *Chapter 6, The Role of the CHRO in Reducing Cyber Risk*.

Collaboration between a CRO and CISO is crucial for effective and successful risk management plans and building cyber resilience. But it doesn't end there. There are core questions the C-suite can ask their CROs to guide them through their journey of managing cyber risk. This also serves as an internal checklist for CROs to develop their perspectives and communicate them effectively.

## Questions to ask your CRO

The risk landscape is rapidly changing. Geopolitics, technical advancements, global economic integration, and climate change are all interrelated, which means the manifestation of one risk is more likely to trigger others.

Thus, firms that create a multidimensional strategy to detect and manage complex hazards often achieve success in their risk management goals. The following list provides some questions you can ask your CRO to ensure they are prepared to support cyber risk management:

- Who's at the top of your calling list? Are you in open communication with the CISO and their cyber team?
- How are you educating yourself about cyber and ensuring you are a powerful advocate in your organization and the community?
- As the CRO, can you agree that the current risk appetite is adequate for the organization?
- How do you rank cyber risk compared to other risks?
- How are we ensuring cyber risk is integrated into our ERM strategy?
- What are the right risk metrics to help the business accurately understand our cyber risk profile? Are the metrics more focused on incidents and attacks, or more on external/internal controls and ensuring risk management actions are in place?
- How is your cyber risk tolerance aligned to or compared to other risks?
- How are you keeping your finger on the pulse of staff security awareness and the cyber risk culture in your organization? How are you working with your communications team and/or HR in reporting the right things to keep everyone on their toes?
- In the last three years, has your attention, time, and focus on cyber increased? If so, how much more do you think it will grow over the next three years?

These questions are meant to widen the boundaries of how we think about our cyber risks, challenges, and cyber culture, and explore how we can align more closely with different stakeholders in our perspective on and tolerance of cyber risks.

## Summary

As organizations strive to manage cyber risk at the front line of an ever-changing environment, the CRO's role is instrumental. We unpacked the different layers of the CRO's responsibilities and motivations in this chapter. We also looked at the experiences of CRO experts and extracted approaches that aspiring CROs can tap into.

Whether you're a new CRO or another C-level executive, this chapter provides understanding of the CRO's approach to designing a technological strategy, system, or framework and grasp the required language to communicate it effectively. The development of this framework is best done in collaboration with the CISO to achieve meaningful business outcomes.

Next, we will address the priorities of another C-level executive and their role in building a cyber-resilient business. The following chapter shows you how your CIO can be your cyber enabler.



# 4

## Your CIO—Your Cyber Enabler

The **Chief Information Officer (CIO)** is the organization's executive in charge of, and accountable for, the administration, deployment, and use of information and computer technology.

The CIO's role in an organization is shifting from delivering enterprise services to a enabling strategic business processes. This is evident, especially in recent years, with more organizations pushing digital transformation agendas. As technology advances and reshapes firms worldwide, the CIO profession has grown more popular and relevant. Today, the CIO studies how different technologies help the organization enhance existing business processes, decrease costs, and improve customer experiences, among other things, to achieve business outcomes.

The CIO has evolved from simply selecting technologies to making business-critical decisions on technology adoption based on a sound IT strategy matched against an enterprise architecture that scales with the business, maintains operational stability, and drives cost efficiency. Cyber resilience is a natural extension of a CIO's activities to help attain these goals.

The CIO's remit is already large and cyber resilience is a specialized knowledge area. Just as with the CFO and CRO, to expect a CIO to also possess the full breadth of cybersecurity knowledge would be a stretch too far. This is where the CISO steps in.

The **Chief Information Security Officer (CISO)** role is centered on preserving the confidentiality, integrity, and availability of an organization's information and technology assets. The CISO role complements the CIO's role, the latter of whom is more focused on securing appropriate tools to enhance productivity, identifying trends that affect the business, and identifying possibilities to use and create better technology adapted to the firm's business models.

CISOs and CIOs often work together and support each other in preserving and protecting an organization's information and technology assets. According to the 2021 ISACA State of Cybersecurity survey (<https://www.isaca.org/resources/infographics/state-of-cybersecurity-2021-part-2>), of the 3,700 global cybersecurity professionals surveyed, 48 percent of security teams report to a CISO while 25 percent report to the CIO. Notably, respondents did not demonstrate a preference to whom cybersecurity ownership should belong. However, the survey does make apparent that the ownership of cybersecurity—whether the CIO, CISO, or CRO—does weigh on how the C-level executives respond to the valuation of cyber-risk assessments, whether the board of directors prioritizes cybersecurity, and whether there is strategic alignment between IT and cybersecurity.

In today's environment for building cyber resilience, it's more important than ever for a CISO and CIO to collaborate to maintain compatibility between the IT strategy and the cybersecurity strategy. Doing so will allow for the best organizational outcome. There are already industry discussions today on how the accountabilities between the CISO and CIO are distinct enough for the functions and ownership of information security to be split, where the CISO no longer reports to the CIO. However, this is still a fairly fresh perspective that requires time to be tested.

To better understand the CIO, we will cover the following topics in this chapter:

- Understanding the CIO's role and the impacts their decisions have on cybersecurity
- Challenges a CIO may face with the current reporting lines
- Getting ahead of cybercriminals
- How the CIO supports your security
- Questions to ask your CIO

## Understanding the CIO's role and the impacts their decisions have on cybersecurity

Today, the CIO is the most senior executive in an enterprise who enables the business with technology solutions. Sometimes, in smaller organizations, this role can be referred to as the IT director.

The role of the CIO has evolved significantly throughout the years. Starting in the 1980s, businesses started utilizing technologies such as computers, databases, and even communication networks as a way to improve workforce productivity. This meant that the CIO was highly focused on technical solutions for a very utilitarian purpose. As business needs have changed, with technology universally seen as a business enabler, the importance of the CIO has expanded. Nowadays, CIOs must possess various hard and soft skills to succeed in this position, striking a balance between business requirements and organizational productivity with the appropriate technology solutions, while operating their very own business unit to support it all.

Rogier Roelofs, Asia Pacific CIO at **ABN AMRO Clearing Bank**, added his top three recommendations for the enablement of our CIOs:

- Be aware of the regulations around information and cybersecurity. It is an increasingly complex area, especially for companies operating across different countries. This creates a lot of complexity because the CIO has to think about different requirements in multiple jurisdictions and how to comply with all of those items at the same time. Where in the past CIOs would mostly think about compliance and regulations as a geographical concern related to the jurisdiction in which they were located, nowadays you will not get away with that. The CIO needs to have a holistic cross-border view of distributed, processed, and stored data.
- Most organizations designate one person to be ultimately accountable for cybersecurity. However, it's the responsibility of all senior management to manage cybersecurity risks in their areas and protect the interests of all stakeholders. Unfortunately, many executives do not see cybersecurity as a senior leadership issue, and therefore, creating cyber-savvy boards is of the utmost importance. The role of the CIO is to take ownership and develop a robust cybersecurity culture. This does not simply mean implementing



various policies and procedures. Instead, senior management must make clear through their own actions that cybersecurity is essential to the organization's mission, and the CIO should take the lead in this by creating transparency, accountability, and strong communication within the organization.

- CIOs should embed cybersecurity into the company's software development processes. Although the focus is a lot on DevOps, this is not good enough, as it should be DevSecOps. This means everybody in the IT organization needs to have the mindset that they are responsible for fast *and* secure software delivery.

To ensure the organization stays ahead, CIOs often establish strategies and roadmaps so core technology systems are selected that are appropriate to the organization's business needs, enabling the business to remain competitive in a fast-changing global marketplace. The CIO's technology strategy can include the adoption of innovative and disruptive technologies, such as cloud computing, artificial intelligence, virtual reality, and even drones.

A CIO's primary role is to forecast the future of computer technology advances that will provide their corporation with an edge over its competitors. One of the most important tasks of a CIO is understanding how each business unit or department operates, establishing the technological requirements and choices, and providing a clear **return on investment (ROI)** to their business stakeholders. The day-to-day operations of maintaining the technology landscape are often delegated and/or outsourced by the CIO.

## Rapid technology adoption

A 2020 McKinsey Global Survey of executives (<https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever>) indicated that the COVID-19 pandemic accelerated digital transformation efforts by three to four years. More surprisingly, digitally enabled products were advanced by a shocking seven years. At the same time, anecdotal observations show that cybercriminal organizations have also followed the same trajectory, progressing through their own digital transformation by matching and responding to the new ways of working their targets have adopted as a result of the pandemic.

As organizations continue to reimagine and revamp their processes, technology, resourcing, and customer experience, there needs to be an equal, if not greater, awareness that cyber threats such as account takeovers, business email compromises resulting in wire transfer fraud, and ransomware attacks against organizations are also accelerating at a rapid pace, too. A prudent CIO understands that creating new customer experiences while adopting new technologies might seem exciting, and often provide a great ROI. However, a misjudged choice could also lead to significant financial losses and undue business risk.

No matter what drives an influx of new technologies, CIOs cannot ignore new technology solutions that solve business issues or improve customer service for their organizations—but at what cost? New technology is exciting and eagerly anticipated. It also often is held that the older (more mature) a technology is, fewer bugs and security vulnerabilities exist, having been addressed in new releases. Therefore, a newer technology theoretically may have more undiscovered security vulnerabilities.

## Balancing digital transformation

A CIO must always consider the balance between business drivers, the risk of unmitigated and undiscovered security vulnerabilities, and the likely costs and financial losses following a cyberattack or a data breach. Another consideration is whether new technologies are on-premises-only solutions, which require ongoing **operational expenditure (OPEX)** to support and secure.

To illustrate this, let's consider three scenarios that highlight the struggle between innovation, future investment, and liquidity management. These scenarios will show how the CIO's decisions affect the organization's cyber resilience and financial stability.

- The CIO chooses an **Internet of Things (IoT)** technology that has been purchased from an innovative new start-up that is a **minimum viable product (MVP)** to its solutions, meaning the product is still under development and has the minimum possible functional and security requirements. The offer is financially attractive, and the product gives a competitive edge to the CIO's organization. However, because it is an MVP, it often means that the product does not include enterprise-grade security controls or fully meet compliance requirements. Therefore, the start-up is challenged to fulfill its obligations when a larger organization requests a third-party security assessment.

While the CIO's decision is not wrong when deciding to work with a start-up, the CIO would need to consider the costs associated with securing the MVP product and/or even taking the start-up within the CIO's organizational security umbrella. A CIO needs to be aware of those challenges.

- The CIO chooses to adopt **artificial intelligence (AI)** to enhance a production line's productivity. This choice of utilizing AI introduces an unknown vulnerability, which leads to a cyberattack. The attack creates major delays by interrupting the production line and causes immense reputational damage to the organization. The organization also incurs massive financial losses as deadlines are not met and contractual obligations are breached.

While this scenario is specific to certain industries, the example highlights the importance the CIO and CISO need to put on assessing the risks associated with new technologies. Every technology comes with new cyber risks because no technology is secure by default.

- The CIO forecasts that cloud adoption will be driven by increased flexibility to access digital infrastructure and computing resources, underpinned by lower monthly OPEX costs. However, cloud adoption is approached with an “on-premises” mindset and architecture, meaning people who adopt cloud services configure it in ways that make more sense for on-premise systems. This will almost certainly drive up security costs because the security team will need to reconfigure traditional security solutions to meet the security requirements of the cloud. Security solutions such as the use of a **next-generation firewall** will need to run 24/7 on their cloud tenancy to gain full visibility. Or the company could opt for the more pervasive **Web Application Firewall (WAF)** to better control all web traffic, but this would no doubt drive up monthly OPEX costs. The CISO will also need to consider a security solution to improve cloud-service usage visibility through a **Cloud Access Security Broker (CASB)** to monitor the use of unsanctioned cloud services, as the corporate network is now exposed to more internet services.

Scenarios such as these show how any digital transformation driven by the CIO needs to be balanced between business requirements, innovation, productivity improvements, and cybersecurity. In almost all instances, any transformative changes in technology increase your organization's exposure to cyber threats.

## Complex regulatory landscape

In addition to cyber threats, CIOs need to consider the ever-expanding regulatory and compliance landscape relating to privacy and security. Noncompliance with, or breaches of, regulatory requirements must be taken seriously, as they often attract very large regulatory fines and, in most cases, the ability for civil lawsuits to be filed against the organization.

For example, financial institutions in the United States must comply with standards such as the **Payment Card Industry Data Security Standard (PCI DSS)**, the **Sarbanes-Oxley Act of 2002 (SOX, P.L. 107-204)**, the **Gramm-Leach-Bliley Act**, and the **Financial Services Modernization Act of 1999**, among others. Amidst these regulations, technology adoption and general digital transformation must take into account security, compliance, and privacy from the onset.

## Third-party risks

Many technology service providers do place more focus on security these days, adopting secure coding practices and regular security penetration testing. However, many vendors do not yet have the adequate maturity or investment in cybersecurity to ensure the minimum fundamentals to maintain a resilient and secure solution. It is important the CIO understands the difference between a security activity (for example, checking the box after performing a penetration test) and mature security practice (understanding overall exposure risks).

Security, especially when using third-party vendors, should not be seen as a defensive expenditure with a low ROI but as a necessary and fundamental component of any organizational decision. Security should be considered early in the decision-making process rather than as an add-on at the end.

Having a better understanding of the CIO's role, the next section draws parallels between the CIO and the CISO roles, and unpacks the differences.

## Differences and commonalities between the CIO and CISO roles

The CISO reports to the CIO in many organizations, with a dotted line to the CEO. While this structure might be effective, the CIO and the CISO have different goals and priorities.

Both the CIO and CISO, as C-level and senior executives, primarily focus on strategic planning, innovation, leadership, and management. CISOs strategize for business cyber resilience while securing all company assets and data. They align security policies and practices with the company's goals and risk tolerances. On the other hand, CIOs focus on the overall, broader strategic use and management of an organization's technology and define the roadmap for the implementation and utilization of IT systems and technological tools.

IT and cybersecurity are two different domains, although sometimes they do intersect. The CIO is typically a skilled professional with a significant background in IT as well as having an understanding of enterprise business functions. They are focused on driving business value through the adoption and operation of technology. The CISO is typically a skilled professional with a significant background in information security management along with having an understanding of enterprise cybersecurity, information security, security governance, compliance, and risk; two very different roles for two very different domains. Table 4.1 is an excellent overview of the differences between IT and cybersecurity, and their priorities.

<b>Information Technology (IT)</b>	<b>Cybersecurity or information security</b>
Ensuring hardware, software, and other technological tools remain functional	Protecting data and assets from theft, unauthorized access, loss, and disruption, among other things
Responsible for adopting and operating technology solutions	Responsible for adopting and operating information and cybersecurity solutions
Implements controls	Defines and monitors controls
A fix-it mentality	A secure-it mentality

Table 4.1 – The differences between IT and cybersecurity

The commonalities between both roles include the need for extensive communication skills, leadership qualities, strategic understanding of business and technology management, and, especially, business alignment with cyber-resilient choices, ensuring secure innovation, proper cash-flow forecasting, and liquidity management.

In the next section, we take a deeper dive into the CIO's role as it concerns cybersecurity.

---

## Getting ahead of cybercriminals

Although handling cybercrime is challenging, there are ways that CIOs, with the CISO's support, can outthink, outsmart, and outmaneuver cybercriminals. CIOs must play a role in driving technology transformation efforts that include planning for better cyber resiliency.

Theresa Payton, CEO at **Fortalice**, author of *MANIPULATED: Inside the Cyberwar to Hijack Elections and Distort the Truth*, and the first female CIO at the White House, shared her views with Shamane on the actions critical for CIOs to fortify resiliency in the face of cybercriminals. To make an evolutionary change, her top three actions are:

- Understand and educate yourself about what drives human nature and incorporate that into your cybersecurity.
- Get to know the criminals. Create decoys of authentic-looking human profiles and systems that look valuable and leave them vulnerable to cybercriminals. Then, study the criminal elements that attack the decoys and learn from what they do.
- Beat the criminals at their own game. Leverage the power of AI and behavior-based analytics to create behavior-based profiles of criminal activities, and then use those profiles to create a *digital bodyguard* to protect employees and systems against digital criminal behavior.

If we study the human psyche, we can empower and inform ourselves to stop or slow growing cybercrime. Profiling cybercriminals and better understanding how they operate is another proactive step in building cyber resiliency.

The cybersecurity burden should not rest solely on a security team or a user's shoulders. Instead, the CIO needs to build a digital bodyguard around each human and their digital life every single step of the way. To begin, Theresa recommends CIOs take two critical actions:

- *Know your user stories.* Start collecting your organization's user stories now. Don't try to fix things at first; just listen. Listen for the opportunities to redesign your process and security around the employees' experience using the technologies.
- *Focus on awareness and behavior.* Leverage AI to study legitimate use cases and behavior at your organization and then train the AI to alert your security team when behavior doesn't match that baseline.

Give your users a safety net by installing easy and elegant **Multi-Factor Authentication (MFA)** options—there are some great technologies out there, and the benefits of using them are significant. According to research studies conducted by Microsoft (<https://techcommunity.microsoft.com/t5/azure-active-directory-identity/your-pa-word-doesn-t-matter/ba-p/731984>), MFA stops 99.9% of password-based cybercrime in its tracks.

Magda recalls a CIO who was hesitant to implement MFA, due to concerns about low user adoption. Magda provided an alternative by making MFA optional initially and enforceable afterward. This approach worked, demonstrating that there is always a compromise to be found.

In the next section, we will discuss additional important activities where a CIO can clearly support the firm's cyber resilience.

## How the CIO supports your security

The CIO focuses on managing the information technology for the business while balancing business goals, ensuring competitive edge, and advocating for innovation, all in alignment with the CISO to ensure that security and privacy are part of the technology roadmap. The CIO's role in cybersecurity extends further, ensuring the effectiveness and continuity of operations. Rogier Roelofs of ABN AMRO Clearing Bank puts it very clearly:

*“Although the CISO might be primarily responsible for the cybersecurity roadmap, the CIO should have an in-depth understanding of how this affects the IT landscape and the consequences for the business, something the CISO doesn't have. I do see too many CIOs being very traditional in how they see their role and responsibilities. Too old-school. They are too closely focused on the IT landscape itself and therefore missing out on what this means for the business. CIOs should utilize their technical know-how with a robust knowledge of the business side of the organization, increasing their visibility and authority through strong communication about cybersecurity so the environment can act accordingly.”*

This requires a strong relationship and regular collaboration between the CIO and CISO. Security might be perceived as a challenge or an issue by the CIO, slowing down specific deployments or initiatives. Rather than seeing their roles and goals as a conflict of interest, the CIO and CISO should collaborate on cyber strategy.

Because the CIO has a holistic understanding of the business activities and business model, they can consider all implications and discuss those with the CISO to find the right balance between cyber risk, business operations, and revenue. Such discussions support finding compromises with a balance between usability and security for end users, a common concern for all parties.

Having the latest security solution is not a foolproof answer to securing an organization. Instead, a collaborative approach to focus on people and culture is critical, and this requires the CIO's support and leadership.

The following list details some of the activities of the CIO and their role in supporting cyber resilience:

- Establish goals and plans for the company's information technology strategy, considering cybersecurity and privacy as key decision-making components.
- Choose and install appropriate technology to simplify all internal processes and optimize their strategic advantages while balancing security and privacy.
- Don't compromise usability for security; discuss with your CISO and find the right balance.
- Enhance the consumer experience by designing and customizing technical systems and platforms, focusing on cybersecurity and privacy as a differentiator and added value instead of cost.
- Plan the installation of new systems and give directions to IT specialists and other organizational personnel, while ensuring the CISO's security requirements are met. This includes managing the expectations of business stakeholders in relation to the organization's exposure to cyberattacks and data breach risks.
- Approve technical equipment and software acquisitions, and form strategic alliances with IT companies while considering their security and privacy posture, to support the organization's cyber resilience.



- Supervise the organization's technical infrastructure (networks and computer systems) to guarantee optimal functioning, and leverage this to support your CISO's priorities in detecting and responding to security events.
- Manage initiatives using information technology while involving your CISO in the initial steps. It is always cheaper to build security controls into a solution versus applying remediations when a vulnerability is compromised, or an attack occurs.
- Keep an eye out for innovative solutions or improvements in technology that might give the business a competitive edge while always remembering that cyber maturity varies from company to company, from country to country, and from function to function.
- Analyze the costs, benefits, and risks associated with information technology to advise management and make recommendations while considering potential financial losses and important security investments when making technological choices.

As digital transformation continues apace and the threats of cyberattacks remain ever present, the CIO can and should play a vital role in building and maintaining an organization's cyber resilience. In the next section, we focus on the questions that you should ask your CIO.

## Questions to ask your CIO

The following questions help frame the cybersecurity considerations for a CIO and empower them to make decisions in alignment with a business's resiliency goals:

- Do we treat cybersecurity as a business or IT responsibility and risk?
- Do our security goals align with business priorities?
- Is our current IT architecture designed for cybersecurity?
- Is the business going to embark on any significant programs in the upcoming years, such as digital, big data, cloud, mobility, outsourcing, or third-party ventures and what are the cyber risk concerns?
- Do we initiate decisions with a consideration of privacy and security?
- Do we consider cybersecurity investment while discussing new technologies?

- Do we evaluate our vendors and technologies for security risks before making strategic decisions?
- What is the most critical information collected and held by the business, and are they aware of the level of protection required for that information?
- What balance do we consider between usability and security?

This list serves as a healthy baseline and an internal checklist to guide CIOs in their execution of the roadmap.

## Summary

In this chapter, we defined the CIO's role in building a cyber-resilient business. Cybersecurity is a massive undertaking. It necessitates acquiring diverse skills and specialized talents. It certainly requires collaboration and support from key stakeholders, including between the CIO and CISO.

We emphasized various cybersecurity considerations, including additional investments, cash flow, liquidity, and usability. Cybersecurity is a business enabler, and a balance between usability and security is a matter of finding the right compromise. In a strategic role that ensures any technological adoption is in support of the business having a competitive edge, the CIO cannot ignore the requirements for cybersecurity. It must be embedded in the decision-making process and the overall digital transformation and technology adoption.

The CIO must empower and support the CISO's strategy and goals. This is accomplished by listening to each other and understanding the other's perspectives; doing so is an essential requirement for success—the end goal always being to keep the business prosperous.

In the next chapter, we look more closely at the role of the CISO. We will define their role in detail and go further into their vital impact on cybersecurity.



# 5

## Working with Your CISO

The **Chief Information Security Officer (CISO)** or **Chief Security Officer (CSO)** of an organization ensures the organization's personnel, physical infrastructure, and digital assets are available to the business and protected from unauthorized access, loss, theft, or disruption and physical damage through appropriate **cyber risk management**.

Security breaches exploit people, processes, and technology. It is no longer a technical problem but a business risk and must be treated as such. Efficient recommendations need to be provided for controls across the elements of people, processes, and technology, mitigating cyber risk in alignment with the company's risk appetite. This is the responsibility of the CISO in collaboration with their CxO peers.

The shift in focus on cybersecurity—integrating cyber risk into the overall enterprise risk management process—underpins the foundations of this chapter.

A good CISO should be a great communicator, a manager, and a thought leader with a foundational understanding of the business. They should report regularly to the executives and the board on cyber risks and clarify whether the company's risk appetite and tolerance align with them.

In this chapter, we will cover the following topics:

- Understanding the role of the CISO
- Addressing cybersecurity challenges
- Your CISO's understanding of your business
- Priorities for a new CISO
- Addressing cybersecurity challenges
- Questions to ask your CISO
- A bonus segment for our CISOs—decoding your CxOs' expectations
- A bonus segment for our CISOs—purchasing cyber insurance
- A bonus segment for our CISOs—reporting to the board of directors

## Understanding the role of the CISO

As CEO, your role is to challenge your CISO to think differently, to move beyond their technical knowledge and align their thinking with business priorities. It is in your interest to help the CISO succeed as a strategic partner, creating a framework that enables a business's progress toward its goals while achieving security and privacy.

The role of a CISO is still greatly misunderstood, and while things are progressively improving, too many organizations have yet to hire a CISO. Many organizations still believe their security is a technical requirement provided by their IT department. In Asia, when Magda inquired about vendors' cybersecurity, she was typically directed to an IT manager instead of a CISO.

Businesses that comprehend the expanding relevance and power of digitalization and digital transformation must appreciate the value of a CISO. The dependency on and increasingly faster adoption of new technologies means the consequences of a cyberattack or data breach can result in dire consequences.

The CISO's primary responsibilities are to manage cybersecurity, mitigate cyber risks, and handle all cybersecurity incidents. These responsibilities extend to using controls and measures for people, processes, and technology to ensure the ever-expanding business landscape is duly defended from evolving cybersecurity threats. The CISO also needs to consider a complex and growing environment, with third- and fourth-party suppliers.

A CISO who takes a balanced approach between a business and its threats will ensure no significant gaps can form that might limit the effectiveness of any cybersecurity risk mitigations. In other words, the CISO's cybersecurity strategy needs to be developed in lockstep with the organization's business and technology strategy, which goes far beyond firewalls and antivirus solutions.

The CISO's responsibilities include:

- Establishing a well-thought-out cybersecurity strategy that aligns with a wider business and technology strategy.
- Defining a robust cyber-risk management system and its associated processes.
- Developing a hierarchy of security governance and policy structures.
- Driving an appropriate cybersecurity awareness culture within an organization.
- Designing and developing a set of effective cybersecurity dashboards for management reporting.
- Having a broad view and understanding of the legal and regulatory obligations of the jurisdiction that a business falls within.

To perform these functions, a CISO must build their team with the skills and capabilities necessary to deliver the business strategy and key milestones.

The modern-day CISO, or the *business CISO*, as Shamane calls it, is great at communicating with other leaders in the organization. In addition to understanding the pros and cons of a traditional cybersecurity risk management framework, they report to the business stakeholders in a language a non-cybersecurity person can understand. The business CISO is an exceptional communicator, resourceful, and an influential manager—a great storyteller who can talk about cybersecurity and how it affects the organization.

Many CISOs first started their career in IT and have a deep technical background. This is not surprising because it takes years of study and practice before becoming qualified to lead such an important position within any organization. Nowadays, many CISOs also hold business degrees. CISOs need to have a deep understanding of both technology and business to make effective cybersecurity decisions.

Bridging the gap between technical jargon and a business is important, and while a CISO with a technical background helps, it does not preclude someone with no technology experience taking on the role of CISO.

To effectively perform the responsibilities listed earlier, it's important for CISOs to have a strong understanding of the latest trends and developments both in emerging technologies and evolving cybercrimes to make sure their organization is prepared for whatever comes next.

Cybersecurity requires collaboration and buy-in across an organization. That must first come from the top. Under the direction of the CISOs, the leadership and board of directors must do the following:

- Understand who owns and is liable for cyber risk. Following a data breach or cyberattack, the board of directors, *not the CISO*, will bear most of the consequences, legal fines, and other impacts.
- Define cyber risk in the context of business risk. The majority of firms cannot appropriately define the cyber risk they face, nor the potential for substantial business disruption due to a cyberattack. Has your organization thought through the impact of a cyberattack, leading to a product recall? Probably not. It is vital to put such risks in a business context rather than considering them as technical issues.
- Quantify cyber risk through identifying, protecting, detecting, responding to, and recovering from cyberattacks.
- Consider the cybersecurity implications of third-party vendors and suppliers. They are often the weakest link, especially when cloud technologies are used and, too often, security is assumed by default. Generally, contractual provisions often do not include explicit reference to security or privacy obligations.
- Establish indicators for resilience and monitor your cyber maturity.

It is in the organization's best interest to maximize the CISO's value to apply a cyber risk management process and integrate it into the overarching risk management framework. In the following section, we will demystify important aspects of cybersecurity, the role of the CISO, and their understanding of the business.

## Your CISO's understanding of your business

Depending on their career progression and experience, some CISOs may have little to no understanding of the other areas of the business or the business itself. Because cyber resilience is a business risk, an effective CISO must align all cyber frameworks with the business goals.

A common misconception many CxO teams make about the CISO is that the CISO is an enforcer of security. Instead, the CxO team needs to appreciate that the CISO brings a boardroom-level, risk-focused conversation about the impact cyber risks have in terms of business disruption, data breaches, data loss, non-compliance with regulatory requirements, and so on. More crucially and specifically, the CISO understands the financial consequences of these risks, which can in extreme conditions affect the viability of the business itself.

The CISO needs to be a part of your corporate or enterprise risk management team. They must communicate with others on the team and understand their priorities; those on the risk management team must understand the priorities of the CISO.

Although the CISO is responsible for cyber risks, in the case of a breach or a cyberattack, business owners or company directors are ultimately accountable, not the CISO. Thus, the stakeholders must clearly understand cyber risks and the CISO must clearly understand the business priorities and goals. Neither can be achieved optimally without the other.

As part of the risk management team, a CISO should communicate cyber risks regularly with the business and learn about and understand the business goals and vision. If your CISO has the support of key stakeholders, you reduce the risk of your CISO failing and working in a void.

The challenges and roadblocks CISOs face in enforcing cyber resilience are not removed with this understanding, but they are reduced when everyone has a stake in building cyber resilience. It also enables the CISO, whether new to the company or shifting to a holistic business risk approach, to prioritize specific cybersecurity elements.



## Priorities for a new CISO

The first months of a new CISO in an organization are crucial and represent a critical timeframe to align the organization's business goals and objectives with cyber risks. It is during this period that a CISO establishes their credibility throughout the organization.

It is the establishment of this core cyber foundation that allows the CISO to create a security roadmap that includes mitigation controls that aligns with the organization's risk appetite and business goals.

But first, it is critical for the CISO to understand the existing environment and culture of the organization before designing any strategy. For the CISO, the avenue to do this is in understanding the cyber challenges the organization faces, and what approaches the business has taken (or not) to mitigate them.

## Addressing cybersecurity challenges

Organizations tend to underestimate the challenges cybersecurity presents. It is not something that can be addressed as a one-time exercise. A high focus remains on addressing cybersecurity challenges with a technology-based solution. However, cybersecurity challenges require a holistic approach across people, processes, and technology, and involve a continual journey of refactoring and improvements, and communication across the organization of what each person's responsibilities are.

This is best illustrated by how an organization handles the risk of a ransomware threat. Ransomware threats will never be zero, as the business needs an internet presence and can't avoid using email communication. Applying technology-based controls is often the very first step an organization takes to address this risk: implementing malware protection, firewalls, and even intrusion-detection systems. But these are just the first step. These solutions are technically sound but do not address the organization's ability to respond when faced with such threats. Instead, a complete cybersecurity response plan needs to be defined and communicated:

- Provide awareness and training to ensure employees know not to click on malicious links or, at the very least, are aware of how to report it if they do.
- Run phishing exercises on all employees as a reminder of these lessons.

- Ensure a response plan is defined to handle this threat scenario.
- Undertake periodic table-top exercises to refine and improve the response process.
- Create a predefined set of internal and external communication plans.
- Draw up a predefined financial budget to help respond to threats.

Ransomware threats require more than the latest technology safeguards. Such is the case for all cyber risks. This also demonstrates the need for an organization-wide cybersecurity culture. If everyone is aware of cyber risks, and what they can and must do to prevent attacks, or what they can do in the event of one, the organization will be better protected. It necessitates that everyone, from the board and CEO down, to recognize cyber as a business risk that needs to be addressed proactively in a continuous manner and not reactively.

To that end, it must be communicated (as appropriate), accepted, and reinforced that:

- There is no “end state” in cybersecurity. The CISO will prepare an organization for as many cybersecurity threats as possible and will prepare to respond to cyberattacks when they happen. The required controls to mitigate the cyber risks of your business will align with the risk tolerance of the organization.
- Cybersecurity controls go beyond technical solutions such as antivirus, a firewall, and other expensive tools. There should always be a balance between people (that is, roles and responsibilities), processes (that is, defined procedures), and technology solutions.
- It is not a question of *if* but *when* your organization *will* be a victim of cybercrime. Many malicious hackers or cybercriminals are capable of compromising your systems quietly and without attracting attention. So, if you are not looking for them, it may seem as if your data has not been compromised. Unlike physical assets, data assets can be stolen without removing the original copies. Despite the security controls the CISO defines in their roadmap, your company can still become a victim of a cyberattack.
- A CISO cannot guarantee that cyberattacks will not affect your organization. The CISO will ensure your cyber risk is mitigated and treated according to your risk tolerance. They will help minimize the likelihood and frequency of attacks with preventative and detective

controls. They will also minimize the business impact and damage through corrective controls and help your organization resume normal operations faster.

- The cybersecurity strategy is effective when your organization is able to detect and respond to a cybersecurity incident quickly, continue business operations, and recover from the incident with the least amount of business impact.
- You should ensure your organization has a well-documented and well-rehearsed security incident response process and plan, a business continuity plan, and a disaster recovery plan (which will be covered further in *Chapter 10, The World of the Board*).

Cybersecurity must be a concern and responsibility, led by the CISO, of everyone in the organization. As CEO, it's crucial to empower your CISO to achieve cyber resilience in your organization. Their understanding of the business is key to this.

With a foundational understanding of the business, there then are core fundamentals the CISO has to address to establish a security framework. Cyber-risk identification and quantification management strategies, and cybersecurity metrics and indicators for dashboarding/reporting, are the starting point for building cyber resilience.

## Cyber risk identification and quantification

In addressing an organization's cyber risks, a CISO must have some visibility of the organization's cyber exposure. Here is where the challenge starts.

The CISO might inherit an existent risk register with a list of identified cyber risks for a business. More often than not, those risks have been defined or described in multiple scenarios as IT security risks and not cyber risks. Often, security professionals associate a cyber risk with a technical IT risk—for example, describing a cyber risk as a **Distributed Denial of Service (DDoS)** attack, where a service or network is flooded with traffic thereby preventing legitimate users access. When attacks such as this are described solely as an IT problem, it closes the door to the business stakeholders, as it is not thought they can offer any value to the solution. In fact, such risks, when described as business disruptions, are opportunities for a business discussion.

Conversely, many of today's cybersecurity practitioners, having spent time in a cybersecurity risk silo, are trained in traditional qualitative frameworks, the "red, yellow, green" or "high, medium, low" risk classification paradigm. The lack of clarity, precision, and expressiveness inherent in this paradigm is a significant impediment to business risk management initiatives. Instead of broadening the risk assessment and mitigation in the larger business risk context, it silos the response and any solution runs the risk of being a stop-gap effort, unique only to the specific incident. Cybersecurity risk management that is built on instinct cannot objectively measure the risk with accurate financial figures. The CISO with a holistic approach and an understanding of business goals and risks should be prepared with an appropriate remedy.

While this framework has its own benefits, it does not allow security professionals and, especially, CISOs to answer the following questions:

- What is the probability that the company will be the victim of a significant cyber incident in the next six months?
- Is the risk higher than 60 percent?
- What are the financial consequences?
- What are the potential scenarios?

These are important questions, but this framework does not support clear communication with key business stakeholders where they can understand an organization's cyber risks. Without this understanding, it is difficult to attain the support for the necessary investments to mitigate/treat or transfer the cyberthreat in alignment with their risk tolerance. Therefore, it is crucial to put financial numbers to cyber risks, ensuring the visibility of the potential financial losses following cyberattacks and/or data breaches.

When the CISO identifies possible financial consequences, the board of directors and the C-suite can collaborate more effectively on strategic cybersecurity initiatives. A successful CISO should be capable of identifying and matching an organization's security investment to the board's risk tolerance, and in a diplomatic manner. This awareness, and acceptance, of cyber risk better positions the CISO to build effective mitigation measures by investing in security controls and identifying risks that may be transferred through cyber insurance.

This is the primary benefit of using a quantitative framework—adding accuracy and defensibility to cyber risk, with measurable outcomes. It is an undeniable benefit for CISOs to understand the organization's exposures, prioritize cyber initiatives, request additional budgets, and, especially, prove the cybersecurity **return on investment (ROI)**.

Another tool CISOs should focus on are scenario analyses: predicting the financial impact and severity of cyberattacks with reasonable accuracy. While calculating the probability of an occurrence, such as a successful phishing effort or ransomware attack, is difficult, the CISO can modify quantitative models to account for their organization's risk profiles and relevant situations. CISOs can support the business by quantifying the impact of a cyberattack rather than focusing on the probability alone. While specialists have a variety of models at their disposal, no model is perfect. We will provide further details on this in the *A Bonus Segment for Our CISOs* sections in the second part of this chapter.

Once the CISO has identified and assessed the company's cyber risk, the next step is to look at the various ways they can handle those risks.

## The different approaches to handling your cyber risk

There are various approaches to address cyber risk. One is *risk acceptance*, which is when an organization recognizes that the potential loss associated with risk is insufficient to justify investing money to prevent it. This also holds true for cyber risk. If the cyber risk incurred does not exceed your risk appetite, you may accept it.

*Eliminating risk* is the simplest and most often overlooked strategy of risk management. This is a technique that should be used whenever feasible, since it entails simple risk removal.

*Risk termination* may be used, particularly in the context of **merger and acquisition (M&A)** due diligence, when a deal fails to close due to significant cyber risks affecting the company acquisition costs, future investments, and possible substantial residual cyber risks and expenditures.

*Cyber risk transfer* is a topic that increasingly interests boards because of the liquidity and cash support it brings to a business in case of financial losses following a cyberattack.

Risk transfer includes the transfer of future risks or hazards to another party. Purchasing insurance is one of the most frequent forms of risk management generally and cyber risk specifically. It transfers a business's risk to a third party, in this case an insurance company. The transfer of residual risks ensures the recovery of any losses and maintain cash flow and business liquidity.

*Cyber insurance* is a catch-all word that refers to a variety of insurance policies. Defining cyber insurance is not easy, considering the evolving cyber threats and risks. A former colleague of Magda's likened it to *a growing teenager*.

At its simplest, cyber insurance is a contract between an insurance carrier and a business that protects the business against financial losses caused by computer- or network-based incidents. Yet it is unrealistic to anticipate a full list of coverage, since insurers often apply policy extensions in response to the dynamic nature of cyber risk. However, the following list contains those most commonly encountered and accounted for in a cyber insurance policy:

- First-party coverage for the cost of replacing or restoring lost data
- Data privacy and network coverage for the liability claims of a third party
- Business interruption coverage for revenues lost as a result of network downtime
- Cyber-extortion coverage for investigation costs and, sometimes, the extortion demand as well
- Fees for PR firms to manage the business's reputation in the event of a breach
- Legal costs due to litigation or lawsuits

The list is not comprehensive of all the types of potential cyberattacks. For example, it does not include financial crime or financial fraud while using a computer. This is commonly covered under commercial crime policies and is an important insurance coverage due to the increasing number of social engineering attacks, such as phishing attacks or other means of manipulating a person or people to gain access to a system or networks.

Insurance providers no longer provide cyber insurance coverage without an extensive assessment of a company's cybersecurity posture (or what is called *underwriting data*). Thus, it is becoming harder to get optimal coverage for all cyber risks as companies sometimes do not even have the fundamental controls in place to manage cyber risks.

Nonetheless, cyber insurance remains an important control for any cybersecurity strategy. A CISO must consider it as leverage for cash flow management and liquidity control when a cyberattack happens. A CISO new to the organization should review and update the cyber insurance the organization has, or if there is no policy, recommend insurance be purchased to protect the company.

## Cyber risk management strategy

Once the CISO is aware of the cyber risk they are working with and the various ways of mitigating it, the next step is to formulate the organization's cybersecurity vision and strategy.

The CISO's main objective is establishing business cyber resilience and managing cyber risk, which can only be effective if security is incorporated into all planned investments and initiatives. In addition, the CISO needs to take into account the reliance of existing digital tools and services, combined with the likelihood of increased remote working and extensive dependence on third-party suppliers. This may require significant investment.

The CISO should prepare a strategy and associated roadmap, outlining the organization's capabilities to achieve technical and strategic cyber resilience. A clear cyber strategy must align with all important business decisions, as well as a defined roadmap for cyber-risk management.

Specifically, the cyber strategy involves estimating exposures, implementing the right mix of technology solutions and processes, and developing specific recovery plans in the event of a breach. Additionally, the strategy should outline how the organization will manage its ties with partners and third-party vendors worldwide to extend your organization's cyber capability and visibility, moving your cyber capabilities from a siloed function to a resilient and cyber-ready ecosystem.

Further, the CISO will introduce several new strategic initiatives. These include initiatives around governance, processes, culture, and new technological tools. The strategy usually includes initiatives to be implemented within the first three, or even the first five years, for detecting, preventing, and responding to cyberthreats.

One purpose of this strategy should be to establish stronger lines of communication to the C-level and board of directors about cyber risk, focusing on measures or key performance indicators (further explained

in the *Cybersecurity Metrics* section) to evaluate the organization's cyber maturity progression over the next few years.

Under the cybersecurity strategy, the CISO might define a budget for the initiatives they plan. For example, Magda uses the costs in her high-level draft roadmap and then updates her strategy with the budget requirements.

Once the strategy is in place, it is then supported by a roadmap with initiatives that address the following areas:

- **Protect:** These initiatives are intended to deploy and verify adequate cybersecurity protections in place for your organization's systems, networks, and facilities.

Included in protection initiatives are risk identification; mitigation measures spanning people, processes, and technology; and the development of a cyber culture across the firm. Now, the strategy can include concepts such as zero-trust.

Zero trust represents a fundamental change in the way organizations think about security. It starts with the assumption that both users and devices cannot be trusted at face value regardless of their location, and all access requests must be verified before being allowed access to resources. This is a major shift from the traditional perimeter-based security model, which placed inherent trust inside the walls of the organization and blocked external access altogether. In a post-pandemic, modern technology world, our assets are no longer always within the four walls of organization, opening up major holes in our perimeter-based approach of old. Zero trust modernizes this approach—embracing the new way of working while bolstering security both inside and outside our organization's four walls. However, it is important to mention that enabling fundamental controls is still required first before aiming to adopt newly emerging concepts and industry buzzword solutions.

- **Detect:** These initiatives are used to ascertain the degree to which your organization promptly uncovers cybersecurity incidents. Following protection and mitigation, a CISO provides an organization with the tools necessary to identify any suspicious behavior or incident.



- **Respond:** These initiatives are intended to verify the organization has policies and processes in place that outline how the company will respond to cybersecurity incidents. Your organization should have an incident response plan as part of the business continuity plan. It should be tested regularly while engaging the correct stakeholders in the response actions required to mitigate the effect of an attack. As CISO, you provide your organization with the tools necessary to react to security or data breach incidents.
- **Recover:** Those initiatives are to guarantee the organization plans for and executes suitable resilience operations restoring any capabilities/services that have been compromised as a result of a cyber incident. The recovery function mitigates the damage caused by a cyber incident. The CISO ensures a proper recovery following a cyber incident.

The following figure showcases the **National Institute of Standards and Technology (NIST)** government agency cybersecurity framework used by many CISOs as a good baseline of controls to follow while preparing their roadmaps.

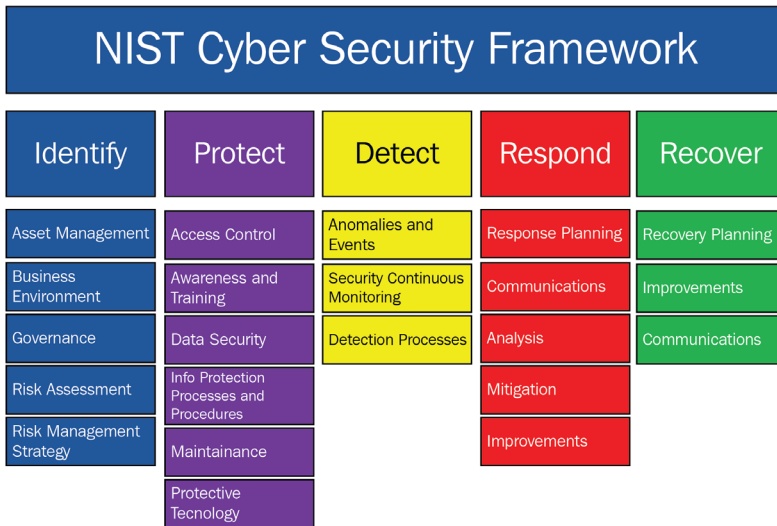


Figure 5.1 – The NIST framework

CISOs use frameworks to ensure full coverage of cybersecurity controls; however, the key is to ensure relevance to an organization itself. This is done using metrics to support improvement and corrective actions.

## Cybersecurity metrics

**Key performance indicators (KPIs)** are beneficial for the CISO to assess the performance of the cybersecurity program and assist with decision-making. One popular maturity model is ISACA's **Capability Maturity Model Integration (CMMI)**, a product and service development maturity model created by Carnegie Mellon University's Software Engineering Institute.

The defined CMMI procedures chosen for integration with risk management processes include actions that lead organizations to implement highly mature development and service processes. CMMI procedures are general in nature and may be applied to a wide variety of specific business processes. CMMI has a broad scope and, hence, may be used to incorporate IT risk management into the (re-)design phase of any kind of IT process, meaning IT risk management can be integrated into the efforts to enhance IT processes or cybersecurity.

The following figure showcases examples of the maturity levels.

**STANDARDIZED DEFINITIONS OF MATURITY**  
PEOPLE, PROCESS, TECHNOLOGY

	<b>LEVEL 1</b> PERFORMED	<b>LEVEL 2</b> MANAGED	<b>LEVEL 3</b> DEFINED	<b>LEVEL 4</b> QUANTITATIVELY MANAGED	<b>LEVEL 5</b> OPTIMIZED
<b>PEOPLE</b>	General personnel capabilities may be performed by an individual, but are not well defined	Personnel capabilities achieved consistently within subsets of the organization, but inconsistent across the entire organization	Roles and responsibilities are identified, assigned, and trained across the organization	Achievement and performance of personnel practices are predicted, measured, and evaluated	Proactive performance improvement and resourcing based on organizational changes and lessons learned (internal & external)
<b>PROCESS</b>	General process capabilities may be performed by an individual, but are not well defined	Adequate procedures documented within a subset of the organization	Organizational policies and procedures are defined and standardized. Policies and procedures support the organizational strategy	Policy compliance is measured and enforced Procedures are monitored for effectiveness	Policies and procedures are updated based on organizational changes and lessons learned (internal and external) are captured
<b>TECHNOLOGY</b>	General technical mechanisms are in place and may be used by an individual	Technical mechanisms are formally identified and defined by a subset of the organization; technical requirements in place	Purpose and intent is defined (right technology, adequately deployed); Proper technology is implemented in each subset of the organization	Effectiveness of technical mechanisms are predicted, measured, and evaluated	Technical mechanisms are proactively improved based on organizational changes and lessons learned (internal & external)



 | 

Figure 5.2 – Maturity models

Maturity is certainly a good indicator. Nonetheless, CISOs need to have a better understanding of the company's cyber maturity and its alignment with business expectations. However, when it comes to reporting metrics to the board, it is crucial the CISO keeps it relevant and concise.

Creating dashboards to capture and report data are important to validate the cyber strategy and roadmap.

## Indicators for dashboarding/reporting

The clearest way for a CISO to bring all stakeholders on board with the organization's cyber strategy is to present the indicators relevant to them. Those likely include:

- New business initiatives and associated cyber risks.
- Unmitigated cyber risks and the cost associated versus forecasted costs.
- Transferred risks and gaps.
- Intrusion attempts.
- Rates of incidents, their severity, reaction times, and the time required for recovery.
- Response times for vulnerability patches.

## Questions to ask your CISO

Because the CISO is the focal point for cybersecurity, the following questions help you determine if your CISO is leading your cyber resilience effectively. For CISOs, this is a helpful way of assessing this for yourselves.

- How do our strategy and roadmap address our business priorities?
- What is our residual risk, and how do we measure it?
- What are our major black swan events?
- What is the potential financial loss following a cyberattack?
- What is the potential loss following a data breach?
- How do we measure our ROI?
- How do we monitor improvement?
- What is our response when a cyber incident or data breach happens?
- How do we recover associated costs?

In the next part of this chapter, we include bonus segments for our CISOs. The segments include tips and advice for aspiring CISOs. They are also good recommendations for C-suite executives to read while trying to leverage further knowledge on cybersecurity and to help support their CISO. To this end, we will next take a look at decoding your CxO's expectations.

## **A Bonus Segment for Our CISOs— Decoding Your CxOs' Expectations**

Boards of directors have a challenging task when it comes to cybersecurity. On one hand, they must guarantee their business remains competitive and profitable, adopting technology and executing digital transformations to stay ahead of the market. On the other hand, they must ensure their business is cyber-ready and compliant with applicable laws and regulations around privacy and cybersecurity.

Over the decades, there have been plenty of technical discussions around cybersecurity. However, the presentation ends pretty quickly when presented to the board or other CxOs if the CISO is not clear in their communication and/or uses too much technical jargon.

Every professional, including the CISO, has a domain of expertise and feels comfortable discussing that skill set. Nonetheless, a modern CISO needs to adapt further, as the expectations are higher, often putting themselves outside their comfort zone. They need to understand the other CxOs' challenges and priorities and put themselves in their shoes to build trust and have effective communication. The expectations of your CxOs in cyber briefings differ from each other but subtly yield significantly similar outcomes—cybersecurity benefits for their initiatives and roles. Once the CISO decodes the rubrics of each executive's expectations, aligning the responses to each of the target CxOs becomes a less onerous task.

A CISO needs to build a reputation as an enabler of the business and not an inhibitor. They need to realize and understand that the first goal of the business is business and not cybersecurity. The business objective is to generate a profitable product or service, ensuring higher gains and growth. The CISO adapts the business perspective to achieve the optimal cyber strategy.

The CISO communicates cyber risk to CxOs through routine updates or reports—for example, a company-wide quarterly executive meeting. However, communicating should occur more often than quarterly. Cyber reports sometimes have to be sent via email. Thus, it is critical that the routine updates or reports are clear and simple, and identify anticipated questions that might be on the CxOs' minds and provide answers.

## Key Communication Non-negotiables

“*Simple reports often work the best,*” says Dr. Siva Sivasubramanian, CISO at telecoms giant Optus. Siva provided examples of the different approaches a CISO can take for the various stakeholders:

- The **CFO** and **CRO** focus on the risks of the cyber issues that have the potential to impact an organization, particularly in specific operational domains. They need to know how initiatives that are underway, and those that are planned, will mitigate those risks. They need quantified responses with clear and defensible figures.

Often, the CISO will struggle to provide these responses, as they are more comfortable with qualitative risk assessments. The reports to the CRO and CFO must be in business-speak and risk-focused, with a clear articulation of ROI and quantified risk reduction per dollar spent. Strict avoidance of cyber buzzwords is critical. Every statement must be logically and quantitatively defensible with facts and figures. Engaging finance or risk groups when preparing the report will help.

Here are some quick tips:

- Present easily understandable relevant data to the CFO in simple tables.
- Avoid complex diagrams or graphs that are technical and unrelated to the CFO’s priorities.
- Have a cohesive storyline of the problem (for example, what is being done, what will be done, how it will eliminate or mitigate the problem, and the cost and timeline involved).
- **Chief Human Resource Officers (CHROs)** are often not tech-savvy but are widely read. They quickly get excited about media reports on recent cyberattacks and their impact on corporations.

The CHRO’s focus is centered entirely on the human and organizational aspect of implementing cyber protection. To them, *employees* mean an aggregation of direct employees, contractors, and third-party vendor resources both on- and off-premises. Their concern is on the logistics of getting staff to participate and act per directions. They also need metrics to measure what constitutes action and how inaction should be handled. In addition, the CHRO likely

will seek some assurance that the proposed activity will be effective, as they are wary of employee fallout from botched activities.

CISO statements such as “*security is everyone’s responsibility*” and “*employees must be held accountable for security*,” without actionable recommendations and simple explanations, will concern the CHRO, as such statements are overly broad. Statements free of rhetoric with quantifiable measures of compliance and suggested responses to noncompliance (limit these to educating and bringing into the fold; avoid punitive recommendations) will hit the target for a CHRO.

Here are some quick tips:

- Ensure your presentation is simple and relevant to the CHRO.
- Integrate privacy and compliance, as they are easily understood by CHROs.
- Articulate what is expected and how that could be achieved for the CHRO.
- Suggest methods and compensating controls to bring noncompliant matters on board.
- Have a clear storyline (for example, the problem, the broader solution the company is following, the human aspect of the solution, and what is expected from the HR department).
- The **CEO** and **board of directors** are the most demanding stakeholders to deal with. Both expect all the details condensed and presented in a prescribed format that is usually very short and rigidly structured. They are masters of words and read between the lines. Every word in the report has to be well crafted, and the narrative must flow well. The report must be reviewed and ratified by their reporting lines or their team members to ensure it aligns with their expectations.

The CISO report and/or dashboards must be in business speak, provide a comprehensive picture of the problem, and call out the unknowns candidly. Any risk called out must be fully supported by the risk group. Any solution suggested must be ratified by relevant stakeholder groups. The board and CEO view solutions as team responses from the stakeholders. Therefore, the CISO’s report should be a *team response* from the different stakeholders, with the CISO functioning as the presenter.

Here are some quick tips:

- Align with the business priorities.
- Focus on the risk and not the technicalities.
- Talk dollars and not threats.
- Maintain a strong narrative and have proof for every point made.
- Craft every sentence well; check for potential alternative interpretations and edit or delete them.
- Do not include any unnecessary words; keep the sentences sharp and make every word count.
- Avoid complex graphs and pictures; provide simple visual aids to substantiate your message without the need for explanation.
- Have the report reviewed, ratified, and agreed to by the stakeholders.

## Cyber Risk Quantification—the Holy Grail for Your Success

Cyber risk quantification has been mentioned several times throughout this book. It is increasingly considered an irreplaceable tool to address the gap between cybersecurity and business.

Enterprises long have used risk management to assess financial risks and operational risks, among others. The traditional risk management process has evolved along with a business's scope, size, and value, and each category of risk (operational, cyber, financial, and so on) has been followed by its own risk approach and methodologies in the risk management process.

Today, business risk management techniques need to be adapted because most businesses are either technology-dependent or rely on IT to run their operations. In reality, though, we still face significant divergence in the understanding of stakeholders of risk management language, especially regarding cyber risks. This distinction is particularly pronounced between business managers and IT security, risk analysts, and CISOs. Because of this misalignment, companies continue to face challenges in implementing important controls to mitigate their risks.

Cybersecurity experts have long used qualitative frameworks for years – “*green, yellow, and red*” or “*low, medium, and high*” are on most CISO's risk

registers and, sometimes, combined with cyberthreats such as ransomware or DDoS. But this framework has little meaning to the CEO, board, or other stakeholders. Using qualitative descriptions remains subjective—especially for business stakeholders who need precise information about the potential consequences of a cyberattack. What might seem critical or high for one individual might appear green or yellow for another.

Instead, having solid quantitative estimates for both impact and probability enables CISOs and business stakeholders to be prepared in the event of a cyberattack.

Magda has addressed quantification on various levels, following extensive published research and the development of techniques and quantification models. She believes many lack industry standards or do not have potential global applications in the cyber-industry space. The most popular quantification framework is **Factor Analysis of Information Risk (FAIR)**, which emerged as the premier **Value at Risk (VaR)** framework for cybersecurity.

For a CISO, a good place to start is by reading and understanding a firm's financial statements. This first step helps identify the business's priorities and concerns. The financial statements sometimes are published publicly and often include risk scenarios, risk appetite details, and key products and services. The financial statements also provide insights into which service or product generates the most revenue for the organization.

Using what they learn from the financial statements, a CISO needs to build out cyber-risk scenarios. What could happen that would lead to the business's strategic initiatives, products, or services being disrupted? Scenario-building enables CISOs to see risks and opportunities more widely, envision cybersecurity challenges or roadblocks, and identify sources of risk that the business has not considered.

To succeed in this activity, a CISO needs to follow a few basic rules:

- Prioritize major risk scenarios and not minor disruptions
- Strive for realistic occurrences and not focus on the probability, as we know it is a case of *when* and not *if*
- Ensure the scenarios are business-oriented and not technical, and carry sufficient information to estimate losses appropriately



The following are some examples of high-level cyber risk scenarios:

- Interruption or disruption of core systems and business platforms for sixteen days due to a ransomware attack
- Corruption of databases and loss of data integrity, leading to major consumer complaints and cancellations
- A product recall due to a cyberattack on the production line impacting the labeling
- Physical damage and fire due to a cyberattack on a factory
- Extended third-party supplier disruption due to a cyberattack

Once good scenarios are constructed, the CISO starts the quantification process. As part of this process, the CISO needs to identify the different areas that could be affected and whether alternative work practices can be used during a period of downtime. This activity is done in collaboration with the relevant CxO in charge of the affected business activity or initiative.

The following are examples of the impacted areas:

- **Business:** Profit loss, market share losses, and share value fluctuation, among others
- **Resources:** Employees' overtime and resources to address specific requirements, among others
- **Legal:** Lawsuits due to service unavailability or further damages
- **Communication:** Communication requirements due to a lack of service availability
- **Data:** Loss/theft of data or data encryption
- **IT:** Including the time of recovery and build

We provide additional details in the *A Bonus Segment for Our CISOs—Purchasing Cyber Insurance* section; however, the objective is to show clearly that with each scenario, the consequences that affect the wider business are identified, not only IT systems.

This helps the CISO forecast the potential losses and costs associated with each scenario when it happens. This certainly helps start the discussion and showcase how a cyberattack can lead to business risk, and it supports the quantitative aspect where clearly identified costs are listed, allowing business stakeholders to make informed decisions based on their risk appetite.

The following figure shows the what a forecast may look like.



Figure 5.3 – A high-level cyber-risk quantification example

This is high-level, and a CISO should be able to identify the costs in greater detail with the support of their colleagues and peers.

Furthermore, forecasting provides visibility to the board on the ROI for cyber. The benefit (or return on investment) of an investment is calculated by dividing it by the cost of the investment. The calculated value is then given as a percentage or presented as a ratio.

The **European Network and Information Security Agency (ENISA)** introduced a concept called **return on security investment (ROSI)**. To calculate cyber ROI, an investment's net loss is divided by its potential cost. The actual cost of an incident represents a critical component of the ROSI calculation.

This quantification forecast enables an organization to raise its understanding of current cyber exposures, and its capacity to mitigate their repercussions by making deliberate and transparent judgments.

## A Bonus Segment for Our CISOs— Purchasing Cyber Insurance

In some instances, cyber insurance is considered an alternative to internal cybersecurity controls by business stakeholders or IT managers. This is absolutely not the case. Cyber insurance is a fundamental cybersecurity control and is part of the cyber risk management process as a complementary treatment, providing further support when a cyberattack or data breach happens. It helps with liquidity and cash flow management and covers for losses that the firm might incur.

Foolproof security does not exist. By now, you are either convinced or at least bored from reading the same statement. However, it's important to repeat it because it's not *if it happens, but when*.

Cyber insurance is designed to protect businesses and individuals against risks associated with the internet and, more broadly, risks associated with IT infrastructure, information privacy, information governance liability, and related activities. Typically, these risks are excluded from standard business general liability policies or are not clearly stated in standard insurance packages.

Cyber insurance policies typically provide:

- First-party coverage against losses caused by data destruction, extortion, theft, hacking, and denial-of-service attacks.
- Liability coverage that compensates businesses for losses caused to others by errors and omissions, data loss, or defamation.
- Other benefits such as regular security audits, post-incident public relations, and investigative expenses.
- Ransom reimbursements in some cases (at the time of writing)

In short, cyber insurance compensates for cyber-related financial losses.

There are different types of cyber coverage. Also know that coverage differs from one underwriter to another, and one company to another. The following are a sample of the kinds of cyber insurances (*first-party losses*) available:

- **System recovery:** This insurance assumes the expenditures associated with technically restoring the data and eradicating the infection—for example, when a cyberattack impacts the business operations and leads to downtime.
- **Reconstruction of data:** As a result of a cyberattack, not all data can be recovered using backups. Some must be manually rebuilt. This insurance bears the expense of the additional work and personnel needed to do this.
- **Profit loss as a result of suspended activities:** For instance, a DoS attack affects the systems of an online e-commerce website, causing major financial losses. Customers cannot access the website, and for more than 2 weeks, all operations come to a halt. This insurance compensates for lost revenue during this time.
- **Forensic investigation:** For instance, the **Monetary Authority of Singapore (MAS)** requires a detailed incident response with forensic details. This insurance covers the cost of digital forensic vendors.

- **Notification costs:** For instance, a cybercriminal uses a phishing email to steal sensitive patient data from a doctor's office. This insurance bears the expense of alerting affected patients and, if required, authorities.
- **Communication costs:** This insurance pays for external crisis experts to protect a company's brand and aggressively mitigate its reputation online.
- **Production that is defective:** For example, a competitor seeking to harm your organization employs someone to hack into the company's IT system and make changes to the company's product formula. The wholly automated manufacturing factory produces 50,000 bottles of erroneously labeled beverages. The beverages manufactured can no longer be sold. This insurance provides support for the expense of replacing the batch and properly disposing of the unused items.

Along with enhancing security directly, cyber insurance is advantageous in the case of a large-scale security breach. Insurance offers a streamlined financing option for large loss recovery, assisting firms in resuming regular operations and decreasing the need for government aid.

As cyber risks evolve and companies adapt their cyber strategies, insurance solutions are being tailored in conjunction with cybersecurity programs. Because of their financial benefits, they are becoming an integral part of the process.

Again, we emphasize that financial fraud and social engineering might be covered under commercial crime policies and not cyber insurance. The CISO needs to verify and acquire confirmation of coverage. Knowing that social engineering scams are growing and are one of the most popular types of cyberattacks, the CISO should also forecast its financial consequences.

Lastly, insurers' underwriting criteria for offering cyber insurance products are still being developed, and underwriters are actively collaborating with cybersecurity businesses to improve their products. However, the trend is going toward extensive initial checks. The CISO should consider this a good added-value service, with external third-party assurances provided as free services—for example, rating reports and automated scans.

## A Bonus Segment for Our CISOs— Reporting to the Board of Directors

Reporting to the CxOs or the board of directors is not easy but necessary. Several factors need to be considered when presenting to the board, including but not limited to:

- **Strategy:** How effectively does the CISO understand a company's goals and strategic initiatives, and to what degree is cyber risk incorporated into wider board-level decision-making?
- **Board ownership:** To what degree does the board drive strategy and how effectively is it incorporated into risk management procedures at the board level?
- **Financial resilience:** Are cyber exposures quantified and included in a disaster recovery plan that has been stress-tested?
- **Accountability of executives:** How are executive duties for cyber-risk management organized, and how are executives held accountable?
- **Assurance:** How does the CISO ensure cyber risk has been adequately evaluated?
- **Reporting:** How is the board informed about a company's cyber-risk posture and progress?

Many organizations treat cyber risk in isolation from other components of their ERM framework, failing to see the connection between cyber risk and other aspects of board-level decision-making. Reporting to the board should close this gap, and the CISO needs to focus on a few limited main points that will help achieve the end goal.

The board presentation should focus on and clearly answer the following questions:

- How well will the board of directors comprehend the company's cyber-risk goals and strategic approach?
- What improvement initiatives are in place to reduce cyber risk to a level that is acceptable?
- How much investment is forecasted for cyber-risk management?
- How is cyber risk integrated into wider board-level decision-making?

In reporting, there should be no technical jargon nor focus on cyberthreats and scare tactics. Those serve as roadblocks and hinder the opportunity for a CISO to justify having a seat in the boardroom.

## Summary

In this chapter, we managed to decode many of the expectations for a CISO, their priorities and challenges. From technical security to a seat at the table and often limited funding, CISOs do not have an easy path to building a cyber-resilient business. While a technical leader in some cases, a CISO oversees cyber-risk management. This includes first understanding the company's exposures and then quantifying potential financial losses to understand and prioritize mitigative initiatives and risk transfer. The mitigation needs to encompass controls for people, processes, and technology and not focus solely on IT.

Nowadays, due to the extensive threats of cyberattack and massive adoption of technology solutions, companies vary in their efforts to measure their cyber-risk exposures. Some do not have any visibility into cybersecurity. Others limit it to their IT environment. This represents a major challenge for a CISO who needs to understand the broader business environment they need to protect, before analyzing and identifying the potential cyber risks.

Communication with the business side is empowered by quantifying cyber threats. While some companies are still not convinced of quantification (for example, stating that without historical data, cyber risk cannot be quantified accurately), others emphasize that quantification is necessary for effective cost evaluations. CISOs need to shift their focus to quantification rather than continuing with the usage of qualitative subjective methods. This is done in collaboration with, or with the support of, the relevant business stakeholders.

In the next chapter, we will address the role of the CHRO and its essential role in building a cyber-resilient organization.



# 6

## The Role of the CHRO in Reducing Cyber Risk

CEOs understand that their companies' human resources are critical to their success. As the saying goes: *"Take care of your people first, and they will take of your business."* People, not businesses, generate value.

CEOs across the globe perceive human capital as a top concern, and HR is one of the most essential roles in an organization. HR has a critical role, not just in its traditional responsibilities, but also in cyber resilience. It needs to:

- Protect employees' personal data and other confidential matters.
- Recruit qualified cybersecurity team members.
- Reduce insider threats, with efficient background checks to mitigate risks.
- Support a culture of cyber awareness through onboarding training and continuous professional development.

A company's employees might consciously or unconsciously represent an insider threat—one of the most prevalent cyberthreats and most successful types in data and intellectual property theft and accidental breaches.



The **Chief Human Resources Officer (CHRO)** typically assists the CEO in maintaining the right organizational culture. The CHRO is crucial also in ensuring that critical roles and teams are resourced with the best personnel. In the case of the **Chief Information Security Officer (CISO)** and the security team, the CHRO also works to reinforce the message about the organization's cyber values and implement the CISO's recommendations when it comes to people, processes, and technology.

The CHRO plays a prominent role in corporate decision-making and needs to be appropriately prepared for that job, including cybersecurity and privacy matters, rather than being relegated as a supporting role whose purpose is to execute choices that have already been made.

We will cover the following topics in this chapter:

- Why the CHRO should care about cybersecurity.
- The transitioning role of the CHRO.
- How the CHRO supports cyber resilience.
- The challenges CHROs face with cybersecurity.
- Questions to ask your CHRO.
- A bonus segment for our CISOs—recruiting and building your cybersecurity team.

## Why the CHRO should care about cybersecurity

In the digital age, information has become the lifeblood of organizations. Companies are increasingly reliant on information and information systems to achieve their business outcomes. Information is also a unique asset and exists in many forms, not just digitally.

An information asset may appear as a physical resource in the form of a document. It may reside in the institutional knowledge of personnel representing human resources. Finally, it may *live* in information systems as a digital resource. Like operational and financial risks, cyber risks come in many forms and, if left untreated, can result in business failure.

The CHRO and their HR team are the custodians of any organization's personnel information. The HR department holds significant amounts of

**Personally Identifiable Information (PII)** on its employees, their families, and their emergency contacts, as well as job applicants and company contractors. HR may also hold financial information, including bank account details and tax file numbers. From initial candidate sourcing, visa inquiries, and background checks to professional development and exit/termination processes, CHROs have access to a vast sea of personal and confidential data. This fact immediately links HR to cyber risk, with potential scenarios including data theft, data loss, and even data deletion or alteration. All this business information is *owned* by HR.

While the storage of this information may include both paper and electronic formats, the risk and responsibility for the appropriate use or protection of the information do not transfer from HR to IT.

An insider threat is a danger to an organization and the CHRO must be a leader in preparing for and addressing such threats. An insider threat can come from employees (both current and former), contractors, and business partners who have access to and insider knowledge about the company's security processes, data, and computer systems. Insider threats include both unintentional actors, such as a user who accidentally loses their laptop that contains PII, and intentional ones, such as a malevolent actor who steals data for personal financial gain (espionage).

The 2020 *Cost of Insider Threats Global Report* by Ponemon Institute showed that the average yearly worldwide cost of insider threats increased by 31 percent between 2018 and 2020, reaching \$11.45 million in losses over the two-year period. The report also highlights:

- Negligent insiders are often the main reason for successful cyberattacks, with the average loss from insider threats reaching \$4.08 million per year.
- Simple errors by employees account for 62 percent of all cyberattacks.
- Credential theft is one of the most frequent forms of compromise.

The CHRO oversees sourcing and hiring strategies and plays a critical role in enabling an efficient process in collaboration with the CISO to mitigate insider threats and associated cyber risks.

Perhaps one of the most crucial roles the CHRO and their HR team play is in sourcing the right talent for the CISO's team. However, hiring cybersecurity professionals is becoming very challenging. Cybersecurity expertise is in great

demand, and CISOs require support to hire and retain the right individuals within their teams. It requires strong collaboration with the CHRO.

There are many challenges faced by the CHRO's team when it comes to talent acquisition and retention for security personnel. This small pool of candidates is the result of a lack of a formal education pathway for security personnel and is exaggerated by the exponential demand of organizations seeking to hire security teams. This challenge is also compounded by the nature of the security roles themselves, which can range from being very technical in nature to more risk-focused and policy-driven roles. This requires very specialized talent acquisition resources within the CHRO's team to effectively author the right job description, as well as having access to the right resource pools and networks.

Poorly written job descriptions for security roles are not taken lightly by seasoned security professionals looking for a new position. For instance, consider the job description in the following figure and the associated comments that were posted on Twitter:

**No. What you really mean is you want a 22-25 year old with 10 years of experience, a CISSP and OSCP, programming experience before birth, have a college degree from CMU or MIT. Bonus: you have given a talk at DEF CON or Black Hat.**

Cast your vote and let's see in whose favour it is:



85 votes · Final results

*Tweets commenting on the job posts and certifications' values*

Team player;

Onsite deployment and or travel within Singapore;

Valid information security related certifications, e.g., CISSP, OSCP, CREST CPSA etc.

**Desired Skills and Experience**

Information Security, Technical Documentation, Risk Assessment, Cyber Security, Architect, Technical knowledge, Penetration Testing, Compliance, Operating Systems, Audits, Web Applications, Web Application Security, Team Player, Vulnerability Assessment, Security Research, CISSP

Figure 6.1 – Example job requirements

*Figure 6.1* clearly shows how easily mistakes can happen. The job requirements include very technical certifications and skillsets but at the same time also include risk assessment skills and a managerial certification. Anyone interested in pursuing a career in penetration-testing will pursue the **Offensive Security Certified Professional (OSCP)** first, whereas anyone interested in pursuing a career in cybersecurity management and risk assessment will aim for the **Certified Information Systems Security Professional (CISSP)** or **Certified Information Security Manager (CISM)**. It is less likely a single candidate will have pursued all three certifications.

Certifications in cybersecurity might help confirm a certain level of knowledge and skills, but they need to be properly linked to a job's responsibilities and not randomly listed. The CHRO's team members do not need to understand what each mean, but they do need to collaborate and work with the CISO to establish the basis for reliable and credible job posts. The purpose of certifications is to complement people's abilities and expertise and shouldn't be considered mandatory, except for certain specific job roles.

Now that we've reviewed why the CHRO must care about cybersecurity, it's important to examine how they can be an enabler of cyber resilience and a leader of a cyber-aware culture.

## The transitioning role of the CHRO

As the senior executive who oversees human resource management and industrial relations, the CHRO is responsible for the *people* component of *people, processes, and technology* in an organization.

The CHRO's duties include developing a workforce strategy and company culture, and attracting, growing, and retaining human capital. Many CHROs also responsible for managing workplace safety and health risks. Unfortunately, most do not realize they are also responsible for cyber risks.

Organizations are established for a variety of purposes, but at its core, an organization is a group of people.

Normal HR tasks include supervising employee happiness, engagement, benefits and compensation, diversity, and so on. An exceptional CHRO goes beyond these tasks and seeks to identify undetected issues, such as behavioral or skill gaps. As it relates to cyber awareness, they need to prescribe measures the *people* component that brings value to the company, such as coaching

and professional development. Broadly, the traditional CHRO role includes the following responsibilities:

- Responsibility for the employees. Employees need to be compensated based on how much value they provide to the company—a mix of the job's significance and individual employee performance. The CHRO establishes such parameters.
- To assess key performance indicators, personnel assignments, and budgets. The CHRO should validate whether these are appropriate for achieving business goals.
- To provide accurate competitive forecasts and support the collection of data on competitors and potential retention challenges. The CHRO should identify any changes in human resources at competitors—such as changes to incentive systems or new expertise hired—and the associated impacts on an organization's market share.
- To compare units, teams, and leaders, not only with established rivals but also unconventional ones that may join the market.
- To identify overachievers, who normally bring lots of value to the organization but are also equally sensitive to reporting line changes, lack of recognition, and promotion without transparent communication and consideration, making them a high risk of leaving any organization.
- To work on competitive intelligence, with insights from headhunters, press, and personnel recruited from other firms, suppliers, or customers.

The traditional duties of the CHRO were thrown into disarray during the COVID-19 pandemic as companies were forced to work remotely. Traditional workplace boundaries blurred, and businesses were forced to allow workers the freedom to work from anywhere. This is now the new norm, and this means HR officers have needed to determine which functions need a physical facility, along with the associated expenses, and which functions do not need one.

When comparing the top strategic initiatives for CHROs from 2020 and 2021, this shift in focus is clear. CHROs now focus on reigning in new and upcoming leaders, honing leadership talent, engaging with transformative learning, and equipping themselves with people analytics solutions. Employee well-being/mental health is now the top priority, followed by diversity and inclusion, leadership development, employee experience, and managing remote employees.

Due to these concerns, the CHRO's priorities are transitioning to include:

- How to source the right talent, provide a smooth onboarding process, and achieve long-term retention.
- Handling the cultural component and a company's values.
- Supporting a hybrid or fully remote workforce on an ongoing basis.
- Enforcing diversity and inclusion.
- Playing a crucial role in employees' mental health and well-being.

Cyber resilience is a key component of these newly calibrated priorities. In the digital age, an organization's HR system is almost certainly digitized using either an internal system or a cloud-based *HR-as-a-service* platform. This immediately elevates the CHRO's role to that of a custodian of personal information, meaning they need to ensure that adequate protection is applied to the systems they use.

This next section addresses several areas where the CHRO and CISO can collaborate to improve an organization's cyber resilience and cyber readiness.

## How the CHRO supports cyber resilience

Perhaps the most direct link between the HR function and cybersecurity is found in HR's ability to help control the insider threats faced by the organization. During the sourcing, hiring, and onboarding of candidates, there are security assessments and processes the CHRO can use to support the company by strengthening its cyber resilience and mitigating cyber risks linked to insider threats.

Here are some pre-hiring and post-hiring examples of where the CHRO can support this:

### **Pre-hiring:**

- In the job posting, the HR process should indicate references will be checked and a background check is necessary before confirmation of the hire.
- The HR process must ensure a nondisclosure agreement is provided and signed before sharing any confidential information with the candidate and should advise the hiring manager accordingly.

- When an employment agreement is prepared, the HR process must ensure that clauses around data privacy, confidentiality, and security best practices are included. In exceptional cases, continuous security breaches can be a cause for dismissal in some companies.

**Post-hiring:**

- The HR process must ensure that security awareness training is conducted with newly hired personnel and then at least annually, or per the CISO's recommendations. In *Chapter 11, The Recipe for Building a Strong Security Culture—Bringing It All Together*, we will address cyber awareness and provide more practical examples.
- The HR officer needs to consider specific training for certain functions—for example, secure coding for developers.
- The HR officer or CHRO is responsible for integrating communication about the information security policies, procedures, standards, and guidelines to all employees into the company's communication plans. They are also responsible for ensuring employees' acknowledgment of this communication.

The effectiveness of a security policy depends on the way HR executes it. In addition to the official security policy, which specifies rules and procedures staff need to follow when accessing a company's IT systems and assets, HR can create an informal document as part of an employee's handbook. This document would highlight the company's vision and views when it comes to security.

Communicating the importance of following security best practices addresses the *why-we-do-what-we-do* question and demonstrates that security matters for the business's growth and sustainability. Simultaneously, the document can make clear to staff the possible consequences of breaching the security policy, such as reputational damage or even a lawsuit.

- The HR process must ensure the collection of company equipment, data, and assets, such as laptops and mobile devices, including telephones, smartphones, USB memory devices, and CDs/DVDs, from employees upon contract termination. The CHRO is responsible for ensuring that terminated employees do not retain any data or intellectual property they have developed during their period of employment. These assets also include physical access control methods, such as smart cards and fob tokens.

This list is not an exhaustive one and will not completely address the insider threat challenge, but it will definitely help. Nor should the CHRO do such things in a silo; rather, then should collaborate with or be in consultation with the CISO to identify, develop, and implement appropriate policies.

## The tools HR uses

Most CHROs use technology to support their HR activities and functions effectively and, in some cases, enhance the overall employee experience. HR tools are a diverse set of technical solutions that assist firms in properly managing their day-to-day HR responsibilities. HR technologies make use of automation to help HR professionals save time, decrease expenses, and manage their personnel more effectively.

Often, these tools are sourced and chosen by the CHRO or their team without assessing security and privacy. Magda (co-author of this book) has seen and assessed various HR tools that lack basic security functionality, such as multi-factor authentication for administrators and clear documentation about data storage locations and encryption, all of which serve as security red flags.

Furthermore, various HR tools now are available using the *software-as-a-service* model or are essentially cloud-based platforms. While providing ease and convenience, those tools require adequate initial assessments of their security implementations and practices, after which there needs to be recognition of shared responsibility between the technology, security, and HR teams to ensure the tools are configured securely and data is adequately protected and safe. Close collaboration with the CISO is key to ensuring a successful choice of a HR tool.

## Recruiting qualified cybersecurity team members

The CHRO and their team play an invaluable role by identifying what a certain position demands and realistically analyzing whether the assigned employee fulfills those criteria. As the match between people and occupations is very important to a company's success (especially in cybersecurity), this activity is vital when recruiting the CISO and when supporting the CISO in building a competent cybersecurity team.



If there is a large disparity between a candidate's abilities and the requirements of the job, this invariably causes issues for the CISO, supervisor, colleagues, and subordinates. An inaccurate assessment by HR of a leader's integrity or values will amplify cultural issues within the organization, which can have very deep impacts on the organization for a role like the CISO.

In *Cyber Mayday and the Day After*, co-authored by Shamane Tan and Dan Lohrmann, the former **Chief Security Officer (CSO)** of the state of Michigan, they covered a story on Mark Weatherford, CSO at the National Cybersecurity Center. When Mark was the CISO for the state of California in the mid-2000s, he picked up a few red flags from a new CISO of a large state agency with significant citizen privacy responsibilities.

After several interactions, he tried reaching the CISO several times only to find out that they were no longer employed with the agency: *"In their haste to hire a CISO, this agency had posted a job description, interviewed candidates, and hired a CISO—all without ever conducting a background investigation. Several months after hiring the CISO, a law enforcement organization met with the agency head and informed them that their new CISO had just been released from prison after serving a term for embezzlement."* (source: *Cyber Mayday and the Day After: A Leader's Guide to Preparing, Managing, and Recovering from Inevitable Business Disruptions*, Dan Lohrmann and Shamane Tan: [https://www.wiley.com/WileyCDA/WileyTitle/productCd-1119835305\\_descCd-buy.html](https://www.wiley.com/WileyCDA/WileyTitle/productCd-1119835305_descCd-buy.html))

This is probably one of the more extreme examples, but it only serves to highlight the importance of checking all the critical boxes when it comes to hiring. Imagine the setback to an organization from the loss of time and resources in needing to start over in their search for a new CISO hire, and the time it takes for a new CISO to get up to speed again and build new relationships with the same business stakeholders? And what of the reputation of the organization after their previous CISO was terminated after a short span of time, especially if it is found out the organization didn't do its due diligence in the hiring process?

Building a strong security team is not just about ensuring that our human resources have the right skills, capabilities, and organizational or cultural fit but also that they themselves are not potential insider threats.

At the end of this chapter, we have included a bonus segment for our CISOs, *A bonus segment for our CISOs—recruiting and building your cybersecurity team*, where we will talk more on this topic.

Like most CEOs, CROs, CFOs, and other leaders in the organization, it's unlikely a CHRO will have a cybersecurity background. But they have just as much of a role in cybersecurity and resilience as other leaders in an organization. In the upcoming section, we will discuss challenges faced by CHROs, mistakes often made, and lessons to be learned.

## The challenges CHROs face with cybersecurity

At one of Australia's largest law enforcement agencies, when an employee requests annual leave, their manager receives an automated email notification that asks them to click on an embedded link to approve the leave application.

This process contradicted the information security training that advised staff against clicking on links in emails. Phishing emails sent by malicious actors asking staff to click on links to malicious code or websites are one of the most common, simple, and cost-effective methods used by criminals to gain access to corporate information.

When it was identified by the CISO and communicated to the IT department that managed the HR information system, it became clear that HR had themselves defined the requirements and the process that IT implemented. HR objected to changing this process because it would make it harder for managers. IT objected to changing the system because there would be a cost to change the IT system.

During a penetration-testing exercise, numerous staff responded to the phishing emails sent by the testing team, encouraged by an HR process that had conditioned staff to respond to emails asking them to approve transactions by clicking on a link.

As a team player, the CHRO needs to take ownership of security and ensure that HR processes are aligned and consistent with the CISO's recommendations. HR needs to play a pivotal part in the cyber-risk management process.

Hai (co-author of this book) highlighted a story published by ABC News (Australia) where an investigation by the Corruption and Crime Commission led to a startling find: the confidential details of the entire **Western Australia (WA)** Police Force were accessed in an audit breach.

It was audit time and an auditor from the Office of the Auditor General requested certain documents from HR. Required under the Auditor General Act to make available whatever was requested, among the documents HR gave the auditor was a spreadsheet that contained the PII of every WA Police employee, including their bank account details. A few years later, the same spreadsheet was found on the auditor's personal computer at home during a search when he was being investigated by the Corruption and Crime Commission.

What there wasn't was a process where the auditor general could be informed of abnormal requests from auditors.

This story illustrates the challenges CHROs continue to face between usability and security, especially in a remote working environment. They need to ensure that workers have access to the information they need and are able to conduct their jobs, while also avoiding exposing sensitive data or compromising a company's networks and systems. The CISO and the CHRO need to have a clear discussion about expectations and define the right balance in alignment with the company's risk appetite.

Employees' personal information, not just customer's personal information, fall within the scope of privacy laws. These breaches can be costly, and their security is the responsibility of the CHRO.

There are practical questions that you can pose to your CHRO and probe deeper into their understanding of the cyber strategy. These questions will help align your CHRO's perspective and thinking around their role and strengthen their collaboration with the CISO to support an overall organizational mission of enhancing cyber resilience.

## Questions to ask your CHRO

- Are you aware of the types of PII and taxation and financial information that the HR department holds?
- What HR tool do we use that safeguards our data's privacy and security?
- How do we manage our sourcing, hiring, and onboarding process in regard to privacy and security? Do our employment contracts include security and privacy clauses?
- How does the HR department ensure employees are aware of information security policies and that they comply with them?

- What activities does the HR department undertake to ensure their HR team is aware of legal requirements, such as the Australian Privacy Principles or **General Data Protection Regulation (GDPR)**?
- What activities does the HR department undertake to protect employees from cyberthreats, including cyber-awareness training?
- How do current HR processes ensure insider threats are taken care of if a disgruntled employee is leaving the organization?

A sizable number of cyberattacks have been attributed to poor cyber hygiene and awareness. Perhaps more concerning is that a disproportionate number of cyber breaches were the result of human mistakes and a lack of security knowledge. The move to more remote working means that employees are no longer constrained to working in a physical office. This shift brings new and emerging cyber risks to the workforce but also presents many opportunities. It also means the CHRO's role in an organization's cyber resilience is key to the business's success.

## **A bonus segment for our CISOs— recruiting and building your cybersecurity team**

As an organization's cyberattack surface continues to grow, it is made more complex with the constantly evolving threat landscape. As a result, the CISO needs to build a capable team to support its security strategy. The CHRO and HR team must be important collaborators in this effort.

All CISOs should understand the challenge of trying to hire for one or more cybersecurity roles while ensuring that they don't overlook the fundamental and nonnegotiable requirements of the roles. The CISO needs to choose the right profiles for the right positions but not create a role that cannot be filled. Hiring qualified, experienced, and trustworthy cybersecurity professionals is critical to the success of every security team.

Some CISOs recruit from social media and their own networks. While this might be highly successful if the company is known for its good culture, it undoubtedly isn't enough if there is more than one role to fill.

The following list identifies a few important points to consider:

- **Align your expectations with profiles that complement your skills, helping you address significant gaps with regard to cyber risks as you build the team:** Addressing critical positions first will strengthen your credibility and support your activities and strategy. *Figure 6.2* provides an example of how some CISOs have built their teams with different vertical specializations that are complementary.

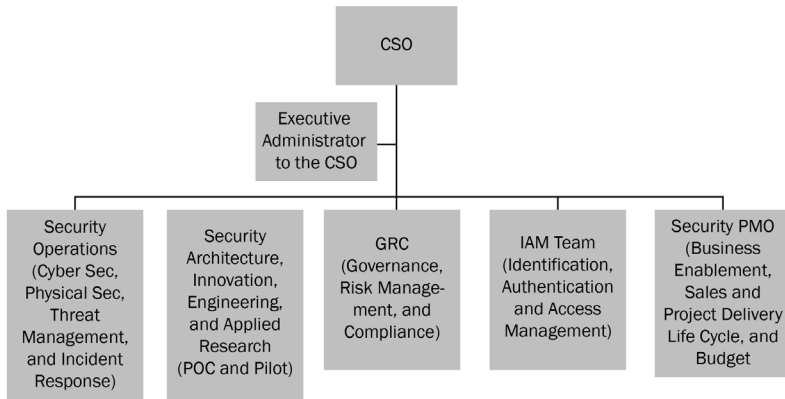


Figure 6.2 – An example of a cybersecurity team structure

The smartest and brightest cybersecurity professionals are almost certainly already employed by another firm. The CISO might need to be more proactive by working with a headhunting agency for more critical and time-sensitive roles.

- **Change the requirements when a role hasn't been filled for four to six months:** Magda found she was able to attract the right resources when she decided to broaden her search and looked at different markets.

With remote working, you can hire almost anyone anywhere. You need the right employee profile, not someone physically sitting at a desk. While this may seem difficult, it can also be an opportunity for many businesses to diversify.

With the Cyber Risk Meetup events ([www.cyberriskmeetup.com](http://www.cyberriskmeetup.com)) that Shamane runs internationally, she has also seen myriad bright and driven individuals who have been very effective in their security roles, despite coming from unconventional backgrounds.

- **Look at career conversion programs and make long-term plans for training:** There is a cybersecurity skill gap. It is a reality. Instead of searching for a perfect profile with all certifications, the CISO can hire someone without the hoped-for technical background and train them up. Such skills can be taught. Attitude, unfortunately, cannot. Focusing on individuals who are ready to learn and improve will help you tap into a fresh pool of exceptional talent who will be more interested in your firm, and you can provide them with opportunities to advance.
- **Look for skills rather than just a degree:** In cybersecurity specifically, many great hackers are self-taught. Do not limit your pool of candidates. One of the most common errors firms make when recruiting is automatically dismissing individuals who do not have the requisite degree or certifications.
- **Collaborate with your CHRO to prepare and publish an appropriate job description:** Getting the job description right is one of the most challenging tasks in cybersecurity recruiting. Often, organizations may not even have the correct job title, which will lead otherwise qualified people to overlook it. This is the CHRO and HR team's area of expertise. Take advantage of it.
- **Seek help:** Sometimes, you simply don't have the time or resources to find top talent. It takes time to build relationships and attend networking events. Hiring a recruiter who is willing to put in the time and effort to identify the best applicant for a job might save your firm time in the long run. Look for a business that specializes in cybersecurity recruitment.

Recruiters who don't speak the language of cybersecurity or aren't familiar with the competence you need won't provide the same outcomes as a specialized cybersecurity recruitment company. This has become a global recruitment challenge, and it is important for cybersecurity recruiting to be recognized for its unique needs, which are different from other types of job recruitment; close collaboration with your CRHO is a necessity.

Every company is different and the CISO owns its team structure. Partnering with the CHRO or HR will yield a better outcome and help you put together the cybersecurity team you need.

## Summary

Traditionally, IT decided what IT systems employees should and should not use, and HR ensured employees were provided with information and training related to policies to maintain appropriate use of the IT systems. When employees were found not to have complied with these policies, HR would be involved in disciplinary action or employment termination.

Cyber risk comes in many forms and, if left untreated, can result in business failure, data theft, or data loss. Today, with the introduction of more cyber-related legislation around the world, the widespread use of technology, and remote working means the CHRO needs to support a strong corporate cybersecurity culture, which requires collaboration with the cybersecurity function in the organization. We must remember that information exists as an asset within people, not just on computer systems or in physical form.

In this chapter, we established how a CHRO can take the lead in managing employee behavior and addressing the *people* and *processes* components of the *people, processes, and technology* triad. The CHRO has a significant role to play in supporting an organization's cybersecurity program and culture of cyber awareness, something that can only be achieved through close collaboration between the HR and security teams.

In light of the current cybersecurity challenges—namely, insider threats and cybersecurity skill shortages—HR professionals themselves will face other organization-wide challenges not covered in this chapter, such as external threats (for example, malicious hackers), software vulnerabilities, and social engineering.

In the next chapter, we will examine the role of the **Chief Operating Officer (COO)**, addressing their critical contributions to cyber resilience, as well as establishing how they can work together with the CISO for business continuity.

# 7

## The COO and Their Critical Role in Cyber Resilience

In the previous chapters, we discussed various **C-level executive (CxO)** roles and responsibilities. This chapter discusses yet another critical executive in your team—the **Chief Operating Officer (COO)**. The COO is the senior executive responsible for managing day-to-day administrative and operational activities. Typically, the COO reports directly to the **Chief Executive Officer (CEO)** and is often second in command to the CEO.

It is not uncommon for the COO to manage a company's internal operations while the CEO serves as its public face, handling all outward-facing communications. As a result, the COO needs to be analytical and possess strong management, communication, and leadership skills. And as the second in command, the COO naturally plays a similar role to the CEO when it comes to their cybersecurity responsibilities.

The COO should proactively engage employees throughout the organization in tackling cybersecurity concerns, playing the role of an enabler and supporter of the **Chief Information Security Officer (CISO)**. Part of an effective cybersecurity strategy is detection, response, and recovery. Regular testing enables the COO and CISO to discover and correct problems, alter procedures, and retrain people as required to assure preparedness for when a cyberattack occurs. This preparedness is critical to avoid significant business interruptions, activity paralysis, and even physical damage.



Therefore, in this chapter, we will cover the following topics:

- Understanding the role of the COO
- Why the COO should care about cybersecurity
- Where the line is between the COO and the CISO in terms of responsibility for business continuity
- Operational technology and cybersecurity—a necessity in today's world
- Business continuity plan management—the dos and don'ts
- Questions to ask your COO

## Understanding the role of the COO

In a modern organization, COOs are at the heart of consumer interaction, innovative technologies, corporate development, leadership, and strategy. Often, they take an active role in the engine room of the organization, while the CEO manages the organization's external image and brand.

The COO's use of technology with automation and monitoring in support of their priorities has greatly optimized their organizational awareness. This optimization has allowed them to refocus their attention on the value of data, and how companies use it to assist in decision-making and drive continuous improvement.

The use of data science techniques and artificial intelligence has provided significant results in fraud detection, consumer trend forecasting, marketing, and data transmission and analysis. For example, the adoption of a well-designed chatbot that can answer customer queries, direct consumers to the appropriate products and services, and even assist with placing orders will reduce an organization's expenditure on its call center. This is a great example of how technology can uncover extraordinary advantages for COOs by allowing them to cut expenses while enhancing customer service.

As a result, COOs can refocus their priorities, with more emphasis on safeguarding the company while increasing its resilience to better survive and maybe even profit from market shocks and variations in business demand as part of its business strategy.

The immediate concern here is the massive expansion of technological adoption. As stated throughout this handbook, while the adoption of new technology is a significant advantage, technology also increases an organization's cyber exposure, which might lead to changes in business activities, priorities, or even operational interruptions due to a crisis-level cyber incident. This must be a priority of the COO.

The COO must have a role in developing solid business continuity and disaster recovery plans with detailed cyber incident response plans. This includes supporting the CISO in the detection, response, and recovery phases. The COO needs to treat cyber risks as business risks, just as every CxO in the organization must. As a result, this may require them to take a step back to consider a holistic view of all operational areas to ensure that the adoption of new technologies does not push an organization's business risk beyond its risk appetite. An experienced COO should be able to distinguish between operational resilience as an offensive strategy and business continuity planning and disaster response as a defensive strategy, as well as why it's critical to switch from one to the other quickly.

Consideration of cyber risks and operational resilience requires the COO to remain up-to-date on threats and communicate these issues with other CxOs or the board or directors. Effective communication needs to balance between the organization's risk appetite for cyber threats and strategic cybersecurity initiatives.

The following section describes the importance of cybersecurity for the COO and how it fits with their priorities.

## **Why the COO should care about cybersecurity**

The COO is accountable for a company's continuous operations in the face of various challenges, including economic downturns, process and technological changes, and natural catastrophes, among others. When it comes to corporate risk concerns, seasoned COOs are masters at dealing with both planned and unplanned risks. This must include cyber risk as a business risk.

Given the COO's responsibilities—vendor management, human resources, operations development, design, and production, among other things—cybersecurity literacy, particularly as it concerns business continuity, disaster

recovery, and incident response planning and execution, is critical. Engaging with the CISO to better understand and define the cyber scenarios that might interrupt business operations is necessary so the COO is prepared to face them head-on in the event an incident occurs.

To accomplish this, the COO must collaborate and communicate with the company's cybersecurity leadership to ensure cyber risk scenarios are incorporated in the overall operational strategy. While your organization's CISO is ultimately responsible for designing cyber incident response plans, their plans are incorporated into its **Business Continuity Plan (BCP)**, which will be discussed later in this chapter.

Lastly, a good COO should be aware of current events in the area of cybersecurity and be mindful of the most recent threats that might impact a company's operations. Cyber response and recovery requires the COO to ask tough questions, such as, *"Have I prepared myself and my business for a cyber incident, and for the recovery afterward?"*

It may appear the lines of responsibility between the COO and CISO are blurred as both must focus on business continuity. To that end, we must identify the line between the COO and CISO's responsibilities.

## **Where the line is between the COO and the CISO in terms of responsibility for business continuity**

The primary responsibility of the COO is to ensure that a company operates smoothly and that operational expenses are kept under control. According to a 2019 Fortinet report, 78% of COOs say they are in charge of protecting operating procedures (see page 3 of <https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/report-coo-and-cybersecurity.pdf>). This requires the COO to reconcile growing security obligations with conventional operational tasks. As such, COOs must collaborate with the CISO and other security executives to protect all operations and business activities from cyber threats.

Understanding cyber risk as an enterprise risk, developing response strategies, and responding fast when an event happens are all things a COO can do to safeguard a firm. A breach is unavoidable, regardless of how well prepared an organization is.

Companies rarely update their business continuity plans for years, allowing them to become obsolete and irrelevant to current and emerging cyber risks. A clear area of collaboration between the COO and the CISO is the integration of cyber incident response into business continuity plans. It is not uncommon for BCPs to present considerations of physical damage and IT disasters, but this is not the same as including cyberattack scenarios. The former is reactive and the latter is proactive. The COO and CISO must take a proactive approach to cybersecurity and resilience. Yet, the ultimate responsibility falls on the COO.

Often, cybersecurity addresses traditional information technology and does not focus on **Operational Technology (OT)**. OT remains critical and requires a dedicated security approach, as its priorities and challenges are different. We discuss that next.

## Operational technology and cybersecurity—a necessity in today’s world

OT is a category of computing and communication systems that manages, monitors, and controls industrial operations, with a focus on the physical devices and processes they use. Manufacturing plants, electricity grids, water utilities, oil and gas extraction, transportation, and other facilities use OT to monitor and manage operations and production activities.

While the integration of cybersecurity in business operations might seem straightforward for most industries, OT COOs have higher stakes in play, with the risk of major disruptions and safety issues caused if there are silos between different operations and cybersecurity.

COOs are dealing with unprecedented levels of change, due to OT/IT convergence and the expansion of their roles to manage cyber risk; such risk management concerns challenge COOs significantly more than any other risk component. At the same time CISOs are expanding their participation in OT cybersecurity.

OT has long depended on hardware and software designed expressly for industrial applications. Consequently, OT and IT infrastructures have traditionally been treated as different entities, both physically and in terms of administration. Many OT networks are unsegmented, with a combination of production protocols, unidentified assets, and older devices. Some have insecure links to corporate/IT networks, while others are completely disconnected from the internet.

More and more OT environments are opening up to the outside world. The use of technology to improve productivity and offer remote support to OT sites is a game changer for the mining, manufacturing, shipping, and logistics sectors, among others. However, providing such access introduces new cyber risks to the OT infrastructure and exposes them to countless well-defined and legacy cyber threats. The impact on a factory or a power grid from a cyberattack can range from a simple interruption to a catastrophic event that might lead to a loss of lives. Magda (co-author of this book) notes that major ransomware events that have impacted manufacturing plants in Asia over the last two years have caused major disruptions, leading to financial losses of millions of dollars.

Given that many firms' OT and IT departments are still separated, it is logical for the COO to collaborate with the CISO and integrate their cyber risk strategies into the business operational plan, as well as the BCP.

Strong business continuity plans are vital to an organization in the event of a cyber incident. The following section describes the dos and don'ts when creating and managing BCPs.

## **Business continuity plan management—the dos and don'ts**

The path to recovery for organizations following a catastrophic cyber event is usually lengthy and challenging. When unexpected circumstances arise, they put good leaders to the test. Any organization's executives, led by the CEO and COO and in collaboration with the CISO, must be able to adapt to the rapid changes in cybersecurity today.

Safe workplace initiatives, employee well-being programs, and business continuity procedures are all examples of plans that must be prepared for when the inevitable happens. COOs must find solutions to maintain business

resilience, or risk the consequences of not being able to recover from it. Even a relatively simple ransomware attack has cost organizations millions of dollars, which some organizations can never recover from.

The COO must, however, first educate themselves as a leader. Fear or uncertainty may lead to emotional choices, leading to bad decisions.

## **Business continuity and disaster recovery must not fail!**

We have all heard of the saying “*Nothing is certain in life except for death and taxes,*” but in the digital age, being the target of cyber crime is fast becoming a certainty. No matter what security vendors may promise, preventative and detective security controls to mitigate cyberattacks are never 100 percent effective. To minimize the impact an attack may have on the business, business continuity and disaster recovery practices must be tested continuously and updated regularly to remain resilient.

Over the last few years, many organizations have had prolonged disruptions to their systems and business operations from cyber incidents involving encryption of critical systems or ransomware demands. These organizations found that their business continuity practices were not set up to deal with large-scale technology disruptions that, in most cases, required in the reconstruction of their entire technology ecosystem.

Shipping giant Maersk is one such example. They had to reinstall their entire infrastructure due to the NotPetya infection. They were without any IT for ten days and ships carrying 10,000 to 20,000 containers were entering ports every 15 minutes. During these ten days, they had to install 4,000 new servers, 45,000 new PCs, and 2,500 software applications, which was a heroic effort within that time frame (see <https://www.itnews.com.au/news/maersk-had-to-reinstall-all-it-systems-after-notpetya-infection-481815>).

Faced with the unavailability of all technology systems simultaneously requires organizations to plan for resource, logistics, communication, containment, and rebuilding requirements before the event. Ten days of disruption might seem unfathomable; imagine the impact on business operations if system disruptions last for months because the organization hasn't planned for such an event.

Having a plan is only half the battle. It must be tested, and retested. Organizations should run simulations and tabletop exercises to ensure that when (not if) the time comes, everyone knows their role and the processes that need to be followed. Business continuity and disaster recovery plans cannot be allowed to fail, and being prepared is key in this.

## What does a good BCP look like?

In the military, the ethos of training and execution is built into their continuity-of-operation plans. There is a famous military saying that goes, *You don't exchange business cards during a crisis*. This is especially relevant for an organization's BCP, as the organization always should plan ahead to know what needs to be done. Planning itself is not enough; there must be clearly defined accountabilities for each role, which are then practiced to instill familiarity.

Building a complete BCP takes time, especially when it comes to identifying the appropriate resources needed, along with the involvement of third-party partners. A very good starting point is to think of the most likely and relevant possible scenarios and then build a plan of action around them.

Another attribute of a good BCP is for it to be benchmarked against similar organizations in the same industry. There is a common misconception that speaking to a competitor about business continuity poses a conflict of interest. This is unfounded as these benchmarks and discussions cover noncompetitive aspects of a business. Organizations that proactively communicate and learn from each other will be much better prepared.

## The methodology

Business continuity and disaster recovery planning around physical hazards such as fire, natural disasters, and theft are core to business operations in many organizations. Very few organizations question the value of creating emergency evacuation plans and rehearsing those plans annually (or more often), yet most organizations seldom suffer a physical disaster. In contrast, the likelihood of an organization being a target of a cyberattack is very high (when, not if), but many organizations still do not have updated **Information and Communication Technology (ICT)** business continuity and disaster recovery plans to address these threats, let alone plans that have been tested and rehearsed properly.

There is no doubt that an organization that can continue business operations while under cyberattack, enact its recovery plan, and reduce the overall impact of the attack is in a much better position than an organization with security policies and cybersecurity tools in place but without an effective business continuity and disaster recovery plan.

Andy Chauhan, former CISO at Ausgrid, the largest electricity distributor on Australia's east coast, highlighted some key points that organizations should consider in assessing their business continuity preparedness:

1. **Before a BCP event:** Planning for a BCP event is key. Organizations should be planning ahead of time to know what needs to be done. The key to a good plan is understanding the following aspects:
  - A. **Which systems are important/critical for the business to operate?** Given the time, resource, and logistical constraints, the recovery of systems must be prioritized. Organizations typically do this through a **Business Impact Assessment (BIA)**, which assesses the priority of business functionalities, such as the effect of reduced operations on the global economy (international trading functions), country (telecommunication services), cross-sector (electricity supply and distribution systems), industry, organization-wide (collaboration systems, financial systems), and divisional levels.
  - B. **What is required to protect and recover the critical systems?** This includes preventative controls such as anti-ransomware controls, backup segregation, isolation controls, or a whole range of cyber controls that protect vital systems from being breached and compromised. While prevention controls are important, they may not, however, be fully effective. Hence, a strong set of monitoring/detection and recovery controls must be designed and implemented.
  - C. **What resources, both internally and from the supply chain, are required to execute the plan?** These include people, equipment (especially if rebuilding systems becomes the only option), access to specialist partners for recovering and rebuilding systems, and negotiating ransom demands. State and federal law enforcement agencies must also be engaged, depending on the nature of the event.



- D. **What insurance cover is available? Does the insurance cover the recovery of systems costs and the financial losses of the impact on business operations?** Typically, cyber insurance providers also now have a panel of specialist providers who can be engaged to assist with recovery activities.
  - E. **Have detailed recovery and response plans (called playbooks) been created?** A detailed step-by-step recovery playbook typically covers who does what in the first hour of an incident, the first day, the first week, and so on.
  - F. **Have recovery and response plans been tested?** There is a saying from Vince Lombardi that “*practice does not make perfect. Only perfect practice makes perfect.*” The perfect practice of your BCP requires your executives and board of directors to rehearse the BCP periodically.
  - G. **How will communications with the organization’s stakeholders, customers, and partners be managed?** In a BCP event, effective communication with the media and stakeholders can significantly impact the share price of an organization. What to communicate, when to communicate it, and with whom need to be planned beforehand. Communication needs to be led by the organization during the event so that the narrative can be effectively managed.
  - H. **What is the governance structure of a BCP event or a crisis event?** Most organizations that have been impacted by weather-related incidents (such as bush fires, storms, or floods) have a well-organized and tested governance structure in place. The board must be involved in critical decisions, such as whether to pay a ransom demand and the implications of doing so.
2. **During a BCP event:** Once your business continuity plan has been created, it must be tested and rehearsed regularly. A common mistake that many organizations make when creating a BCP is making assumptions that the business can revert to manual processes without testing whether the human resources or skills can do so. It could be argued that if the business does not survive because it was not able to maintain business continuity, disaster recovery is pointless. The Heritage Company, a telemarketing firm based in the US, was one such example; after more than 60 years in business, the firm had to shut down its operations for good following a crippling ransomware attack.

There can still be unknowns that come up during a BCP event, despite sound planning and regular testing. All aspects of the plan should be thoroughly tested for sustainability during a cyber event. If the incident is a ransomware event, then the organization needs to consider how to cater to staff fatigue and create a sustainable staff roster, keeping staff well-being in mind. Sometimes, certain equipment may be unavailable or may have lead times, or it may be discovered that assumptions around resources, systems, and the time required for recovery were incorrect. The organization then needs a governance/escalation structure to manage such issues.

3. **After the event:** Chances are that getting back to business-as-usual mode could take months. What, then, are the interim arrangements, roles, and responsibilities in the meantime? Another critical exercise that needs to be carried out is a **Post-Incident Review (PIR)**. A PIR enables feedback and refinement of the processes, playbooks, plans, and impact statements for future events.

When discussing business continuity, it is imperative to understand disaster recovery as well. In the following section, we address the difference between business continuity and disaster recovery, and the COO's role in each.

## Disaster recovery planning

Once an effective business continuity plan has been created, tested, and rehearsed, it must now be maintained. This then allows for the focus to shift to disaster recovery planning. Where a BCP focuses on continuing business operations, disaster recovery planning focuses on restoring ICT systems and information assets to how they were before the disaster. If business continuity planning is likened to the plan to evacuate staff to another location and keep working while the fire department puts out the fire, then disaster recovery planning is like rebuilding the building and its contents as close to the original state as possible.

Most organizations have a reasonably well-established data backup process. However, many organizations fail in disaster recovery planning because of the lack of regular testing to ensure that it actually works when data needs to be restored. A financial technology company that suffered a ransomware attack in South Australia during COVID-19 had their data backed up but found out during the crisis that their custom in-house software was not backed up. This meant they lost their software and could not use the backup

data to restore business operations. They ended up rewriting their software over many months, while processing millions of financial transactions by hand in the interim. Test, retest, refine and update, and test again.

Another failure in disaster recovery planning is keeping copies of your business continuity and disaster recovery plans (which might include procedures and configurations) on the same ICT systems that are at risk of a cyberattack. If cyber criminals gain access to your disaster recovery plans, they can find ways to disrupt them, too.

## Test, test, test. Did we mention your plan must be tested?

There is a common saying that “*practice makes perfect*.” Once the BCP is completed, the next step is to rehearse and test it. A walkthrough tabletop exercise involving everyone with a role in the execution of the plan is critical. The best practice of your BCP requires your executives and the board of directors to take part in the actual exercise. When your board is invested in the process, there will be less doubt about their roles should the business be breached or appear in media headlines after an incident. Their participation in testing builds their confidence about the plan, and the actual execution of the plan in the event of a cyberattack. As a result, this strengthens the organization’s ability to recover quickly. The most forward-looking companies invest time in running these exercises and provide training on what’s expected from the top down, and are committed to improving their BCPs with continual drills.

## Questions to ask your COO

The following is a list of questions to ask your COO about how they incorporate cybersecurity into their business operations planning:

- How do you consider cybersecurity in your operations?
- Do you cover OT (applicable to only specific industries)?
- Who are your main stakeholders?
- Do you hold recurring meetings with the CISO?
- Have you integrated a cyber incident response plan in your BCP and **Disaster Recovery (DR)**?

## Summary

This chapter provided visibility on common practices that might hinder an organization's cyber resilience. We listed the overall responsibilities of the COO and addressed the challenges for them around business continuity and incident response. We identified operational priorities that are implemented for more traditional major crisis events, and showed the need for priorities to shift toward cyberattacks and major disruptions due to threats or attacks such as ransomware.

The COO drives business sustainability and resilience by adapting to new and emerging risks and making the changes required in their traditional practices. These changes will increase over time due to widespread adoption of the technology and the shift to working remotely. This highlights the need to change and evolve while building a transparent and strong collaboration with the CISO and other stakeholders.

In the next chapter, we look at the Chief Technology Officer and what is required from them as a result of the current technological tsunami.



# 8

## The CTO and Security by Design

The **Chief Technology Officer (CTO)** is an executive who handles an organization's technical requirements and **research and development (R&D)**. The CTO often reports directly to the **Chief Information Officer (CIO)** but in some organizations may report to the **Chief Executive Officer (CEO)**. The CTO is also responsible for overseeing technology development for the company's customers, and may handle internal IT operations for smaller companies that have no CIO.

When working with your CTOs, it helps to understand their priorities, potential conflicts of interest with the **Chief Information Security Officer (CISO)**, and the importance of security by design and secure coding for the CTO's role in cybersecurity.

We will cover the following topics in this chapter:

- The role of the CTO
- Why the CTO should care about cybersecurity
- How the CTO becomes a security ally
- Secure coding and secure software development
- Conflicts of interest and collaboration between the CTO and CISO
- Questions to ask your CTO

## The role of the CTO

The CTO oversees and controls a firm's IT components while also focusing on future business technology demands.

Responsible for the technological direction of a company, the CTO oversees R&D to ensure new products are innovative and effective. They also work with other departments to select and implement the best technical solutions for their needs. In addition, the CTO is often responsible for strategizing how technology can be used to achieve company goals.

Among the specific job tasks are:

- Defining technological objectives.
- Developing a technological approach to support business goals.
- Establishing a new infrastructure.
- Maintaining data security and network efficiency.
- Making technical advancements.
- Developing external customer-facing technology.
- Taking charge of initiatives in line with the target audience.
- Reviewing budgets and technology requests.
- Expertise in network architecture, big data, information security management, and software development.
- Innovation and thought leadership.

According to Deloitte's research on CIO reporting lines (<https://www2.deloitte.com/us/en/insights/focus/cio-insider-business-insights/trends-in-cio-reporting-structure.html>), firms where the CTO reports to the CEO are more likely to have a comprehensive, enterprise-wide IT strategy than organizations with different reporting structures.

Regardless of who the CTO reports to, they are responsible for an organization's technical implementation and advancements. As technologies evolve, the CTO is accountable for guiding teams through the adoption of new systems, processes, and procedures. Additionally, normally the CTO is in charge of all engineers and technology-related divisions as well.

With these roles and responsibilities, management skills are a key requirement of any CTO. As RubyGarage, the Ruby on Rails development company, notes, “... *CTOs at some of the world’s most successful unicorns have mostly management-related missions.*”

There are no limits to the challenges a CTO may face. In addition to ensuring C-level priorities and the digital team are operationally aligned, they must focus on boosting top-line growth and managing an aging infrastructure.

Depending on the size of your company, the CTO may have a dedicated security team who reports to them. If not, the CTO needs to work closely with your CISO and other department heads to ensure everyone is following best practices for security.

It is not uncommon to think the CTO is responsible for cybersecurity. Many people in positions of authority think cybersecurity is only about technology, therefore, the domain of the CTO or the IT department. But as we’ve noted throughout the book, cybersecurity is a complex process that involves people, processes, and technology. It’s not just about installing a firewall or a security software package.

However, not all CTOs have the necessary expertise in cybersecurity, and even if they do, it’s difficult to focus on both technology and security at the same time. That’s why many companies now hire CISOs to focus on the security component. CISOs are specifically responsible for security-related issues and can work with the CTO to make sure that the company moves in the right direction and builds cyber resilience.

## The difference between a CDO and CTO

Organizations are increasingly recognizing the need for a **Chief Digital Officer (CDO)**—someone who can lead and coordinate their digital transformation efforts. The CDO role is still relatively new, so there is no one-size-fits-all definition of what it entails. However, common responsibilities include developing and executing a digital strategy, overseeing digital initiatives and projects, and driving innovation across the organization.

The CDO position generally reports to the CEO or CIO, and they may have a direct reporting line to the board of directors. They typically work closely with other senior executives, such as the CIO, the **Chief Marketing Officer (CMO)**, and the **Chief Operating Officer (COO)**.



CDO and CTO are job titles that are often used interchangeably, but there are some big differences between the two. A CDO is typically responsible for leading an organization's digital transformation, which involves developing a strategy for how the company will use technology to improve its operations and grow its business. A CTO, on the other hand, is usually more focused on the technical aspects of the company's operations, such as overseeing the development of new products and technologies.

Cybersecurity should be a chief concern for the CDO leading an organization's digital transformation as a successful transformation depends on a secure and reliable infrastructure. If the organization's networks and systems are compromised by hackers, it could jeopardize the entire transformation project.

Additionally, as more and more business is conducted online, the CDO is increasingly responsible for protecting the organization from cyberattacks. Given that most organizations are not very good at cybersecurity, the CDO has a lot of work to do in this area.

So, while the CDO is more concerned with how technology can be used to achieve business goals, the CTO is more focused on the actual technologies themselves. Both roles are important in today's business world, which is why many companies have both a CDO and a CTO.

## **Why the CTO should care about cybersecurity**

There are a number of reasons why cybersecurity is important for the CTO. First and foremost, as the executive responsible for technology solutions and data collection, cybersecurity is vital to protect a company against data breaches and cyberattacks. Data loss and downtime both have a significant impact on the company's bottom line and reputation. Cybersecurity also helps to ensure compliance with industry regulations and standards.

In addition, CTOs must be concerned with cybersecurity just as they are with every other element of the company's technology infrastructure. The CTO's job is to advance the company's technical agenda, and cybersecurity is an increasingly important part of that agenda.

As companies become more reliant on technology, the role of the CTO has evolved from that of a behind-the-scenes chief engineer to a more strategic role, overseeing all aspects of the company's technology infrastructure. In

many cases, the CTO is now a member of the senior executive team, reporting directly to the CEO.

With this expanded role comes increased responsibility for ensuring that the company maintains its security controls, and adopts new innovative technologies with appropriate security by default.

It makes sense to have a CISO as a colleague of the CTO in organizations that are either less digitally native or extremely vast or complex. The CISO and CTO should work alongside each other, reporting to the board and working to foster a culture of cybersecurity across a company. This entails not only determining what cybersecurity protocols are currently in place but also ensuring that the appropriate people, processes, and technology are in place as well. They also work together to develop incident response plans in case of a data breach.

This means the CTO typically focuses on big-picture issues, including planning for future technology needs, evaluating new technologies, and overseeing major projects, while the CISO focuses on more operational issues, such as day-to-day management of security policies and procedures and employees are following them. Of course, there is considerable overlap between these two roles, which is why the CTO and CISO must work closely together.

The CTO should design and facilitate a technology strategy, but every member of the C-suite should understand what data the firm has, how it is handled and secured, and what role each leader has in protecting that data. As stewards of an organization's data, arguably an organization's most valuable asset, it's understandable that CTOs are worried about its exposure, unavailability, and even its accuracy. As technology is so important to many corporate functions, the CTO must verify that the technological solutions and services implemented remain operational. Any drop in performance or unforeseen failures could have a huge effect on the whole company.

Businesses should consider the sort of CTOs and CISOs that would work best for their organization, in accordance with its size, maturity, complexity, and current cybersecurity profile. According to an IEEE study of 300 CIOs and CTOs conducted in December 2016 (<http://transmitter.ieee.org/wp-content/uploads/2017/03/IEEE-2016-CIO-CTO-Survey-Results.pdf>), cybersecurity was the most serious danger they faced.

There's nothing surprising about this. The CTO's most essential cyber function is collaborating with the CISO to ensure cybersecurity is never an afterthought for their company, but rather a *cultural necessity*.

## How the CTO becomes a security ally

The CTO can become a security ally by working with the security team to ensure all systems are properly patched and updated, firewalls and other security measures are in place and functioning properly, and user accounts are properly secured. The CTO can also help to identify potential vulnerabilities in a system and work with the security team to develop solutions.

The CTO's top priorities should include a culture and work environment that cultivates cybersecurity as one of its foundational cornerstones. CTOs should set a good example for their employees and educate them on the significance of personal and professional cyber hygiene, including security in the technology development process.

Both before and throughout development, security must be a top priority.

The CTO can encourage cybersecurity literacy and awareness training within the organization. Working closely with the CISO can ensure that any implementation of digital platforms and solutions is appropriately protected against cyberattacks, as well as preparing and pushing for best practices in incident response (including simulated exercises and full-scale simulations). Finally, tight collaboration with the C-suite and board of directors can effectively promote a culture of security and cybersecurity readiness from the top down.

Additionally, the CTO can help to set up processes and protocols that will make it difficult for hackers to penetrate a network or steal data. They can also work with the marketing department to create messaging that will encourage users to take precautions when using company devices or accessing company networks. Ultimately, a secure system is good for business, and the CTO should be on board with making sure all systems are as safe as possible.

CISOs and CTOs can work together effectively by building a relationship based on trust and mutual respect. They need to understand each other's roles and responsibilities and be willing to collaborate closely on projects and initiatives.

Ultimately, the goal is to create a secure environment for an organization while also enabling innovation. The CISO needs to be able to assess risk and make decisions accordingly, while the CTO needs to be able to balance security concerns with the needs of the business.

## Secure coding and secure software development

The CTO of an enterprise is responsible for ensuring all security principles are applied within their tasks and teams. This means creating and enforcing principles, including policies and procedures that protect your company's data, networks, and systems from unauthorized access or destruction.

One of the most important principles is secure coding. This means writing code that is more resistant to attacks and exploitation. CTOs should ensure their teams are trained in secure coding practices.

Another important principle is penetration testing. This involves simulating attacks on the company's systems to identify weaknesses and vulnerabilities. There are a number of reasons why CTOs resist penetration testing. First, it can be time-consuming and difficult to find the right resources to do an effective job. Second, it can be expensive to hire consultants or purchase commercial tools. Third, penetration testing can generate security gaps that need to be addressed, potentially taking away from other priorities. Finally, there is always the risk that something will go wrong during the test and cause production outages or data loss. Thus, while penetration testing is important for security, CTOs come up with various reasons for not wanting to undertake this activity themselves. Nevertheless, CTOs should work with their security team to schedule regular penetration tests. It's a key way to ensure the security of the organization's data, applications, networks, and systems. The headache such testing may cause a CTO is nothing like the problems that will surface if there is a successful cyberattack.

Lastly, CTOs should promote a DevSecOps culture within their organization. DevSecOps stresses the importance of collaboration between developers, security teams, and operation teams. After all, everyone has a stake in the security of the company.

It is the CTO's responsibility to ensure developers have the tools and resources they need to do their jobs. This includes access to the code repository, that they have the correct versions of the software they need, and they have all of the necessary dependencies installed.

The CTO also needs to make sure that the developers are following best practices, such as using test-driven development, writing good code reviews, and using appropriate coding standards. Finally, the CTO needs to be available

to answer questions and help resolve any problems that may occur. Software developers have generally been motivated to place greater priority on the rapid delivery of new features and capabilities. That should not be done at the expense of security.

It is difficult to integrate secure web application development testing technologies with traditional development tools and procedures. The pain of security testing, on the other hand, can be more readily reduced with software development and IT operations (DevOps). DevOps is a software development approach that emphasizes communication, collaboration, and integration between software developers and operations professionals. The goal of DevOps is to improve the flow of information and collaboration between software developers and IT professionals so that they create better software more quickly and efficiently.

DevOps is an approach, not a tool or technology. Some of the common tools and technologies associated with DevOps include Puppet, Chef, Jenkins, Nagios, Ansible, Git, and Docker; however, any tool or technology can be used in a DevOps environment, as long as it helps to improve communication and collaboration between developers and operations personnel.

In DevOps, security is no longer the realm of specialist security professionals but rather a standard aspect of the delivery process. Developers can simply and frequently build software that is free of defects by incorporating security into DevOps, which helps to speed up timelines and enhance the quality of each release.

The integration of DevOps is not a new approach for most businesses, but as pressure mounts to complete code development and move it into live production as quickly as possible, DevOps security becomes increasingly important—as code breaks, and bad actors use automated vulnerability-finding tools, not to mention regulators who keep a close eye on data breaches, software security becomes increasingly critical.

Traditionally, security has been more of an afterthought, and many security practitioners have advocated for DevSecOps to emphasize the idea that the *security* team should not be left out of the dialogue.

When it comes to DevOps security, the view is that security features and requirements are identified early in the development process, when they can be built into the software rather than added on at the end, incurring additional redesign/remediation costs and even having a direct impact on user experiences.

DevSecOps is the combined practice of DevOps and information security or, more broadly, the practice of integrating security into the software development process.

The goal of DevSecOps is to make it easier to write secure code and to catch potential security issues as early as possible in the software development process. This is done by bringing security engineers into the team early on, automating security checks into the build process, and using “secure” coding practices.

## Conflicts of interest and collaboration between the CTO and the CISO

The CISO’s job is to secure a company’s systems and data, while the CTO’s job is to build and improve those systems. These two jobs can sometimes come into conflict, since the CTO may want to build new systems or enhancements that could potentially weaken security, and the CISO may want to hold back on changes until they can be fully vetted for potential security risks.

There can also be a conflict of interest if the CTO is also responsible for acquiring new technology for the company. The CISO needs to ensure these technologies are properly evaluated for security risks before being implemented, which could slow down the adoption of new technology.

There are a few key challenges that can crop up between the CTO and CISO:

- **Misaligned priorities:** The CTO is typically focused on driving innovation and growth, while the CISO is more focused on protecting the organization from potential cyber threats. This can lead to tension and disagreements about where resources should be allocated. From Magda’s (co-author of this book) experience, she has found there are usually two main areas of misalignment between a CTO and a CISO: budget and priorities. The budget is often the biggest area of disagreement. The CTO is focused on investing in new technologies and innovation, while the CISO is concerned with being appropriately financed to ensure the security of existing systems. This can lead to tension when it comes to allocating resources. Priorities can also be mismatched, where the CTO may prioritize new initiatives and projects, while the CISO may prioritize maintaining the current security posture and responding

to incidents rather than introducing new technologies. Again, this tension can arise when decisions have to be made.

- **Different skill sets:** The CTO has a technical background and is typically more comfortable with technology, while the CISO has a security background and may not be as familiar with technology issues. This can also lead to disagreements about how best to address certain security concerns as it's not surprising they may have different perspectives on how to do this.

However, it's important they work together to ensure that all aspects of security are considered, and that any disagreements are resolved in a way that best protects both a company's technology and its information. After all, if a breach occurs due to a lack of communication or cooperation between these two departments, both could be held accountable.

- **Communication breakdowns:** If the CTO and CISO are not able to effectively communicate, then they will not be able to achieve their desired outcome of building a cyber-resilient business. The CTO may not understand the complex technical details of the security measures that need to be put in place, while the CISO may not understand the business implications of certain technology decisions. This can lead to miscommunication and misunderstandings.
- **Security as an afterthought:** As mentioned previously, development teams might focus on getting a working product and leave security as an afterthought. The CTO and CISO must create a culture that maintains open lines of collaboration and communication.

The CTO's and CISO's teams can collaborate at a strategic professional level by finding a balance and compromise to better align their respective priorities. If that is not already built into the organizational culture, it needs to be. Security is no longer the domain of IT teams who come in after an incident to explain why and how your service failed, exhaustingly going through the hotfixes they've done to keep it running because of the security mistakes that were introduced when it was first deployed. Instead, they are now part of the team, integral to every step of the development process.

A DevSecOps approach helps the organization attain a stronger security stance while raising its agility and competitiveness. If done well, the security team will find themselves more motivated to dedicate time to higher-value work, such as threat hunting or dealing with critical-rated remediations, as

opposed to repetitive cyber-hygiene work. The CISO's duty is to identify and focus on security expenditures that will enable a firm to accomplish its strategic objectives with the minimum of acceptable risk, as opposed to the CTO's function of raising awareness and providing resources.

Trust and leadership quality are both essential components in forming an authentic relationship.

## Questions to ask your CTO

The role of the CTO is to ensure that an organization's technology architecture aligns with its business strategy. There are a few key things to look for when trying to determine whether your CTO understands cybersecurity. First, does your CTO have a background in computer science? Second, does your CTO have experience in the cybersecurity field? Third, is your CTO up to date with the latest cybersecurity trends and threats? And finally, can your CTO speak the language of cybersecurity?

If you can answer "yes" to all of these questions, it's likely that your CTO understands cybersecurity. However, if you can only answer "yes" to some or none at all, then it's possible that your CTO doesn't really understand it.

Given the increased importance of cybersecurity in business today, here are some other considerations you can discuss with your CTO to get a sense of how they approach cybersecurity at your organization:

- What steps have we taken to improve our cybersecurity posture in alignment with our CISO's guidance?
- How do you evaluate what degree of risk is acceptable in our adoption of technology?
- Is there such a thing as too much security?
- How do you decide which security investments to make?
- Are you allocating appropriate spending to cybersecurity tools and controls that will safeguard our customers' peace of mind?
- How would you respond in the event of a cybersecurity emergency experienced by a customer?



## Summary

We have covered the different responsibilities of the CTO in detail, exploring the reasons why cybersecurity should matter to the CTO. With this understanding, we are able to mobilize the CTO as a powerful ally and utilize the DevSecOps approach to achieve your desired state, through close collaboration with the technology and development team.

As we come to the end of this chapter, it is important you take the time to reflect on what has been presented. You should also begin thinking about how you can put these concepts into action and begin hiring the right personnel to meet your cybersecurity and technology needs. Remember, a CTO is not a CISO.

In the next chapter, we will tackle the roles of the **Chief Marketing Office (CMO)** and **Chief Privacy Officer (CPO)** and examine how they can also advocate for cyber resilience. The CMO and CPO are the voices of your company in regard to online privacy. The CMO is responsible for communicating the company's cybersecurity policies while promoting a shared understanding across all departments on how best practices can be implemented, ensuring everyone can work together toward building a cyber-resilient organizational culture. The CPO is responsible for maintaining privacy practices and compliance.

# 9

## The CMO and CPO—Convergence Between Privacy and Security

By now, you have had the opportunity to discover the responsibilities and roles of most CxOs as they relate to cybersecurity in an organization. The **Chief Marketing Officer (CMO)** has the job of leading a company's efforts to create, communicate, and provide value-added solutions to consumers, clients, and business partners. This includes collecting data used to determine marketing strategies. When it comes to protecting employee data and customer information, the **Chief Privacy Officer (CPO)** is the executive responsible for putting in place policies and procedures and ensuring compliance with privacy laws and regulations. Privacy policies should outline how businesses handle information obtained from customers, clients, and employees.

In simple words, a CMO aims to collect data and ensure the expansion of business with leads, while the CPO may slow down that process by managing the risk of noncompliance during data collection, process, storage, or disposal.

Both roles are incredibly critical to a business and essential to the business's cyber resilience.

There's a lot of talk in the business world these days about the CMO and the CPO, but what do these roles actually entail? What do they have in common, and where do their responsibilities diverge? In this chapter, we'll take a closer look at both the CMO and the CPO and explore what makes them both so important to businesses' cyber resilience.

We will cover the following topics in this chapter:

- What the CMO and CPO roles have in common
- The role of marketing and privacy in cybersecurity
- The intersection of privacy and security
- The role of marketing and communication following a cyber incident
- Questions to ask your CMO and CPO

## What the CMO and CPO roles have in common

Everything revolves around data, and data is what both of the CMO and CPO roles have in common—one collects it and the other protects it.

With regard to clients, marketing has access to the most sensitive information. It is the responsibility of the marketing team to indicate how the information was gathered with technology, and how it will be utilized by the company. (The technology marketing uses generally will have been approved by the CTO or CIO.) As a result, the CMO must ensure the team adheres to data best practices. Those best practices are usually defined by the privacy policies established by the CPO, in alignment with the relevant privacy regulations and laws. For example, features such as unsubscribing from mailing lists or notifications of privacy policies are mandatory by law in certain countries.

As soon as the data is collected, *both* the CMO and CPO need to make sure they handle it properly, as each data record relates to an individual, and a breach can cause long-term harm to the victim—for example, identity fraud. On the surface level, there might seem to be a conflict of interest between both roles, as the CMO looks to acquire and use customer data while the CPO endeavors to safeguard it.

CMOs and their teams today are incredibly data-driven. They ingest and exploit vast volumes of data with analytics to do more than just create new leads. Data-driven CMOs and their teams are entrusted with ensuring every touchpoint of a firm is personalized to each client's unique customer journey.

To collect the data, a company must acquire and use a variety of tools and systems. In addition to these tools, marketing departments also use third-party suppliers for a broad range of tasks, and many of these services are linked directly to a company's core systems through its website or applications. While these technologies are essential in ensuring a memorable customer experience, they also create major security and privacy risks to the company's user data. Unauthorized parties may access consumer data through a third-party tag on a website, all without the company's knowledge.

CPOs need to be aware of any marketing suppliers that may have access to a company's customer data because of the risks that marketing technology poses to the organization. However, this does not imply that the CMO and CPO's aims are directly in conflict. Both roles are concerned with making sure consumers have a positive experience with the business, and this includes protecting their personal information.

Vendor screening, internal communication, and manual procedures can't completely remove the risks associated with third-party vendor partnerships. CMOs and CPOs need to realize this. If CMOs and CPOs want to avoid a tug of war over customer data and third-party technology and work together for a company's interests, they need to put in place effective marketing security and data protection measures, bringing the CISO into the game.

In the end, CMOs and CPOs have more similarities than they realize. They may be the two most knowledgeable people in the company regarding the importance of customer data and a positive customer experience. Both roles need to work in sync and foster a strong and collaborative relationship.

In the next section, we will describe how these two executives can focus their time on the initiatives that matter most to the future of their company, with the help of the proper technology, rather than just being micro-focused on data privacy procedures.

## The role of marketing and privacy in cybersecurity

There's no doubt the introduction of the **General Data Protection Regulation (GDPR)** in 2018 has had huge regulatory impacts on all businesses, including those outside of the EU and UK. The GDPR replaced the 1995 Data Protection Act and sets out new rules around how personal data must be collected, processed, and stored. Businesses that don't comply with the GDPR can face hefty fines, so it's essential to understand what these changes mean for your organization.

GDPR mandates that all companies introduce new policies, methods, and practices for handling the personal data of their customers, users, suppliers, and employees located in the EU. As a result, any organization anywhere in the world interacting with EU residents' personal data must adhere to the new transparency, security, and accountability criteria set out by the EU.

In Singapore, the **Personal Data Protection Act (PDPA)** provides a basic level of security for personal data. As a supplement to industry-specific laws and regulations, such as those governing banking and insurance, it consists of a number of standards that regulate how personal data is collected, used, disclosed, and handled in Singapore. As a part of this legislation, there will be a nationwide **Do Not Call (DNC)** registry.

In Australia, the **Notifiable Data Breaches (NDB)** scheme aims to strengthen the protection of people's data and improve consumer confidence that their data is safe. As part of the NDB scheme, Australian organizations must notify individuals who may be at risk of serious harm from a data breach—where a reasonable person would expect the breach to cause serious damage in the form of physical, emotional, financial, economic, or reputational harm.

Individuals are increasingly aware of the trend toward collecting personal information and monetizing data. Consequently, customers' expectations for data privacy are rising.

According to the Trusted Tech Report from the Consumer Intelligence Series, 84 percent of customers will stop doing business with a firm if they don't feel confident it processes, stores, and transfers their personal information safely and securely. A company's ability to preserve client data is critical to maintaining consumer trust.

As customers' expectations increase, privacy and security become even more intertwined.

It starts and ends with data management, or rather data governance. The collection, generation, identification, categorization, inventory, protection, and destruction of data are governed by processes and technology.

- **Data protection:** Both the marketing and privacy functions should enable effective communication programs and training, raising employees' understanding of how the data governance process happens and where risk might arise, focusing especially on potential risks around data breaches and regulatory noncompliance.
- **Business differentiator:** Customers and other external stakeholders, such as regulators, want to understand and ensure data protection across the data life cycle within the technological realm. This competitive advantage can only be achieved with an unwavering and united view of the company's approach to its customers, shareholders, and regulators.
- **Privacy by design:** Adding software capabilities and features that generate or gather large amounts of data, most of it personal data, is a common practice for most businesses. It is cheaper to integrate privacy and security controls and practices right from the design phases, rather than having to add them to a product or service after it has been launched. Companies can generate a single set of specifications and a uniform experience for developers to guarantee products and apps are developed in a trustworthy way, by converging the cybersecurity and software development teams.

## Risk mitigation

CMOs and CPOs have a key role in risk mitigation and cybersecurity response. Data loss, information corruption, unauthorized access to confidential documents, and the inability to access critical systems are all possible outcomes of cyberattacks, and they represent critical cyber risks for a firm.

For CMOs, however, the most important consideration is the impact on brand reputation, consumer trust, and revenue. Nick Flude, Sekuro's CMO, and former CMO of Secure Code Warrior and F5 Networks' Head of Marketing A/NZ, shares his perspective that *"CMOs are the head cheerleader for the company's customers and brand. As such we are acutely aware of that responsibility to protect both. We also have access to the company's CRM, so have access to all that valuable personally identifiable information (PII).*

*“Global CMOs also grapple with differing regulatory environments regarding PII. As a marketer, I really want to know everything about you, but as an ethical marketer, I know I can only ask for what is deemed necessary to achieve the thing being engaged with, and I have to be able to demonstrate my handling of that PII when asked. I’ve worked with the governance, risk, and compliance team on privacy policies, terms of use, collection statements, etc. Personally, I’ve taken the strictest regime—GDPR—and built all my systems and processes to adhere to that, irrespective of where my business has been geographically located.”*

The legal consequences for marketing activities can be quite severe, especially if data theft is involved. Depending on the severity of the noncompliance, a company could be fined up to several million or even be forced to dissolve entirely. In addition, individuals responsible for protecting the compromised data in the event of theft may also face jail time in some countries.

With more and more companies collecting and storing customer data, the risk of this data being stolen or leaked has also increased. This has led to a number of high-profile legal cases, such as the 2016 LinkedIn data breach case that saw the personal information of over 100 million users leaked.

The financial costs to companies keeps going up, too, as we’ve noted several times throughout the book.

For CPOs, the most important consideration is compliance with the regulatory requirements during a data life cycle. An organization’s reputation and brand might be tarnished if sensitive or personal data is leaked, damaged, or destroyed.

A company’s ability to continue operating might even come under threat if it is involved with a major data breach. Financial costs have risen 10 percent from its prior year, with losses estimated at \$4.24 million per incident on average, and with 38 percent of that amount coming from lost revenue, according to Ponemon Institute and IBM. When a firm’s reputation suffers as a result of a breach, customers are less likely to do business with that company in the future, further impacting the bottom line. At the very least, people want to do business with those who can keep their personal information safe.

Brand damage from cyber risk—in the form of fines and the on-flow impact of losing customer trust—can be very tangible. This is illustrated by Marriott’s loss of about \$600 million after its 2018 data breach (<https://www.reinsurancene.ws/marriott-breach-cyber-industry-loss-could-be-up-to-600m-air/>); it suffered long-term brand damage and saw some customers switch to its competitors. Every company,

and everyone within the company, should be aware of the ramifications of external data breaches like this.

Figure 9.1 demystifies the overlapping responsibilities between the CMO, CPO, and CISO.

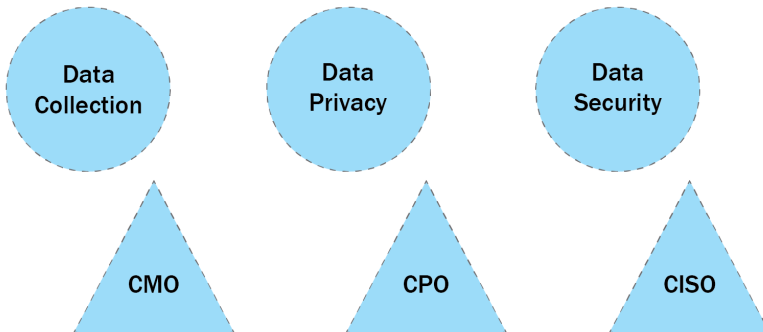


Figure 9.1 – High-level roles and responsibilities

An organization's data governance structure defines who has power and control over data assets and how those data assets may be utilized. People, procedures, and technology are all part of the data asset management framework. All personal data must be maintained with the utmost care, including *real* protection while using technology.

To guarantee protection, the CMO needs to provide clarity and visibility on the company's data collection processes, among other things, and then collaborate with both the CPO and CISO to maintain data protection through established standards for security and privacy. This includes but is not limited to all current legislative requirements and those that may come into effect, while data is stored online or by digital means.

A policy that integrates both security and privacy should assure that the CMO champion the deployment of the most up-to-date security procedures. The CMO plays an important role throughout the data life cycle in ensuring all investments and customers are protected. In the following section, we will discuss adopting this convergent operational model, integrating security and privacy programs, and aiming to safeguard personal information, and how the best practices used to do this have a lot in common and can be leveraged widely.



## The intersection of privacy and security

Organizations' data owners often face conflicting mandates and data requests when privacy and security teams work independently. A single information risk governance team may save money and create a more efficient process. As a result, it is easier for the company's data owners to fulfill their responsibilities of interpreting and enforcing the law.

Separate programs for privacy and security put stakeholders in danger of being misled, and resources are at risk of being wasted because of the separate, sometimes duplicate, plans and implementation efforts. Integrating both programs allows for much more effective work.

In the context of privacy and security, this usually means developing risk assessment procedures that stakeholders must complete before implementing their projects (sometimes known as "security reviews" or "privacy impact assessments"). With a single risk assessment team, both programs' criteria may be met, eliminating duplicative procedures that demand the attention of the stakeholders and providing essential knowledge on new business endeavors and technologies. It is thus possible to offer a single set of requirements and suggestions for a risk-managed business activity, which results in a more timely and cost-effective execution.

Per the World Economic Forum, privacy laws increasingly and oftentimes require data protection. Enabling and achieving this requires the support of the CISO.

The privacy framework Venn diagram in Figure 9.2 depicts the convergence between privacy and security very well. Traditional privacy and cybersecurity tasks have overlapping areas of interest.

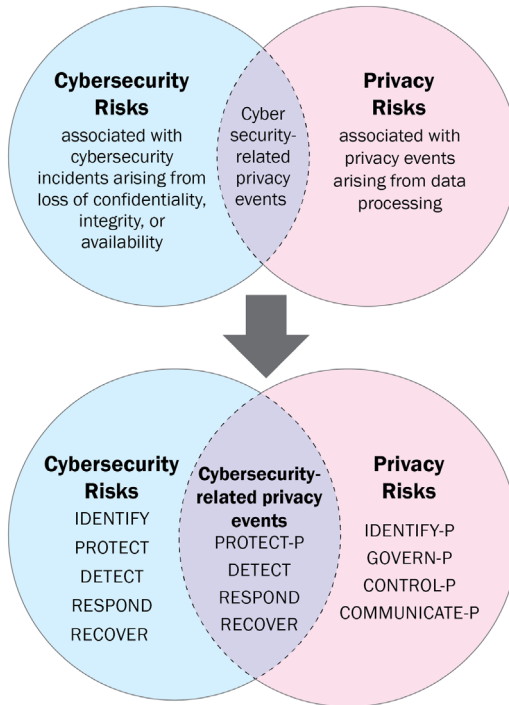


Figure 9.2 – The privacy framework Venn diagram

Although strategic data deletion is one of the most cost-effective and efficient ways to reduce data security risk, security teams frequently disregard privacy controls, even though strategic data deletion is a critical component of most privacy initiatives. Data that has been disposed can be a target of cyber criminals.

In Figure 9.2, individuals’ rights to access and erase their data are protected by a number of practices found on the diagram’s privacy-only side, such as having a legal basis for data collection, being clear about data-sharing procedures, and being fair in how personal data is put to use.

The CMO and CPO share a number of goals in cybersecurity, such as protecting an organization’s valuable data and ensuring the availability of systems critical to the organization’s operations. This includes protecting product designs, strategy documents, and company financials. However, there are many domains where the security and privacy functions perform comparable or related duties with similar aims, and interact with the same stakeholders in the middle.

For this reason, companies should try to take advantage of the synergies between privacy and security teams and consider merging their operations.

In the following section, we will take a closer look at how these advantages can be exploited in more detail with a specific case of a data breach response.

## The role of marketing and communication following a cyber incident

When a company is breached, news spreads. It hits the news headlines. The brand and reputation of the business are threatened. People speculate, and customer confidence is impacted. You also often see a sudden downward dip in the company's share price on the stock market.

More and more mature companies increasingly recognize the importance of having a cyber-resilient organization, which contributes to the business's sustainable growth, and the CMO plays a valuable part in this.

It is chiefly the CMO who is responsible for customer trust, brand, and reputation. With the marketing and communication resources they have at their disposal, much can be done to support and promote cybersecurity awareness internally. In building a healthy security culture, the CMO plays a key role in focusing on the customer/client data, ensuring simple things such as not sharing or sending spreadsheets of PII, and working closely with its vendors to establish what level of PII needs to be shared so that services can be delivered.

For businesses that have strong existing security practices, promoting their internal practice externally can also be leveraged as a marketing tool to instill confidence in their customers.

In a cyber incident or a cyberattack emergency, communication is key and the breach response messaging is critical. The CMO's role, together with their access to CRM systems and data, will become instrumental for **public relations (PR)** and communications. They have to operate quickly and objectively, working closely with the CISO to communicate internally and managing PR and external communications to everyone who has been impacted. As much detail as possible should be given without finger-pointing or blaming. An organization requires an incident response that involves the key stakeholders, including the CMO, CPO, and CISO. Such

communication plans should be included in the business continuity plan and disaster recovery plan.

In the event of a privacy or data breach, it must be analyzed immediately and the CPO notified as soon as possible when personal data is involved. The CPO needs to be involved to determine whether the company is obligated to report the incident, per regulation requirements. The mandatory incident reporting requirements in Australia require every private and public company to report a cyber breach to the **Office of the Australian Information Commissioner (OAIC)**. Also, if the company's annual turnover is \$3 million or more, they are obligated to notify the customers affected as soon as they become aware of the breach.

In Singapore, as another example, the PDPA requires data breaches that involve more than 500 records to be reported. After such an incident, CMOs and the marketing team might work to repair the damage for months, if not years. They need to make sure everyone on the team and the company's social media accounts are conveying the same consistent message and tone.

During the hysteria and confusion of a cyber event, it is easy to overlook accountability and the involvement of key stakeholders. In addition to cybersecurity and risk officer updates, the CMO, CEO, and board members should get reports on reputational risk from the CRO/**Environmental, Social, and Governance (ESG)** department. Customers' faith in the CMO and CEO must be safeguarded in the event of a security incident.

An example of a good response occurred in 2017, when a third-party provider, through a human error, exposed an Australian Red Cross Blood Service file containing information on roughly 550,000 potential blood donors. Those who were impacted and the Australian Information Commissioner were quickly alerted by the organization. According to the Commissioner (<https://www.oaic.gov.au/updates/news-and-media/australian-red-cross-blood-service-data-breach#australian-red-cross-blood-service-data-breach>), *"Australians may be assured by how the Red Cross Blood Service reacted to this situation. At every stage of this process, they have been completely truthful to the public, open with my office, and accept full responsibility."*

In times of crisis, it is key to communicate properly with consumers, suppliers, employees, regulators, and other stakeholders to ensure that cyberattacks aren't made worse by inadequate planning and communication. CMOs are professionals in this area. They must be prepared to be at the forefront of

an organization's response during a cyber event. If a company's marketing staff downplays the gravity of a data breach, they risk further harming their company's reputation. In *Cyber Mayday and the Day After*, by Shamane and her co-author Dan Lohmann, their different research studies revealed that the gravity of post-crisis outcomes is impacted by the communication that goes out during the crisis. Even if the information is not be available right away, a company that takes ownership of the crisis through speedily acknowledging it and providing an official channel for updates and feedback can be a game changer in rebuilding trust and mitigating the loss of customers.

With the current communication landscape, where misinformation and disinformation abound, an information vacuum will only be detrimental to an organization's reputation. The crisis communication process must be part of regular simulation exercises testing an incident or data breach. This will ensure that a holistic and pragmatic approach is taken and that efforts are streamlined, with no redundant tasks.

So, it's crucial your CMO and CPO are in alignment, and are part of the cyber risk management team. The following section highlights the most important questions to ask both your CMO and CPO executives.

## Questions to ask your CMO and CPO

When a firm starts growing quickly with a data-driven marketing strategy, it is critical to ensure privacy and security are integrated at every step, rather than considering them at the end of the process. The following questions for your CMO and CPO are the ones we recommend focusing on initially:

- Who owns the data governance process? Does this process involve our CPO (or CMO) and our CISO?
- Is there any redundancy in our privacy and security assessments? How can they be further streamlined?
- How do we ensure efficient compliance with data protection requirements, especially with the current massive technological adoption?
- Does our incident response process include the CMO, CPO, and CISO?
- Is there a communication/PR plan to respond to a cyber incident and data breach?

We close this chapter with an important message in relation to the correlation and convergence between various roles and responsibilities. In our current environment, highly technologically dependent organizations need to consider streamlining most of their programs to reduce costs and mitigate risks.

## Summary

In this chapter, we have seen the importance of the CPO and CMO in building a company's cyber resilience, as well as their roles during a data breach incident. A data breach could tarnish any company's reputation permanently, and the reputational damage might be more difficult to recover from than monetary losses. It may result in customer churn and revenue losses. Potential new clients will be turned off by tainted Google searches and constant unfavorable coverage in the media.

A data breach is a long-term problem rather than just a single incident. It requires appropriate data protection and a proper data breach response in case of an incident. To achieve those results, collaboration between various CxOs is critical and remains at the core of successful preparation and recovery. From the CEO to their executive team, everyone in an organization needs to understand their role and collaborate with each other.

The next chapter addresses the key success factors for developing an effective cyber-resilience strategy that includes all these key players working together from the top down, specifically the board of directors.



# 10

## The World of the Board

A board of directors' essential role, whether it serves a publicly listed company, a privately owned firm, or a not-for-profit organization, is to offer leadership and governance to enable an organization to fulfill its objectives and purpose. Board members function as fiduciaries or legal advisors to the organizations, instituting solid ethical and legal governance and financial management procedures. Additionally, they often are responsible for fundraising and advocacy for the organization.

Commonly, boards are made up of non-executive and executive directors, led by the board chairperson. The board is jointly accountable for the company's performance and governance. It assigns day-to-day operating responsibilities to the CEO. They are aided in their efforts by an executive committee and other committees, including but not limited to the audit committee, risk committee, nominations committee, and remuneration committee. The board should conduct active oversight and control over the development and execution of the firm's risk management policies and procedures.

In this chapter, we will discuss the critical requirements for a board to understand with regard to cyber risks, and how to empower it to make decisions about those risks.

It's important for an organization to have a board of directors that will help provide stability and guidance as a company grows. But what does this group of individuals do, exactly? This chapter will explore the role of the board and identify some of the key considerations that come into play when making decisions about cybersecurity and cyber risks.



We will cover the following topics in this chapter:

- Understanding the world of the board
- The board's structure
- The board's interests in cybersecurity
- The CISO's seat at the table
- Speaking the board's language
- What *not* to do in the boardroom
- Reporting to the board (an add-on for CISOs and a reference for CEOs)
- Boards and mergers and acquisitions
- Asking the board the right questions and setting up your CISO for success

## Understanding the world of the board

In this information age where most organizations are connected to the internet and dependent on information technology and information systems, a cyberattack could easily result in an organization suffering irreparable damage to its reputation, trust, and brand. Cyberattacks disrupt business operations and have a real financial cost. Put simply, a successful cyberattack is highly likely to cause complete disruption to the business and has the potential to put it out of business.

Nonetheless, many firms fail to prioritize cyber risks in the boardroom, resulting in concerning gaps in their cyber-risk evaluation and mitigation. As public and investor awareness of cybersecurity concerns grows, boards increasingly are compelled to commit more time and resources to manage their cyber risk. By adopting a more proactive stance at the board level, firms may embrace the opportunity to enhance their cyber-risk management, expand their access to capital, and better fulfill investor expectations.

Alternatively, businesses risk being exposed to long-term financial and reputational consequences. This applies especially when making major decisions such as mergers and acquisitions. Consideration of security early on may pave the way to better value in the form of increased revenue, increased customer happiness, and cost savings.

Forward-thinking firms are attempting to simplify the insights and knowledge gleaned from their cyber-risk analysis to the point where executives and the board can take action. They closely link risk to the organizational strategy and address it as part of their risk management decision-making process.

First, it is worth noting that the board's main mission is to maximize the value of shareholders' investment, although in particular cases, this could be detrimental to other stakeholders' interests (such as employees and consumers). Hence, it is important to find a balanced outcome for both shareholders and other parties in a world marked by an increasing need to preserve a social license.

To achieve that mission, the directors of a board should have different but complementary experiences that can combine to produce a holistic view of the decision-making process, while still considering risks. In other words, the board of directors must be able to see the forest surrounding the tree, not just the tree itself. Nonetheless, both the law and daily practice continue to support the concept that the board cannot and should not be engaged in risk management on a day-to-day, hands-on basis.

Rather, directors should ensure that the risk management policies and procedures are developed and implemented by the company's senior executives and risk managers and are aligned with the company's strategy and risk appetite. Directors also should make sure these policies and procedures operate as intended and that the steps necessary to foster an enterprise-wide culture that promotes appropriate risk awareness, behaviors, and judgments about risk are taken.

The board should be aware of the nature and scale of the company's primary risks and should expect full participation in risk management from the CEO and top executives. Through its oversight function, the board can communicate to management and staff that comprehensive risk management is neither a barrier to business behavior nor a mere complement to a firm's total compliance program. Rather, it is an intrinsic part of the organization's strategy, culture, and operations. Additionally, the roles and duties of various board committees in supervising certain risk categories should be examined to ensure the board's oversight function is coordinated and comprehensive.

The risk supervision obligations of a board are generally derived from state law fiduciary duties, federal and state rules and regulations, stock exchange listing requirements, and some recognized (and changing) best practices on a national and international level.

Comprehensive risk management should not be considered a distinct corporate activity but, importantly, an essential, enterprise-wide component that influences how a business assesses and rewards performance. Risk assessment, accurate risk-reward analysis, and smart risk reduction should be included in every company's decision-making process.

Transparency, consistency, and communication are critical in defining the proper *tone at the top*—the board's vision for the business, including its commitment to risk oversight, ethics, and intolerance of compliance failures, should be successfully conveyed across the organization.

Major firms often include in their statements assurances that executive management provides regular updates to the board of directors on risk management issues. Some corporations even include such rules in their annual reports and financial filings. Although many organizations have explicit processes and predefined triggers for reporting—or “escalating”—risk concerns to the board of directors, many others do not. This includes considering the board's supervisory function as appreciating cyber risk as an emerging risk to the firm and being informed of the criteria utilized by management in deciding which information is referred and reported to the board. In making this determination, the board of directors first has to understand the company's cyber-risk exposure and be informed of the company's cybersecurity program and methods for mitigating risk. The board should also encourage a crisis response strategy that requires involvement from various stakeholders in collaboration with management.

## The board's structure

The board's structure is often determined in an organization's constitution or a shareholders' agreement, a legal document executed by all the parties who have a stake in the company. There are also board charters describing the firm's governance. Good governance rules would recommend that a minimum number of independent directors also be appointed to the board to provide different perspectives, including directors who have a range of experiences in a particular subject.

Usually, the board creates different committees to evaluate specific decisions. To operate more efficiently and leverage its resources, the board could gather some of its members with particular expertise into a committee that addresses technical matters and provides points of view to the whole board

to facilitate a decision. Depending on the industry, the following committees might be formed: an audit and risk committee, a regulatory committee, a remuneration committee, and a health and safety committee, among others.

A board director of a New South Wales government critical-infrastructure body shared the opinion that “whatever you do in a company, you always need to take risks to generate returns. But the risk taken must be appropriate and thoroughly monitored. At the board level, the audit and risk committee will consider whether the risk register has been properly documented (identification and qualification of the main risks concerning the internal processes, tangible and intangible assets, and employees).”

He continued: “This register rates the various risks in terms of their probability of occurrence and impact significance for the company. The audit and risk committee must ensure that the company’s management has elaborated and implemented a mitigation plan to limit the occurrence of risks as well as their significance before they materialize.”

This is done to preserve the sustainability/resilience of operations as well as financial profits.

The board must also acknowledge that risks cannot be eliminated but *can* be mitigated most of the time. This is incredibly important for the board, as ultimately it will be held responsible if major event damages the company’s business as a result of a lack of due diligence (*risks not identified and/or adequately managed*).

Shareholders might have divergent interests because of the nature of their business or certain internal constraints not necessarily related to a company. It might happen that shareholders who are represented by board members may engage with each other to learn more about their expectations in terms of the broader strategic direction for the company. The management recommendations are approved, rejected, or subject to board members’ amendments at the board meeting itself.

Ideally, the board usually wants to come to an agreement and empower top management with the agility to execute key decisions for the best interests of the company and shareholders.

A persistent disagreement on a board decision could eventually lead to a deadlock, preventing management from taking action until the matter is resolved. A party could have a minority investment position but with a

“negative control” on board decisions. This governance framework is designed to provide veto rights to smaller investors to protect their interests vis-à-vis major shareholder decisions. The negative control threshold is a commercial decision decided by shareholders as part of the shareholder agreement.

## **The board’s interests in cybersecurity**

Cyber risk should not be considered in isolation, and cyber-risk data should not be presented as random numbers or lists when discussing it with the board. Management must clearly communicate to the board how one risk impacts another risk, including cyber, so all parties can effectively formulate a solution, rather than creating confusion and disinterest.

The capacity to demonstrate how cyber risk is interconnected with other risks is just as critical as the ability to demonstrate how cyber-risk mitigation measures are succeeding. In turn, this can assist the board in prioritizing expenditures on mitigation efforts, understanding the actual return on such investments, and recognizing the value the CISO brings to the organization by developing programs and providing tangible insight into which initiatives are successful and which are not. This enables you and the board of directors to assess whether initiatives are having an effect and should be given further attention, and how your organization’s preparedness and cyber maturity compare to those of other organizations in the same industry.

This is more difficult to do when cyber-risk discussions are conducted using technical terms and numbers. To integrate cyber-risk data, it is essential to uncover vital information from internal and external data, and then standardize the data so it is comprehensible and presented in the context of business risk. When data is trended through time, this report will demonstrate what is effective, what is not, and how the CISO protects the company’s interests and aligns with its goals.

Instead of speaking at the board, the CISO should engage the board in a discussion. Conversations make for the most effective presentations. If you want the CISO to create a lasting impression in the boardroom, they must engage board members rather than just reciting information about important cyberthreats or your overall cyber-risk management strategy. And if board members have questions, your CISO should be able to provide answers ... and quickly. When it comes to conveying cyber risk to board-level stakeholders, these qualities are critical.

In Shamane's research studies with board and executives, her presentation on "Birds and Buttons" focuses on how the four bird characteristics (the **dove, owl, peacock, and eagle [DOPE]** personality test created by Richard M. Stevenson) play out in the boardroom and the trigger buttons that get board members to sit up and pay attention.

After countless conversations and engagements with boards and executives around the world, Shamane has narrowed it down to the following top six criteria for success:

1. Business ownership
2. Appropriate investment
3. Rightly equipped
4. Risk transfer options
5. Maintaining foresight
6. Industry resilience

## Business ownership

First and foremost, the board needs to be aware that they own the organization's cyber risk, and their C-suite executives are jointly responsible for cyber-risk management, not just the CISO.

Although cyber increasingly is recognized by more boards of directors as a priority issue, there is still a lack of formal governance frameworks to support board oversight. The chairperson of the board can contribute by ensuring there's sufficient time allocated in the board agenda for cyber-risk discussions. Some questions to prompt discussion include:

- Do we know who owns cyber risk, especially since it is a strategic business enabler?
- How are we aligning cyber-risk management with business needs? Cyber risks are similar to financial, health and safety, and operational risks; there is an inherent risk, and the executive's role is to approach them from an enterprise-wide perspective, minimizing risk and maximizing business performance.
- Do we have a formal cybersecurity framework or strategy in place? Is the board asking the right questions to ensure cyber risk is woven into business processes right from the beginning? Has it been baked

into major business decision processes in a timely fashion, including mergers and acquisitions, partnerships, or new product launches?

- Does the board have oversight of our detection and response capabilities?
- Is our management team able to detect any cyberattacks or critical events requiring senior-level involvement?
- If an event does occur, do we have a plan? What is it, and how quickly can we recover?

## Appropriate investment

This is an important question the board needs to ask itself: Are we investing appropriately in cybersecurity? Is our current investment (security budget) in cyber defense too much or too little?

The board needs to continuously invest appropriately in the security budget, weighing the costs and benefits of the different risk mitigation and reduction activities, while being mindful that there is no silver bullet solution.

A lot of these things can and will be resolved by more investment, controls, automation, and processes. But that still leaves us with the naïve and compassionate humans—our employees—and we need to continuously raise awareness and build a healthy security culture, highlighted in more detail in the next chapter.

## Rightly equipped

Are we rightly equipped to protect our most valuable assets? This includes securing our supply chains by holding our suppliers to high standards.

How does our organizational design and structure fare in supporting our cybersecurity strategy? Residual risks that cannot be mitigated within the security budget should be accepted by the board, and if not, additional resources should be looked at to reduce those risks.

In terms of protection, do we have the right tools, processes, and people (including at the board level itself) in place to protect our boundaries? Do we have access to expert **SMEs (subject matter experts)** to make well-informed decisions? How are we incorporating cybersecurity expertise into board governance? Do we have appointed board directors with cyber

skills? How often do our board directors receive training on cybersecurity? In the AICD survey conducted of 856 board directors in May 2022 (<https://www.aisa.org.au/common/Uploaded%20files/Research/FINAL%2008299-3-5-Cyber-Security-Report-30pp-v3B.pdf>), only 23 percent of them have appointed directors with cyber skills, and 43 percent of boards do not receive any training on cybersecurity.

A more proactive approach to providing ongoing education to the board is required, given the increasing and evolving nature of cyber risk.

## Risk transfer options

This is a simple question: If there is no adequate cyber insurance, do we know what the exposure to the board is? And if there is insurance, does the board know what is exactly covered? What are the benefits and does this effectively align our cyber risks with our business risk tolerance? And if not, are there risk transfer options that can be considered?

## Maintaining foresight

It is important for organizations to keep up with current affairs and be prepared for regulatory changes. Has the board determined who will provide top-level sponsorship for upcoming cybersecurity-related legislation and regulation?

Have we tied in future economic drivers and digital transformation with their impacts on our cyber risk? And if so, how do we track, respond to, and budget for new threats? Do we understand the legal ramifications for the company?

We are in a constantly evolving landscape where people are now more aware than ever about securing their personal and private information. How can we champion a secure culture within the organization?

## Industry resilience

Finally, we need to know that to stay resilient, we cannot do it alone. Collaboration is needed for our industry to be cyber resilient. The board should explore ways of participating with other information-sharing organizations within the wider ecosystem.



How are we doing in peer reviews? Do we know how we benchmark against other companies in the same industry and of a similar size?

As long as the board is aware of the preceding six criteria for success, they are on a strong footing and can use these criteria to guide them and their executive team accordingly.

## The CISO's seat at the table

As the CISO's position evolves and develops, your organization must assess the success of its CISO by ensuring you hired the right candidate, asking yourself the following questions to do so:

- Is our CISO equipped with the necessary skills?

The good news is that there is no one-size-fits-all approach to success. A good CISO does not need a technical background or a degree from a well-known university. Indeed, research published by Digital Guardian found only 27 percent of CISOs have IT degrees, while those with computer science degrees accounted for 23 percent.

Modern-day CISOs need to have good management and leadership skills and recognize cybersecurity as a business risk. The CISO needs to collaborate with leadership to establish a shared understanding of security architecture, define the responsibilities of IT and security operations, and deliver outcomes via the development of the relevant team and internal connections. In summary, you need to establish the CISO's suitability for the C-suite by making sensible judgments and engaging with other company executives as peers.

- Is our CISO capable of succinctly communicating risks—including current threats, probability, and impacts—in language that corporate leaders and the board of directors can comprehend, support, and act on?

CISOs must have an intuitive understanding of which facts and concerns should be brought to the board's attention and the ability to communicate them effectively. When cyber risks are explained in financial terms, the board is more likely to comprehend their implications and approve investment requests, no longer seeing it as just a cost.

- Is our CISO capable of advancing the enterprise's cybersecurity risk management to a more precise level?

The CISO is accountable for developing and executing a cyber-risk plan that safeguards critical information assets via the use of cost-effective, risk-based measures. The critical first step in managing cyber risk—or any operational risk—is to define the risk.

In understanding the key goals of your CISO, how can you provide them the much-needed support for them to succeed in their role? Simple: sit down, grab a cup of coffee, and enjoy a frank discussion. Your conversations with your CISO should focus on the burning questions about the business, security challenges, and thoughts about cybersecurity policy.

C-suite executives and board members must support and empower the CISO—this is particularly critical. CISOs have the ability to create change, which is crucial for the success and survival of businesses today. Boards of directors and C-suite executives must ensure that they pick and then support the CISO in their increasingly crucial position inside the organization. Additionally, boards and C-suite executives must reinforce the message that all leaders across the organization are responsible for cybersecurity and must collaborate with the CISO and be responsive and embrace their own specific cybersecurity responsibilities. It is the only way to ensure the business's continued success.

## Speaking the board's language

When the board of directors fails to interact with critical risks, including cyber risk, to the same extent they engage with rewards and opportunities, this is referred to as **board risk blindness**. This certainly can be avoided if the CISO employs a proper communication strategy.

An aware and involved CEO and board of directors seek updates on cyber risk, do not treat it as a simple and small IT problem, and entrust their CISO with a cyber-risk management strategy and roadmap. The CEO and the board need to feel confident that, in the event of a breach, appropriate measures are part of the business continuity plan and disaster response plan to minimize the damage to consumers in particular and the firm in general.

Although cybersecurity has been increasingly declared a high-priority issue for many board directors (*72 percent of the AICD survey respondents indicate it as so*), it is interesting to note that most boards indicate they still have yet to

receive regular reporting on key cyber issues, not to mention internal cyber training and testing. Only 36 percent of boards receive regular reports, which means that staff within an organization might not be getting the appropriate message about the importance of cyber vigilance.

Also, in the same survey (see *Figure 10.1*), only one in five directors receive regular updates on the cyber risk that comes from their supply chain relationships, which should be another important risk consideration for the business.

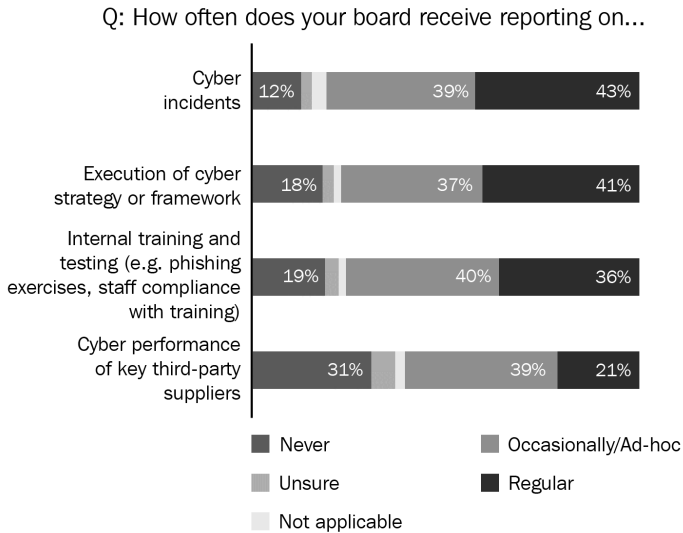


Figure 10.1 – AICD survey findings of board-reporting cyber-risk areas

In ensuring the right message is conveyed to the board, people presenting to the board need to understand how the board thinks before talking to them.

Most people are unfamiliar with the environment of the boardroom and what goes on behind the scenes. To understand how the board thinks, it is important to understand *who* the board members are.

Here are a few things to know when engaging with the board:

- The board is expected to have read the board pack sent to them ahead of the presentation.
- Generally, 10 to 20 minutes is taken for each presentation item, followed by a period for questions.

- The chair always provides adequate time for board members to ask questions. *It is the responsibility of the board members to ask questions and to have done their own due diligence.*

Michelle Beveridge, chair and board director of several committees across finance, education, and government, shares her preference: *“Personally, I like to receive the recommendations right at the beginning of a board paper. That way I know what I am making a decision on, where to focus, and what other research I might need to do. This format makes so much of a difference!*

*“Most board packs are 200+ pages, and I would like to know what I should be looking out for to make a decision in the best interests of the relevant stakeholders. A good board paper will tell me this upfront.”*

- The material presented to the board must be relatively easy to understand for everyone, since board members usually have different backgrounds. A total lack of questions following a presentation is often due to three reasons: low strategic materiality of the discussed item, a lack of interest, or a lack of understanding. If a board does not understand what was presented, then the presenter needs to re-evaluate their content and approach.
- Board members understand business risks, the language of revenues and margins, risk mitigation, compliance requirements, and legal ramifications. Presentations should be given in those contexts. Keep technical jargon out of it.
- Every presentation must include a recommendation to the board, from which the board members must clearly understand what they are asked to do as decision makers (be it approval or simply taking note), what you need from them in terms of resources, what the timeline is for implementation, and what risks/issues the company will face (if applicable).

Magda recalls a few positive experiences; one in particular with the board of a financial institution. The feedback was that the presentation was succinct, clear, and within the assigned time. Another experience was very different, but equally positive. Magda gave a presentation to the board of a publicly traded multinational oil and gas company. She was extremely surprised by the interest from the board members. Some mentioned *exceptional insights*. She had studied the business's priorities and initiatives and showed how current and future cybersecurity initiatives work to mitigate the associated risk, and quantified the potential residual risk. She also described the gaps and the

required investment. The conversation went on for an hour and a half, as a few board members canceled other meetings to ask further questions. It was a unique experience, and a very enjoyable one for all parties. The presentation turned into a discussion with the board.

## What *not* to do in the boardroom

As a result of the increase in global rules and legislation, cyber-risk management increasingly is part of the board's agenda.

Cybersecurity is complex. There is a plethora of expertise, guidelines, standards, requirements, and vulnerabilities, among other matters. However, there is a growing emphasis on avoiding extra complexity and ensuring that cyber-risk management contributes to the enhancement of current company structures by acting as an integrated part of established processes, rather than in opposition to them. This requires a common understanding of the impact of cyber risk on company goals and good communication between business executives, the CISO, and the board.

The CISO's role is to make sure the board understands the threats cyber poses to the business and should have a place on almost every board agenda. A key question for CISOs to ask themselves before every board presentation is: *Are we overcomplicating things?*

In several of Shaman's fireside chats with board chairpersons and directors, the highlighted their common frustration with technical experts getting too technical in their presentations: *"If you present something and the board does not understand what you are saying, they leave the meeting thinking you're too incompetent to explain things."* Keep things simple.

Magda recalls one board member saying every cybersecurity expert speaks their own language, and that they—board directors—don't understand it.

*Are we selling our message using fear?*

Yes, cybersecurity is a risk. However, it is not the only risk that matters to the board. Delivering your message using fear might be useful only so often, and it can also backfire if the board becomes desensitized. Show how cyber risk affects investors and organizational risk in the bigger scheme of things.

*Are we being the roadblock?*

The role of cybersecurity is to solve the problem of cyberthreats and cyber risks. Decisions around risk avoidance should be made by the business owner, not the CISO. The CISO is there to help the board understand the risks and provide it with options that either mitigate, reduce, or transfer that risk.

## **Reporting to the board (an add-on for CISOs and a reference for CEOs)**

Reporting to the board of directors about cyber risk should be done in plain English so that the board can quickly get a sense of what is happening within the organization. A cyber-reporting structure aligned with the business strategic initiatives or scorecard generated by the CISO may assist the board of directors in assessing existing cyber risks and tracking progress in cybersecurity.

A multi-year strategic plan, a current-year business strategy, resources, a cyber-training program, and other relevant information regarding the company's cyber operations should all be made available to the board for a comprehensive picture of the company's cyber activities, again in alignment with the strategic business initiatives.

According to a recent poll done by the Ponemon Institute, just 9 percent of security teams believe they are extremely successful in conveying security threats to the board of directors and other C-suite executives.

A CISO may feel that communicating the relevance of an organization's cyber-risk program to an audience that sees cybersecurity as yet another tough-to-comprehend technical issue is impossible. Consequently, many security-related decisions are made by the board and the C-suite based on gut instinct and inadequate information. Or worse, decisions are not made and those organizations remains particularly vulnerable to cyber threats.

Today's CISOs must define metrics and quantify cyber risks to make more informed decisions. These efforts assist in the prioritization of the most significant cyberthreats and the alignment of capital allocation requirements with those risks. They assist in ensuring that cyber funds are directed to the areas that will most affect the firm. It is this language that is understood by most boards and C-level executives.

At the end of the day, the amount of cyber risk must be compatible with the organization’s risk appetite. Specifically, boards of directors want to know whether management is focusing on the appropriate cyber risks, how management manages those risks, and whether the efforts are sufficient. This begins with gaining an overview of the company’s cyber-risk management program as well as its cyber-risk tolerance.

Magda uses the report template in Figure 10.2 after carefully studying the financial reports of a company.

Current state: Where are we now?		Target state: Where do we want to be?			Strategy and roadmap: How do we get there?		
Scenario / Current Cyber Risks	Strategic initiatives	Mitigation Status	Qualitative Risk	Quantitative Losses	Budget Required	Risk Appetite	Target Risk
Data Breach and Privacy Violations Non-compliance with regulation (PDPA, GDPR)	M&A with Company A	Not ready	High	20 000 000.00	500.00	Fail	Medium
Business Interruption due to Technological Failure or Cyber Attack	Deployment of smart robots for cost reduction in factory A	Implementation ongoing	High	5 000 000.00	250.00	Pass	Medium
Supply Chain Cyber Risk	New strategic partnership with Company B	Mature	High	12 000 000.00	0	Pass	Low

Figure 10.2 – Example of reporting

Different scenarios need to be explained and then tied back to the strategic business initiatives.

## Boards and mergers and acquisitions

Cyber risk considerations for mergers and acquisitions are increasingly important. In fact, investing in a company with low cyber maturity might result in massive financial losses and incorrect valuations, and eventually lead to reputational damage in the event of a cyberattack or data breach.

At various stages of a **merger and acquisition (M&A)**, various risks exist—from information leakage prior to public disclosure, from the risk of insider threats, from disgruntled employees stealing valuable intellectual property fearing changes and dismissal, from the unadjusted risk as two organizations merge, potentially resulting in contagion between the two entities or conflicting approaches being exploited. The timing of M&A transactions is always a delicate balance between speed and risk—the need to consummate the

transaction quickly before values rise and to exploit new business opportunities (to unlock value), and the danger of not doing enough due diligence.

During the course of an M&A, cyber risk will change at different stages, each stage necessitating careful consideration. In addition, unforeseen changes in the risk profile, uneven trust levels, and contradictory approaches to policy and compliance, for example, SOX, PCI DSS, FCA DSS, ISO 27001, and the EU's GDPR (which replaced the Data Protection Act), among other things, might all have an influence.

The board and the CEO should consider whether elements of the security program may be taken into account during the negotiation phase, and bring the CISO on board as appropriate.

The following section focuses on the questions to ask yourself—the CEO—and the board to build your organization's cyber resilience.

## **Asking the board the right questions and setting up your CISO for success**

It is the responsibility of the CEO and the board to discuss the following questions in to achieve cyber resilience:

- Do we have a collaborative approach to emerging cyber-risk issues? Consider whether or not the top executives in charge of developing risk management strategies and resilience are working together with the CISO toward a single objective of achieving success.
- How responsive and adaptable are we in the face of cyber threats and our management of them? Cyber risk might still be considered an IT problem, or lack integration with enterprise risk management processes, or just be seen as a compliance exercise (for example, achieving an ISO 27001:2013 certification). However, this is not enough to enable and build effective cyber resilience. Senior management should take a close look at cyber risk and collaborate to identify, quantify, treat, and transfer that cyber risk. They also should be aware of the proportion of cyber risk the organization handles as opposed to third parties, potential partners, or during an M&A.



- Are we forecasting and anticipating cyber risks as they emerge? The CEO and the CISO should support the board to look at future changes and their implications—for example, emerging technologies such as quantum computing, which has the very real potential of disrupting traditional security controls. This is very important, as it might require years of planning and significant budget resources.
- Do we have the right metrics in place? As firms confront an increasing variety of cyber risks that are complex and interlinked with other risks, many of the classic methods of presenting and measuring cyber risk may no longer be appropriate or effective. Boards of directors and C-suite executives should evaluate relevant indicators to inform and progress their business's decision-making.

In the end, businesses that flourish in this age of growing complexity will be those that distinguish themselves in their risk management, and the way in which they employ risk capital to remove the risk from innovation and growth as much as possible.

How the board of directors and CEO address these questions will enable the CISO to develop appropriate cybersecurity strategies, build business continuity plans, and effectuate disaster recover procedures. It is all an essential part of the success of a CISO and a firm's cyber resilience.

## Summary

Managing cyber risk is difficult for almost every firm and its board of directors. Cybersecurity is a sophisticated technological field in which new threats emerge almost weekly. Despite the fact that most board members are not cyber professionals, boards of directors have a duty to recognize and monitor this risk. This requires active participation with leadership and access to experts, as well as comprehensive information and reporting from an organization's upper management.

Specifically, boards of directors want to know whether management is focusing on the appropriate cyber risks, how management manages those risks, and whether the efforts are sufficient. This begins with gaining an overview of a company's cyber-risk management program as well as its cyber-risk tolerance.

Furthermore, some boards have determined that cybersecurity is a risk that requires the oversight of the whole board, rather than a specific committee. Whatever the case, if supervision is delegated to a board committee, it is critical the whole board receives frequent and complete reports.

It remains beneficial to review the board's means of oversight on a regular basis to ensure they continue to function properly. Among the factors to evaluate are whether the existing structure engages the appropriate board members and whether they have sufficient time to handle the issue in question. It's also critical to ensure your board has access to the right subject matter experts it needs. Many boards of directors look for candidates with experience in cybersecurity. This may be beneficial but has some cons as well, particularly when the expertise is limited. The presence of a cyber specialist on the board may cause other directors to be less likely to express their thoughts on the subject.

The fact that this topic is so wide-ranging might make it difficult to devise a plan for approaching board presentations, which can be a challenge. However, it remains a critical part of building a resilient business nowadays with increasing technological dependency and complex ecosystems.

By understanding the importance of cyber resilience and implementing the necessary measures, your business can protect itself from these threats. The final chapter will discuss cyber culture and the importance of businesses bringing all the previous recommendations together to build the right business culture.



## **The Recipe for Building a Strong Security Culture— Bringing It All Together**

Cyber resilience prepares an organization to maintain and even accelerate business growth by anticipating, reacting to, and recovering from cyberattacks. A cyber-resilient organization can adapt to both known and unknown crises, dangers, adversities, and obstacles. The ultimate purpose of cyber resiliency is to help an organization thrive in the face of adversity (be it a crisis, pandemic, financial volatility, and so on).

The previous chapters have provided many profound insights into the roles and responsibilities of the C-suite regarding cybersecurity. Collaboration will produce a more powerful cyber-resilient outcome by incorporating the different lenses and perspectives of the CxOs. The accelerated transformation from conventional channels to digital, both during and after the COVID-19 pandemic, has been one of the most significant changes imposed upon businesses. Of the risks that now take center stage, the geopolitical, business continuity, reputation, trust, competitive, regulatory, insurance, and legal impacts are only some of the concerns related to those emerging risks.

This final chapter addresses a key and important core of any flourishing organization—the culture necessary to build a cyber-resilient business. For a business to have the best chance of being cyber resilient, we must tackle the security culture across all levels of employees and empower the CISO in their responsibilities by making sure they have a seat at the table.

In the chapter, we will cover the following topics:

- Building a robust security culture
- Bringing it all together
- CISO add-on – building a cybersecurity culture
- The different building blocks
- Varying your training
- Cloud-sharing responsibility
- A hands-on cyber-awareness program
- What kind of community are you building?
- Questions to ask yourself about building a culture

## **Building a robust security culture**

A strong security culture is essential for a comprehensive cybersecurity program as well as for a cyber-resilient organization.

Employees who are security-aware become your first line of defense as they share the same values, philosophy, and behavioral approach to security established by the business. A strong security culture implies your employees are more scrupulous in adhering to security standards, are more aware of security concerns, and take responsibility for security concerns.

Safety and security, whether it is digital or physical, is a shared duty, and there are significant advantages gained from reducing cyber risks when security best practices are integrated into employees' everyday routines. All hands must be on deck, beginning at the very top.

An organization's culture is informed from the top. The CEO and board of directors establish the expectations. For there to be an effective security culture, your organization's leadership is involved in and dedicated to security, and they consciously develop a security culture appropriate for the organization.

If security has not been a priority in the organization, it is common for the CEO to need a period of adjustment before they become fully committed. As you move into this position, your security staff may begin by holding frequent meetings with the CEO, an senior management, in which they can explain why security is important to the firm. Education will be needed for all in the C-Suite on the efficiency of the company's present security policies and technologies in mitigating possible threats.

Only then can a resilient security culture be built.

## Bringing it all together

From the first chapter of this handbook, we have noted that cybersecurity has risen to prominence as a key **environmental, social, and governance (ESG)** issue. If businesses do not adequately defend their information assets, they risk losing their reputational or financial status when (not if) a cyber incident occurs. Cybersecurity is no longer a technical issue siloed in the IT department; nor is it a passing fad, but rather an issue that will continue to grow over time. Cyber risk management requires a comprehensive risk strategy that considers people, processes, and technology while adopting mitigation measures. It must encompass everyone in the organization, and everyone must work in partnership to ensure resiliency.

With that in mind, let's recap each of your CxOs' roles and provide a holistic picture.

Cyber risk is a business risk and CISOs today are required to comprehend their organization's operations from a business standpoint and must be able to evaluate all business initiatives (in some cases, even customer engagement). The CEO must serve as the cybersecurity leader and role model for the business. Together they must foster a cyber-safe, proactive, and accountable culture in which every team member knows their role in mitigating cyber risk to the firm.

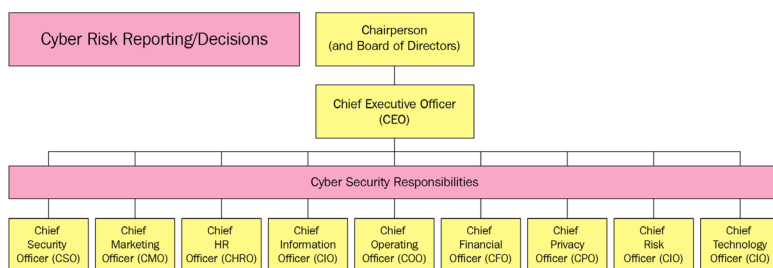


Figure 11.1 – Organigramme

Figure 11.1 showcases an optimal corporate organizational governance structure. However, this does not mean that companies should follow this exactly. The CISO or the CSO is the executive in charge of information security and, as businesses depend on more and more on information, they must have a prominent role in decision-making discussions. The CISO tackles a variety of functional issues on a daily basis, particularly in today's security landscape, overlaid with the pivotal changes taking place in business. As part of their main tasks, the CISO balances technical and management obligations. The CISO must attempt to link its security strategy with the organization's purpose to analyze the organization's objectives and risk tolerance effectively.

The regulatory landscape has also rapidly evolved globally as governments react to new cyber threats and incidents. Following the implementation of EU's GDPR, other governments have started to follow suit, which implies that corporate requirements for information security compliance will continue to get increasingly complex.

As more software migrate from the data center to the cloud, the CISO is responsible for enhancing security, identity, and access management across public and private environments. Simultaneously, it is necessary to protect the security of older on-premises systems.

With an average tenure of two to three years for security staff, a CISO must be an engaging, attentive leader who reacts to the company's needs and promotes career growth and development to reduce turnover. The CISO must also routinely analyze data assets to ensure they are manageable and minimize the quantity of data needed to be safeguarded to prevent the company from significant slow down in the event of a cyber incident.

Perhaps most importantly, the CISO must confront the new reality: data breaches can and will occur. By expanding the CISO's focus on preventative controls to encompass more strategic planning, the CISO can address potential risks posed by ongoing digital transformation as well the growing dependencies on their third-party suppliers.

The CISO is under tremendous pressure to manage the risks associated with an organization's digital transition in the face of an increasingly hostile threat environment. One element contributing to the CISO's challenges is that often they are the rookie amid a group of experienced executives, with job descriptions that have been developed, refined, and traditionalized over many decades. The CISO's role, instead, is not only new, but evolving continuously. Since the CISO post was adopted just a few years ago, the current generation of CISOs is among the first to carry the title in their organizations. It is up to this generation of security pioneers to define the CISO's duties and scope.

One of the most critical components of the CISO's responsibility, in our opinion, is turning other executives into eager collaborators in establishing a cyber-resilient company.

## **CISO add-on—building a cybersecurity culture**

A strong leader does not need to accept the “cultural status quo” and can recruit a group of champions or advocates within the company to drive cyber-related results. A strong leader creates a cybersecurity culture where employees are empowered and led with purpose. Alexandra Mercz, chief of staff at GoToFinancials, a financial services solutions provider, shared that in one of her earlier roles before the pandemic, she frequently did her “office rounds,” which meant personally visiting key stakeholders and teams for a quick catch-up at the office.

During one of these office rounds, she stopped by the desk of a very senior and seasoned cyber-technical program manager tasked with implementing a critical solution for the business. As they discussed the deliverables, she changed the topic and asked him, “*Do you know why you do what you do?*” He looked at her blankly, as if he did not understand the question. She repeated, “*What is the purpose of your deliverables? WHY are you doing what you are doing?*”



The person looked across the room as he sank into his thoughts. Finally, he said, “*Because business said I need to deliver this solution.*” While Alexandra was not surprised by this answer, he seemed unhappy saying these words.

She explained to him that his deliverable was so critical to the business that it would not be able to continue operations if it was not in place by the agreed time. The expression on his face completely changed after hearing this. It was almost tangible to see how the full context and impact gave this person purpose to continue his work and, most likely, even reduce the organization’s cyber-risk exposure.

From an organizational perspective, focusing on the strategic alignment to a business and its key risks can be a practical framework that helps shape a culture. It’s not enough to develop products and processes; the people doing the work need to understand how and why it is critical to the business. Leadership role models with their own security stories convey a strong message. Imagine if the CEO or other C-executives echoed security values in their vision and mission. Imagine if they share personal stories of how they practice good security behaviors, and why it is essential to them. Imagine if there is a lot of attention and focus paid to security from the highest levels of leadership themselves. That *will* have an impact throughout the organization.

In time, there will be a shift in mentality when security had been baked into the organization’s culture. The staff will start to understand that security is part of their story and the work they do. As we seek to bring everyone along with us on this journey, there are ways we can be strategic in building culture.

Sometimes, it does not have to start at the top. Middle management, and even employees on the ground, can play an invaluable role in influencing a culture.

Do not underestimate the importance middle management plays in driving a healthy security culture as they are the ones with direct and consistent interaction with staff. It is important for management to lead by example themselves and have conscientious security-aware behaviors. If managers do something as simple as ensure their computer is always locked before stepping away, it is easier and just a matter of time before the rest start to follow.

Likewise, it takes time and initiative to educate teams on proper workflows and potential security risks to a company. Management can be an invaluable resource to strengthen your human defense layer.

In the next section, Muhamed Noordin Yusuff, the global CISO at Circles. life, a digital telecom, shares his approach to building a company-wide healthy security culture.

## The different building blocks

*“You clicked on the phishing link!”* How many times have we come across someone who clicked on phishing links from unknown recipients? Even though training after training was conducted, not to mention the occasional phishing exercises conducted company-wide or with targeted groups, someone in the company is bound to say, *“Oops! I accidentally clicked on that unknown link. Sorry.”*

Is security-awareness training an avenue to enhance security culture? It definitely is. As a CISO in the digital telco space, Noordin shares that security-awareness training, and conducting phishing exercises have become part of their **business as usual (BAU)** process. Even though it is treated as a de facto, the need to continually make the training more enticing is important to maintain user engagement.

Building a company-wide healthy security culture is an uphill battle. It is also pretty much dependent on the nature of the business you are involved in. Building and maintaining a security-first culture in a regulated industry such as a financial institution is different from building it in a startup environment.

In an information security space, we often hear about the concept of **people**, **process**, and **technology**. While we can implement processes and justify the budget for new security solutions, managing the **people** aspect is usually the toughest, regardless of the industry. This is especially true when it is human nature to find the path of least resistance if an inconvenience (that is, increased processes to address security) is presented to them. Though it is often mentioned that **people** are the weakest link, they can also be our greatest ally if approached correctly.

In building a security culture, it is only right that we start off with the people in a company. Often, an organizational culture is taken for granted, something that is already there that people passively adopt, and not something we actively drive. However, culture shapes everything we do.

In implementing any new changes, it is not only about getting the buy-in from the top but also support from middle management and below. If the CISO has just joined the company, stakeholder management is key. You need to socialize with the stakeholders at every level in the company and understand the concerns they have around security, whether they have experienced past security incidents, and how you can help them enable their business/function to stay cyber safe. Balancing security with agility is typically what all stakeholders aim for; their goal is to proceed with their day-to-day business activities and not worry about their systems getting hacked or data being stolen. They are concerned especially about security becoming an obstacle to the business that could result in delays in rolling out new products to market.

The CISO also must have regular engagement with C-suite executives and understand how they can help the executive teams. “When I came on board as a CISO,” Noordin recalled, “I spoke to the CFO and was surprised at the number of ideas he shared about cybersecurity. I found out that he was part of the risk management committee in his previous role, and his experience has definitely given me some thoughts about my cybersecurity program. Though cybersecurity is supposed to be effective when pushed from top down, it sometimes gets diluted in the middle. This is where the support from middle management is important for a CISO to push forward the cybersecurity program.”

Noordin explained further, “I am a strong believer in knowledge sharing no matter which industry you are in, whether it’s government, financial institutions, multinational corporations, or startups. Doing so tactfully and within the comfort of four walls, knowledge-sharing among CISOs in different industries helps to generate a flow of ideas and opinions that can be experimented with in their respective companies. There could be hidden gems just waiting to be shared among the CISOs in the community. Having attended numerous closed-door CISO events, I have learned a great deal from my counterparts and implemented ideas they shared in the various organizations I’ve worked in. As a CISO, you don’t stop learning. There will always be new ideas that you can try, processes you can develop, or new technology solutions to evaluate and implement.

“CISOs are in this battle together—the only way to rise above the common threats is to support each other and not judge, especially when we hear of data breaches affecting organizations. CISOs should not judge or bring down fellow CISOs who encountered cyberattacks or data breaches as we are not

in that CISO position and do not know the context of the organization's dynamics. Instead, we should give support or render advice where possible.”

Those are words for any CISO to live by.

In the next section, we've put together some tips and different approaches we have seen work well in building a healthy security culture across different organizations.

## Varying your training

As seen in Noordin's approach, building a culture is not something that just happens. It does not just grow organically. It requires investment, commitment, and nurturing. The end goal is a sustainable security culture that is transformative.

One way to do this is to vary your training methods to engage and help staff retain a security mindset. Before implementing any change, it is always important to ask the right questions and understand where your team is and how they behave. Leverage your CHRO and HR team to shape the delivery of your training. It is essential to tailor the training, from its content to its approach, in alignment with the nature of your staff's roles, from the department they are in to the level of access they have, their grasp of security knowledge, and the tools they use. Effective training is not always one-size-fits-all.

Stories of how human error has resulted in a company's downfall can make it easier for staff to remember the lessons. Making it real and personal with the message that no one is impervious to cyberthreats can help encourage staff to be more diligent in adhering to security policies. The tone should not be one of *naming and shaming* but rather objective and educational.

For a message to be constructive, it must be relevant. A blanket training program will not work. For instance, staff who do not have access to your databases will not need database security training.

Some companies look to reinvent the wheel by searching for grand and new training tools or be early adopters of only fresh and innovative approaches; however, there is also research on the effectiveness of employee training (as part of the onboarding process) where they simply sit through a simple training video on security and encounter fewer issues with security as they go about their job.

For a message to be effective, it needs to be simple. Start with plain language so everyone understands the role they need to play. Make your security policy easy to read, a simple one-pager, and complement it with short videos or podcasts. The message can be absorbed across all levels if the message is simple to understand and relatable, whether they are lobby staff, client sales, delivering an audit, or on the tech support team.

Magda spoke about the topic in her TEDx talk, “Why You May Be Alienated by Cybersecurity Topics.” She notes that the assumption that everyone from laymen to experts would be able to understand cybersecurity in the same way does not hold. She explains that using simple words and starting from the very basic concepts without security acronyms is a key success factor.

The next step is to keep the momentum going so the security message is at the forefront of people’s minds.

Gamification has been a popular choice for departments, as it leverages the competitive nature of different teams. Successful teams are recognized and rewarded by leadership for having the best security-aware champions. With the increasing modernization of simulation and artificial intelligence-supported technologies used in scenario-based testing, board games have been proven to be extremely helpful. Wargaming is an old concept, yet U.S. Defense professionals have found that it aids in sharpening the decision-making processes and their tactical and strategic acumen. The value of wargames demonstrates to security professionals that different strategies could affect the company’s response to a cyberincident and influence planning factors as they see how people react in the face of crisis and immense pressure.

Allow time to conduct role-playing games, as they put your staff in a position to imagine the different scenarios around the key cyber risks relevant to the business and give them the ability to work out their approach. Such an interactive framework allows for on-the-job learning and a better understanding of the practical ways to abide by an organization’s security policy or carry out an incident response. This is all part of building the business continuity plan.

Training should not be a one-time event but as frequently as required, a continuous effort for your staff’s business and learning curve maturity. For example, positive feedback and improved results were seen in a few startups by running a phishing writing workshop, where they challenged their staff to write the most believable and innovative phishing email. Continual awareness training and frequent drills (for example, every quarter or six months) can help staff refresh their knowledge and retain them.

As companies become more reliant on cloud-based technologies, this opens up businesses to additional cyber threats. In the next section, we take address this and how a security culture can be shaped by the cloud.

## Cloud-sharing responsibility

Cloud technology is a way of storing and accessing data and applications over the internet instead of on your computer's hard drive. There are three types of cloud computing: **infrastructure as a service (IaaS)**, **platform as a service (PaaS)**, and **software as a service (SaaS)**. IaaS is where you rent storage, servers, and networking from a cloud provider. PaaS is where you use a cloud provider to run your applications, so you don't have to worry about managing the underlying infrastructure. SaaS is where you access to the whole application without much customization available.

There are a number of reasons why cloud technology is being adopted at an increasing rate. One of the primary reasons is the cost savings achieved by using cloud services. A consumption-based model can result in considerable cost savings for an organization.

Another reason for the growing adoption of cloud technology is the flexibility and scalability it offers. With cloud services, businesses can quickly scale up or down their usage as needed, without having to make expensive investments in new hardware or software. This flexibility is particularly valuable for businesses that experience seasonal peaks in demand or sudden spikes in traffic.

Finally, cloud technology is becoming increasingly popular due to its many security advantages.

Nevertheless, there are potential challenges with cloud adoption, though these can vary depending on the specific organization. One challenge is around the concept of shared responsibility. In a traditional on-premises environment, an organization is responsible for securing and managing the infrastructure. However, in a cloud environment, that responsibility is shared between the organization and the cloud provider. The organization is still responsible for securing its data and applications, but it may need to work with the cloud provider to ensure it is done so effectively.

Cloud storage can be secure, but it depends on how the service is implemented and how willing both the provider and the customer are to take security measures. The CISO, in collaboration with other appropriate CxOs, must evaluate the service and make the risk analysis on behalf of the business.

Cloud awareness training is an important part of security, but it's not the only part. It's essential that everyone who has access to the cloud is aware of the dangers and takes responsibility for their own security. That means being careful about what files you store in the cloud, using strong passwords with multi-factor authentication, and being alert to any suspicious activity.

Everyone who uses the cloud needs to be responsible for their own security, guided by a strong security team. Training is a good start, but it's not enough. Security awareness requires a cultural shift. Blaming employees for cyber incidents can foster a culture of secrecy and prevent employees from reporting potential security issues. An overly blame-based culture can also create an environment in which people are less likely to take risks or experiment with new technologies, hampering innovation and organizational growth. Finally, a blame-based culture can lead to decreased employee morale and job satisfaction. Finding the right balance is critical to achieve a great culture across all corporate ladders.

## **A hands-on cyber-awareness program**

Both Shamane and Magda have run security programs for various organizations. In Magda's approach, she provides holistic hands-on training (*Figure 11.2*). The training encompasses several activities and is based not only on consistency but the *why* and the *how*.

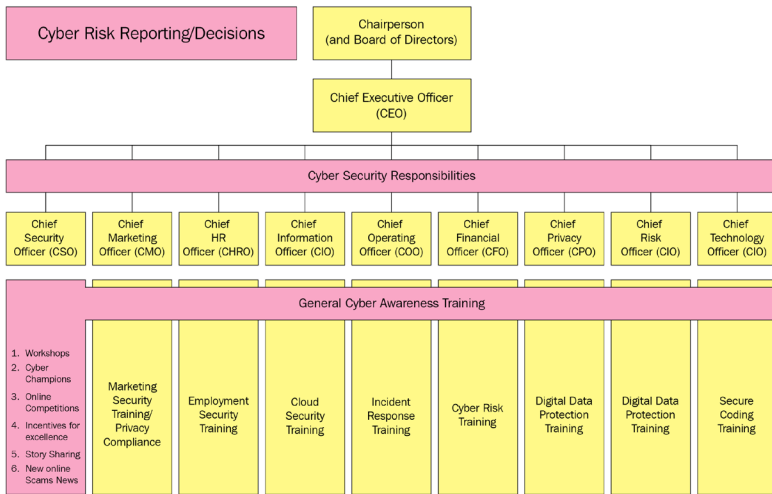


Figure 11.2 – Awareness program components

The assumption that everyone will apply cyber awareness does not make sense if the security awareness training they have to complete is irrelevant to their role. Awareness training activities that align with each function help employees to understand their cybersecurity role and apply best practices in their daily tasks.

As part of her approach, Magda carries out dedicated secure coding sessions while conducting cyber-awareness training. She also uses online quizzes with prizes such as lunch vouchers or Amazon gift cards to encourage attendance. Her sessions have had as many as 300 attendees for a nonmandatory cyber-awareness update for a major international company. Magda makes every attempt to personalize the trainings. People will hear stories rather than security acronyms.

A cybersecurity program does not need to be boring and useless. Storytelling is a very effective training tool. It just needs to be relevant and engaging. As a keynote speaker at global conferences and an invited guest speaker for special executive awareness sessions, Shamane has received some of the best compliments from board directors, chairs, and even law firm partners: “If only security leaders could tell us stories like this! We are tired of just hearing bad news; we want to hear riveting stories that capture us. And it’s refreshing when complex issues are conveyed in such a simple manner.”



## What kind of community are you building?

Think of your company as a community you are building. A community provides connections. It shifts the individualistic lens to a group lens. Collaboration happens when a group is socially responsible and actively contributing to the community. Having the right team is key. With a mix of security advocates (people who have bought into the values of security), the security-aware (who might not be as passionate but still realize its essentiality), and the sponsors (management who are tasked with shaping the security direction), you have an integral group in the community who you can work with.

From mentorship to weekly/monthly gatherings and events that focus on the latest security issues, allowing for open conversations and exchanging knowledge sustains your security community. Active participation is what helps a community to grow and a business flourish.

In a focus group Shamane did with CEOs, she found that they are aware of the critical role CEOs play in shaping a company's culture, and they all had a lot to say about the undeniable importance of a healthy company culture. One key thing they stressed was that the success of building any healthy security culture depends on an organization's existing culture. To achieve, a well-performing team requires employee commitment, backed by the trust they have in their leaders. This creates a safe space for innovation but also honesty in sharing ideas and viewpoints.

If the existing culture is one where people are afraid to make mistakes, then owning up to them would be impossible. There will be a lack of transparency and accountability and this means there is a toxic environment where the management is quick to point fingers. This type of culture is not conducive to a responsible security culture. This is where leadership has to be committed to driving real change.

There has been much talk about humans being the weakest link, yet the harshest punishments do not help resolve the issue. Recent stories of companies suing employees who fell for phishing scams or terminating their employment when they failed phishing simulation tests only create an environment of fear. Staff will be less likely to come forward if something goes wrong, which puts a business at even more risk. The most successful organizations are the ones where the people are treated as an asset and not a liability.

When there's trust, there is more comfort in taking ownership, as staff know they will be supported, instead of management coming down on them like a ton of bricks. The CISO also needs to be more intentional in considering the different departments' journeys and priorities to derive a solution, instead of saying no to everything. Instead of being that obstacle, it serves security teams well to be more accepting and enable people to have the right tools to do their job more effectively.

Be deliberate in building a strong security culture. Complement education with the right level of controls to change the perception of security as everyone's responsibility. Having a secure development life cycle is also a good foundation, as the business builds in security and performs security-testing activities and processes for each software product or system release.

Management should encourage positive behavior and recognize staff publicly who helped detect incidents. When someone completes a security awareness program or progresses to an advanced level, a reward (for example, gift cards or electronic gadgets) will aid as a motivation for the rest to follow. This public promotion and celebration of success sets up a positive culture throughout the company. Not to mention security issues are discovered earlier and the security team is able to respond to threats faster.

Another way to reward is to provide career advancement and a career path into security, encouraging staff to grow into a dedicated security role. This is one powerful way to send a strong message to the entire company.

Finally, everyone is always more receptive to a process that is enjoyable, engaging, and fun. These are the final ingredients in a security culture recipe that is sustainable. At the end of the day, when people are involved, they then remember things that connect them—to their work, to their community, to the business. Be it a security quiz or gameshow event, or a movie and pizza night about cybercriminals, lessons are more memorable amid laughter and enjoyment.

So how is your security culture? The next section poses a few helpful questions that will explore your options in building a resilient security culture.

## **Questions to ask yourself about building a culture**

- As a leader, what are some creative ways I can use to set an example in building a healthy security culture?

- Who are the other allies I can collaborate with to build a culture together? What role can they play?
- What ideas do our C-executives have about building a security-aware culture that we can tap into?
- How can we get support from middle management in driving our cybersecurity program?
- How can we leverage the current organizational culture to build and support a healthy cybersecurity culture?

Try out some of these questions and see whether they lead to a different approach and outcome!

## Summary

The key to corporate resilience is to develop crisis “shock absorbers” that enable businesses to continue operations, expand customer outreach, and accelerate company change during times of crisis.

Cyber resilience is about recognizing security risks, implementing adequate security controls, and ensuring cyber-incident responses are rapid and efficient to mitigate long-term consequences. Cyber risk must be treated with the same seriousness as other risks, such as natural catastrophes or severe diseases. The board of directors and CEO must recognize and prioritize cyber risks on par with other business risks.

Building a strong cyber culture needs a strong organizational commitment. Instead of just adhering to regulations and standards, a principles-based approach will greatly aid in staff comprehension and compliance. The CISO is an essential resource and leader in establishing and implementing the firm’s best cybersecurity plan—but they cannot do it alone. It requires commitment from the CEO and board of directors, all CxOs, and everyone in the organization.

With a stronger emphasis on business development, communication, and mentorship, today’s security leaders can help define the future of the CISO profession. By differentiating their responsibilities, the CISO can establish themselves as the de facto cybersecurity leader upon whom organizations will rely to align their security controls and practices with their goals for business growth, innovation, and success.

# Index

## A

ABN AMRO Clearing Bank 61

artificial intelligence (AI) 3, 64

## B

blockchain 3

board of directors

about 158-160

agenda 170, 171

CISO, setting up  
successfully 173, 174

directors, speaking 167-170

merger and acquisition  
(M&A) 172, 173

questions, asking 173, 174

reporting 171, 172

structure 160, 161

board risk blindness 167

board's interests, in cybersecurity

about 162

appropriate investment 164

business ownership 163

foresight, maintaining 165

industry resilience 165

rightly equipped 164, 165

risk transfer options 165

business

preparing, for cyberattacks 20, 21

business continuity

considerations, for  
assessment 125-127

business continuity and  
disaster recovery 123

Business Continuity Plan (BCP)

about 20, 21, 120, 124

best practices 128

disaster recovery planning 127

methodology 124

Business Continuity Plan (BCP),  
management

about 122

don'ts 122

dos 122

Business Email

Compromise (BEC) 29

Business Impact

Assessment (BIA) 125

business risk 8

business risk custodian 45

## C

Capability Maturity Model

Integration (CMMI) 87

- Certified Information Security Manager (CISM) 105
- Certified Information Systems Security Professional (CISSP) 105
- CFO, about cyber risks
  - communicating with 37
  - data breach costs 39
  - economic costs 39
  - innovative approach 40
- CFO roles, in building cyber resilience
  - about 34
  - cyber insurance, purchasing 36
  - cyber-risk quantification, supporting 35, 36
  - cybersecurity budgets, benchmarking 34
  - cybersecurity spending, defining 35
  - third-party risks, assessing 37
- CFO's cybersecurity supporting, cyber resilience 28-30
- Chief Digital Officer (CDO)
  - about 133
  - versus Chief Technology Officer (CTO) 133, 134
- Chief Executive (CE) 3, 12
- Chief Executive Officer (CEO)
  - about 3, 117, 131
  - cybersecurity, considerations for 21, 22
  - cybersecurity, significance 3, 4
- Chief Financial Officer (CFO)
  - about 12, 25
  - cyber risk, addressing from complex financial view 33
  - cybersecurity aspects, considerations 30-32
  - cybersecurity, consideration 26
  - perspective 32
  - role, in cybersecurity 27, 28
- Chief Human Resources Officer (CHRO)
  - about 90, 102
  - challenges, with cybersecurity 111, 112
  - significance 102-105
  - transitioning role 105, 106
  - about 9, 59, 131
  - actions 67
  - activities, supporting cyber resilience 68-70
  - cybersecurity considerations 70
  - decision, impacting on cybersecurity 61, 62
  - role 62
  - role, on cybersecurity 61
- Chief Information Security Officer (CISO)
  - about 10, 28, 102, 117, 131
  - board of directors, reporting 98, 99
  - business 77
  - CxOs expectations, decoding 89
  - cyber insurance, purchasing 95-97
  - priorities 78
  - role 74-76

- Chief Information Security Officer (CISO), CxOs expectations  
 cyber risk quantification 92-95  
 key communication  
   non-negotiables 90-92
- Chief Marketing Officer (CMO) 133
- Chief Operating Officer (COO)  
 about 20, 117, 118, 133  
 collaboration, with CISO 121  
 responsibilities 119, 120  
 responsibility, for business  
   continuity 120  
 role 118, 119
- Chief Risk Officer (CRO)  
 about 27, 43  
 approach, developing as 52, 53  
 challenges, identifying 47-50  
 focus areas 45, 46  
 priorities, analyzing 46, 47  
 role 45, 46
- Chief Risk Officer (CRO),  
 challenges  
 connecting, dots 52  
 cyber risk 50, 51  
 frameworks 50, 51  
 strategies 50, 51  
 systems 50, 51
- Chief Security Officer (CSO) 12, 110
- Chief Technology Officer (CTO)  
 about 9, 131  
 code, securing 138  
 collaboration, with CISO 139  
 cybersecurity 134, 135  
 job tasks 132  
 role 132, 133  
 security 136  
 security principles, applying  
   between tasks 137  
 software development life cycle,  
   securing 137, 138  
 versus Chief Digital Officer  
   (CDO) 133, 134
- CHRO, support for cyber resilience  
 HR functions 107  
 HR tools 109  
 post-hiring examples 108  
 pre-hiring examples 107  
 qualified cybersecurity  
   team members,  
   recruiting 109, 110
- CIO decisions, impact on  
 cybersecurity  
 complex regulatory landscape 65  
 digital transformation,  
   balancing 63, 64  
 rapid technology adoption 62, 63  
 third-party risks 65
- CIO reporting structure  
 reference link 132
- CIO role  
 versus CISO roles 65, 66
- CIO's enablement, for  
 cybersecurity  
 visibility, providing 67, 68
- CISO's position  
 skills, needed 166, 167
- C-level executive (CxO) 12, 117

- Cloud Access Security Broker (CASB) 64
- cloud technology
  - used, for shaping security culture 187, 188
- CMO and CPO roles
  - similarities, identifying 144, 145
- community
  - building, considerations 190, 191
- company-wide healthy security culture
  - building 183-185
- complex financial view
  - cyber risk, addressing from 33
- crisis management
  - team (CMT) 53
- CRO, and CISO
  - collaboration potential, between 54, 55
- CTO and CISO collaboration
  - challenges 139, 140
- CxOs' roles
  - recapping 179-181
- cyberattack
  - examining 13, 14
- cyberattacks
  - business, preparing for 20, 21
- cyber-awareness program 188, 189
- cyber costs, versus return on investment
  - quantifying 14-17
- cyber incident
  - role, of marketing and communication 152-154
  - cyber incident response preparedness 21
- cyber insurance
  - purchasing 36
- cyber resilience 107
- cyber risk
  - about 4-9
  - addressing, from complex financial view 33
  - handling, approaches 82-84
  - identification and quantification 80-82
  - implications, for businesses 7-9
  - is business risk 11-13
  - management strategy 84-86
- Cyber Risk Meetup events
  - URL 114
- cyber-risk quantification
  - supporting 35, 36
- cybersecurity
  - about 11, 12, 121, 122
  - aspects considerations, for CFO 30-32
  - CFO, role 27, 28
  - challenges 9, 10
  - challenges, addressing 78-80
  - challenges, tackling 12
  - CIO, role 61
  - consideration, for CFO 26
  - considerations, for CEO 21, 22
  - culture, building 18, 19
  - governance pillar 6, 7
  - is critical environmental pillar 6, 7

- 
- marketing and privacy,
    - role in 146, 147
  - organization 9, 10
  - reporting 9, 10
  - risk mitigation 147-149
  - significance, for CEO 3, 4
  - social pillar 6, 7
  - cybersecurity budgets
    - benchmarking 34
  - cybersecurity, challenges
    - approaches, to handling
      - cyber risk 82-84
    - cyber risk identification 80-82
    - cyber risk management
      - strategy 84-86
    - indicators for
      - dashboarding/reporting 88
    - metrics 87
    - quantification 80-82
  - cybersecurity culture
    - building 181, 182
  - cybersecurity, need for CEO
    - dependency, on technology 5
  - cybersecurity spending
    - defining 35
  - cybersecurity team
    - building 113
    - considerations 114, 115
    - recruiting 113
  - D**
  - data breach
    - examining 13, 14
  - DevOps 138
  - DevSecOps 139
  - disaster recovery plan (DRP) 21
  - Distributed Denial of Service (DDoS) attack 80
  - Do Not Call (DNC) registry 146
  - dove, owl, peacock, and eagle (DOPE) 163
  - E**
  - Enterprise Risk Management (ERM) 25
  - Environmental, Social, and Governance (ESG) 6, 7, 46, 153, 179
  - European Network and Information Security Agency (ENISA) 95
  - F**
  - Factor Analysis of Information Risk (FAIR) 38, 93
  - Fortalice 67
  - G**
  - General Data Protection Regulation (GDPR) 33, 146
  - Global Financial Crisis (GFC) 48
  - governance, risk, and compliance (GRC) 46
  - Gramm-Leach-Bliley Act 65



**H**

healthy security culture, across  
different organizations  
tips and approaches 185-187

**I**

industrial control system (ICS) 16  
Information and Communication  
Technology (ICT) 124  
information technology 11, 12  
infrastructure as a service  
(IaaS) 187  
initial public offering (IPO) 15, 39  
Internet Crime Complaint  
Center (ICCC) 29  
Internet of Things (IoT) 3, 63

**K**

Key performance indicators  
(KPIs) 87

**L**

loss curve 38

**M**

merger and acquisition  
(M&A) 82, 172  
minimum viable product  
(MVP) 63  
Monetary Authority of  
Singapore (MAS) 96

Multi-Factor Authentication  
(MFA) 68

**N**

National Institute of Standards and  
Technology (NIST) 86  
next-generation firewall 64  
Notifiable Data Breaches  
(NDB) 146

**O**

Offensive Security Certified  
Professional (OSCP) 105  
Office of the Australian  
Information Commissioner  
(OAIC) 153  
Operational Expenditure  
(OPEX) 63  
Operational Technology  
(OT) 121, 122

**P**

Payment Card Industry Data  
Security Standard  
(PCI DSS) 33, 65  
Personal Data Protection  
Act (PDPA) 146  
Personally Identifiable  
Information (PII) 103  
plan-based business strategy 45  
platform as a service (PaaS) 187  
Post-Incident Review (PIR) 127  
public relations (PR) 152

**R**

research and development  
(R&D) 131

resilient security culture  
building options, exploring 191

return of value (ROV) 40

Return On Investment  
(ROI) 8, 62, 82

return on objective (ROO) 40

return on security investment  
(ROSI) 95

risk considerations  
example 18

robust security culture  
building 178

**S**

Sarbanes-Oxley Act of 2002  
(SOX, P.L. 107-204) 65

security and privacy programs  
intersection 150-152

security culture  
cloud-sharing  
responsibility 187, 188

security strategy 22

Shipping giant Maersk  
example 123

social pillar 6

Software as a Service (SaaS) 20, 187

**T**

third-party risks  
assessing 37

**U**

underwriting data 83

**V**

Value at Risk (VaR) 93

**W**

Web Application Firewall  
(WAF) 64





Packt . com

Subscribe to our online digital library for full access to over 7,000 books and videos, as well as industry leading tools to help you plan your personal development and advance your career. For more information, please visit our website.

## Why subscribe?

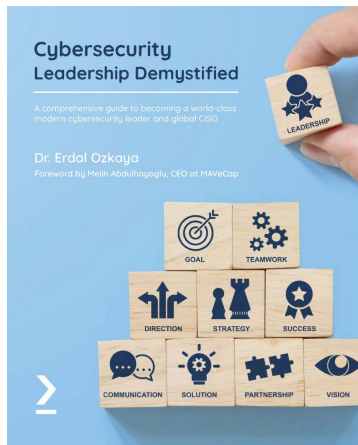
- Spend less time learning and more time coding with practical eBooks and Videos from over 4,000 industry professionals
- Improve your learning with Skill Plans built especially for you
- Get a free eBook or video every month
- Fully searchable for easy access to vital information
- Copy and paste, print, and bookmark content

Did you know that Packt offers eBook versions of every book published, with PDF and ePub files available? You can upgrade to the eBook version at [packt . com](http://packt.com) and as a print book customer, you are entitled to a discount on the eBook copy. Get in touch with us at [customer care@packtpub . com](mailto:customer care@packtpub.com) for more details.

At [www . packt . com](http://www.packt.com), you can also read a collection of free technical articles, sign up for a range of free newsletters, and receive exclusive discounts and offers on Packt books and eBooks.

# Other Books You May Enjoy

If you enjoyed this book, you may be interested in these other books by Packt:

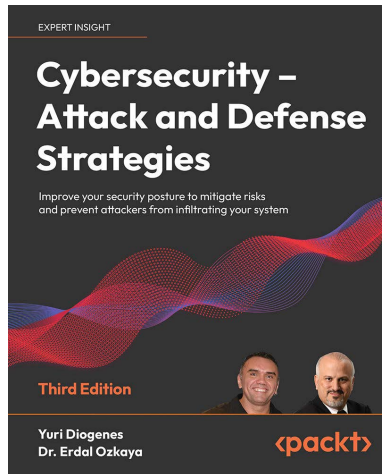


## Cybersecurity Leadership Demystified

Dr. Erdal Ozkaya

ISBN: 978-1-80181-928-2

- Understand the key requirements to become a successful CISO
- Explore the cybersecurity landscape and get to grips with end-to-end security operations
- Assimilate compliance standards, governance, and security frameworks
- Find out how to hire the right talent and manage hiring procedures and budget
- Document the approaches and processes for HR, compliance, and related domains
- Familiarize yourself with incident response, disaster recovery, and business continuity
- Get the hang of tasks and skills other than hardcore security operations



## Cybersecurity – Attack and Defense Strategies - Third Edition

Yuri Diogenes, Dr. Erdal Ozkaya

ISBN: 978-1-80324-877-6

- Learn to mitigate, recover from, and prevent future cybersecurity events
- Understand security hygiene and value of prioritizing protection of your workloads
- Explore physical and virtual network segmentation, cloud network visibility, and Zero Trust considerations
- Adopt new methods to gather cyber intelligence, identify risk, and demonstrate impact with Red/Blue Team strategies
- Explore legendary tools such as Nmap and Metasploit to supercharge your Red Team
- Discover identity security and how to perform policy enforcement
- Integrate threat detection systems into your SIEM solutions
- Discover the MITRE ATT Framework and open-source tools to gather intelligence

## **Packt is searching for authors like you**

If you're interested in becoming an author for Packt, please visit [authors.packtpub.com](https://authors.packtpub.com) and apply today. We have worked with thousands of developers and tech professionals, just like you, to help them share their insight with the global tech community. You can make a general application, apply for a specific hot topic that we are recruiting an author for, or submit your own idea.

## **Share your thoughts**

Now you've finished *Building a Cyber Resilient Business*, we'd love to hear your thoughts! If you purchased the book from Amazon, please [click here](#) for this book and share your feedback or leave a review on the site that you purchased it from.

Your review is important to us and the tech community and will help us make sure we're delivering excellent quality content.

