Building a Cyber Resilient Business

A cyber handbook for executives and boards

Dr. Magda Lilia Chelly
Shamane Tan
Hai Tran

Chapter 1

Images

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

Tables

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

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

Links

- *Allianz Risk Barometer 2020 - From market developments and fire to loss of reputation or brand value*: https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/allianz-risk-barometer-2020-business-risks.html.
- IBM's *Cost of a Data Breach Report 2021*: https://www.ibm.com/au-en/security/data-breach

Chapter 2

Links

- Agari's *Threat Intelligence Brief: The Geography of BEC*: https://www.agari.com/cyber-intelligence-research/whitepapers/london-blue-report.pdf

Chapter 4

Tables

Information Technology (IT)	Cybersecurity or information security
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

Links

- Your password doesn't matter: https://techcommunity.microsoft.com/t5/microsoft-entra-azure-ad-blog/your-pa-word-doesn-t-matter/ba-p/731984
- How COVID-19 has pushed companies over the technology tipping point—and transformed business forever: https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever
- ISACA's State Of Cybersecurity 2021, Part 2: https://www.isaca.org/resources/infographics/state-of-cybersecurity-2021-part-2

Chapter 5

Images

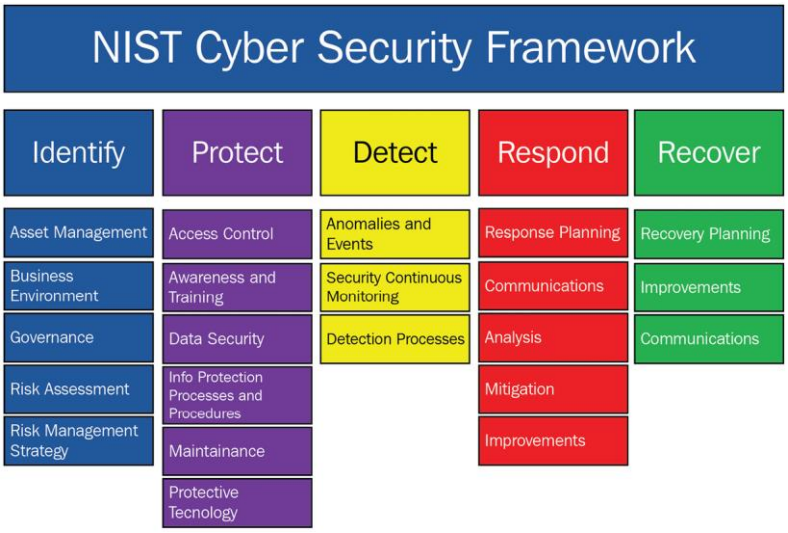

Figure 5.1 – The NIST framework

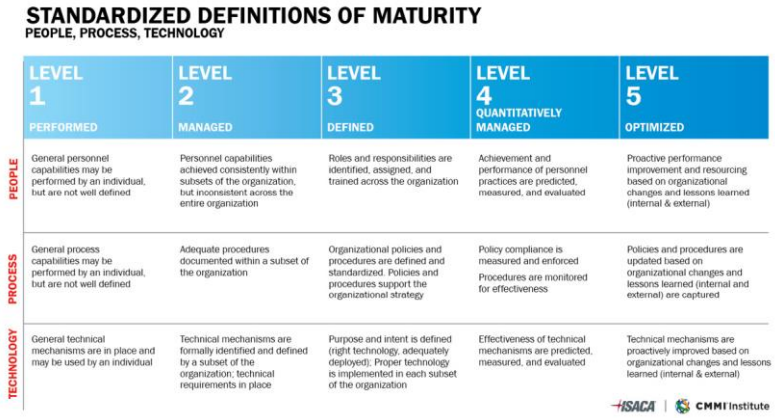

Figure 5.2 – Maturity models

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

Chapter 6

Images

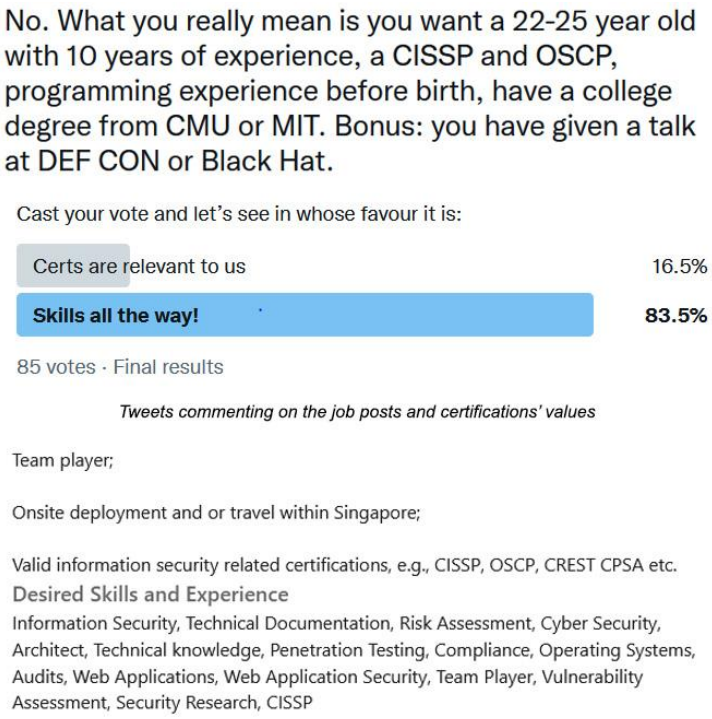

Figure 6.1 – Example job requirements

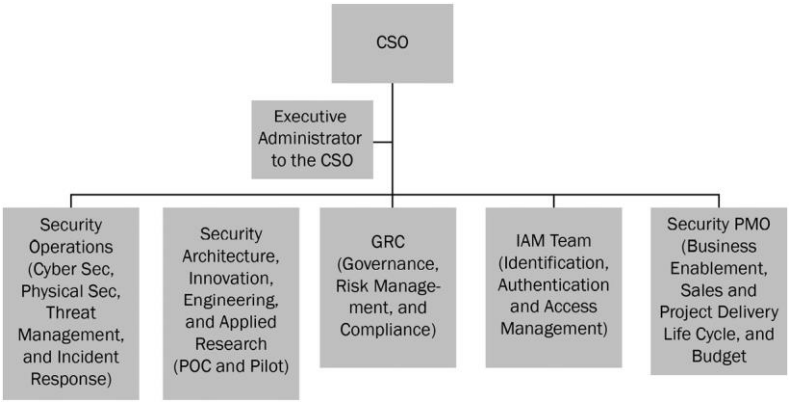

Figure 6.2 – An example of a cybersecurity team structure

Links

- Cyber Risker's Meetup: www.cyberriskmeetup.com

Chapter 7

Links

- The COO and Operational Technology Cybersecurity: A Report on Current Priorities and Challenges: https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/report-coo-and-cybersecurity.pdf
- Maersk had to reinstall all IT systems after NotPetya infection: https://www.itnews.com.au/news/maersk-had-to-reinstall-all-it-systems-after-notpetya-infection-481815

Chapter 8

Links

- Who's the boss? Trends in CIO reporting structure: https://www2.deloitte.com/us/en/insights/focus/cio-insider-business-insights/trends-in-cio-reporting-structure.html
- 2016 CIO & CTO Survey Results: https://transmitter.ieee.org/wp-content/uploads/2017/03/IEEE-2016-CIO-CTO-Survey-Results.pdf

Chapter 9

Images

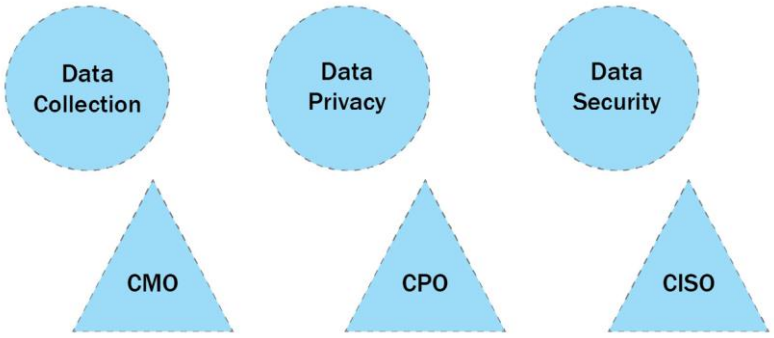

Figure 9.1 – High-level roles and responsibilities

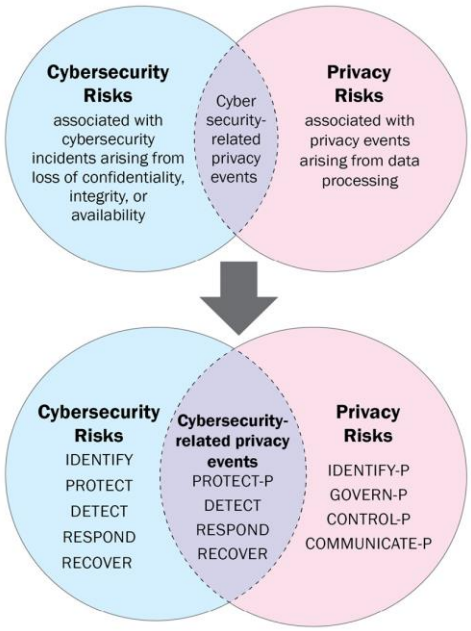

Figure 9.2 – The privacy framework Venn diagram

Links

- Marriott breach cyber industry loss could be up to $600m: AIR https://www.reinsurancene.ws/marriott-breach-cyber-industry-loss-could-be-up-to-600m-air/
- Australian Red Cross Blood Service data breach: https://www.oaic.gov.au/updates/news-and-media/australian-red-cross-blood-service-data-breach#australian-red-cross-blood-service-data-breach

Chapter 10

Images

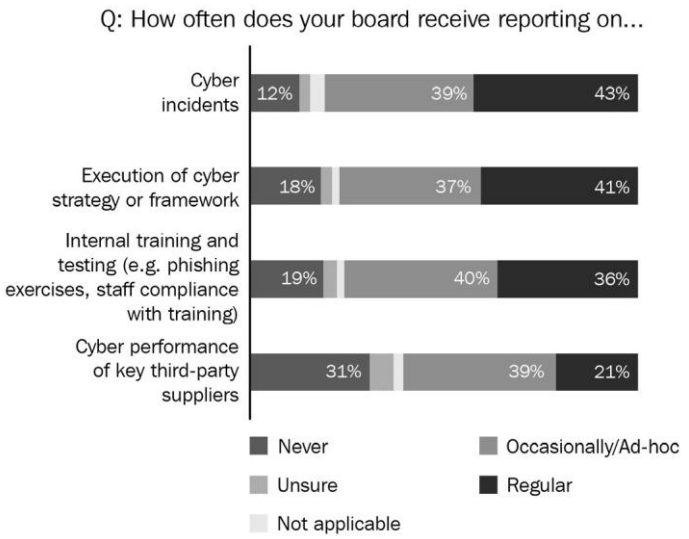

Figure 10.1 – AICD survey findings of board-reporting cyber-risk areas

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

Links

- Boards and Cyber Resilience: SURVEY FINDINGS: https://www.aisa.org.au/common/Uploaded%20files/Research/FINAL%2008299-3-5-Cyber-Security-Report-30pp-v3B.pdf

Chapter 11

Images

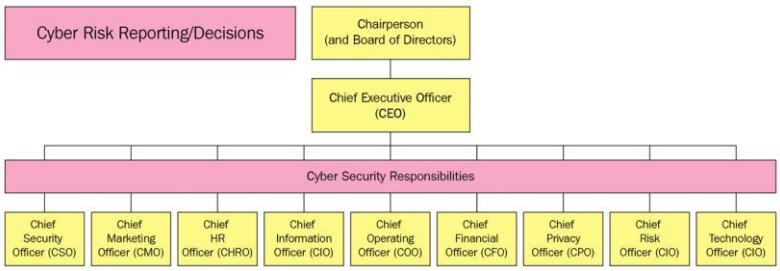

Figure 11.1 – Organigramme

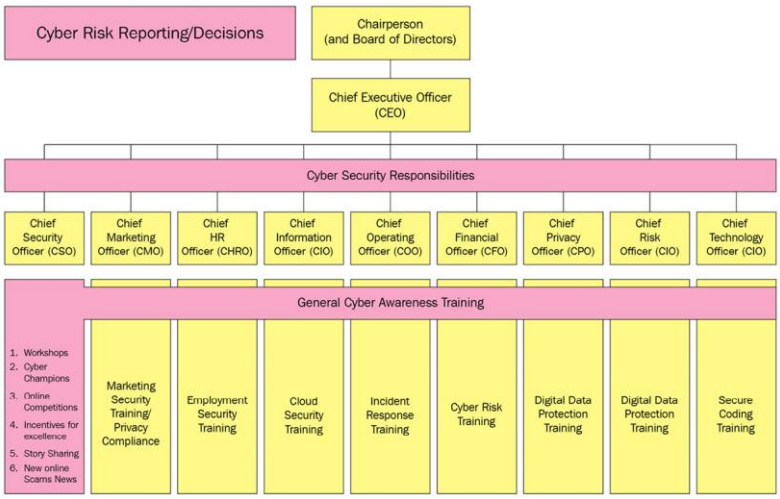

Figure 11.2 – Awareness program components