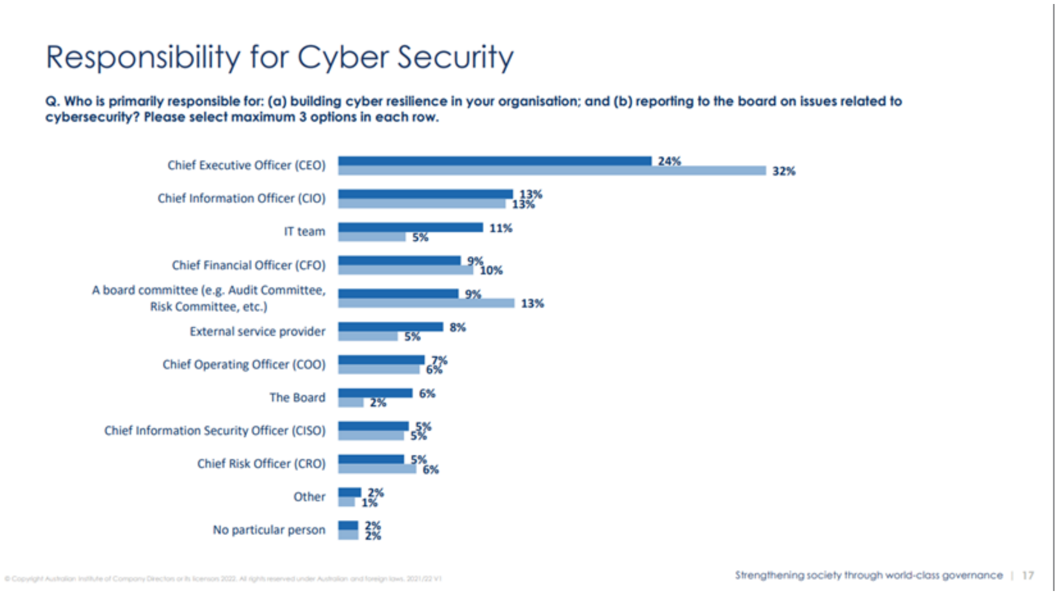
Chapter 1: The CEO Cyber Manual



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.

Strengthening society through world-class governance | 17

Chapter 2: A Modern Cyber-Responsible CFO

No Images…

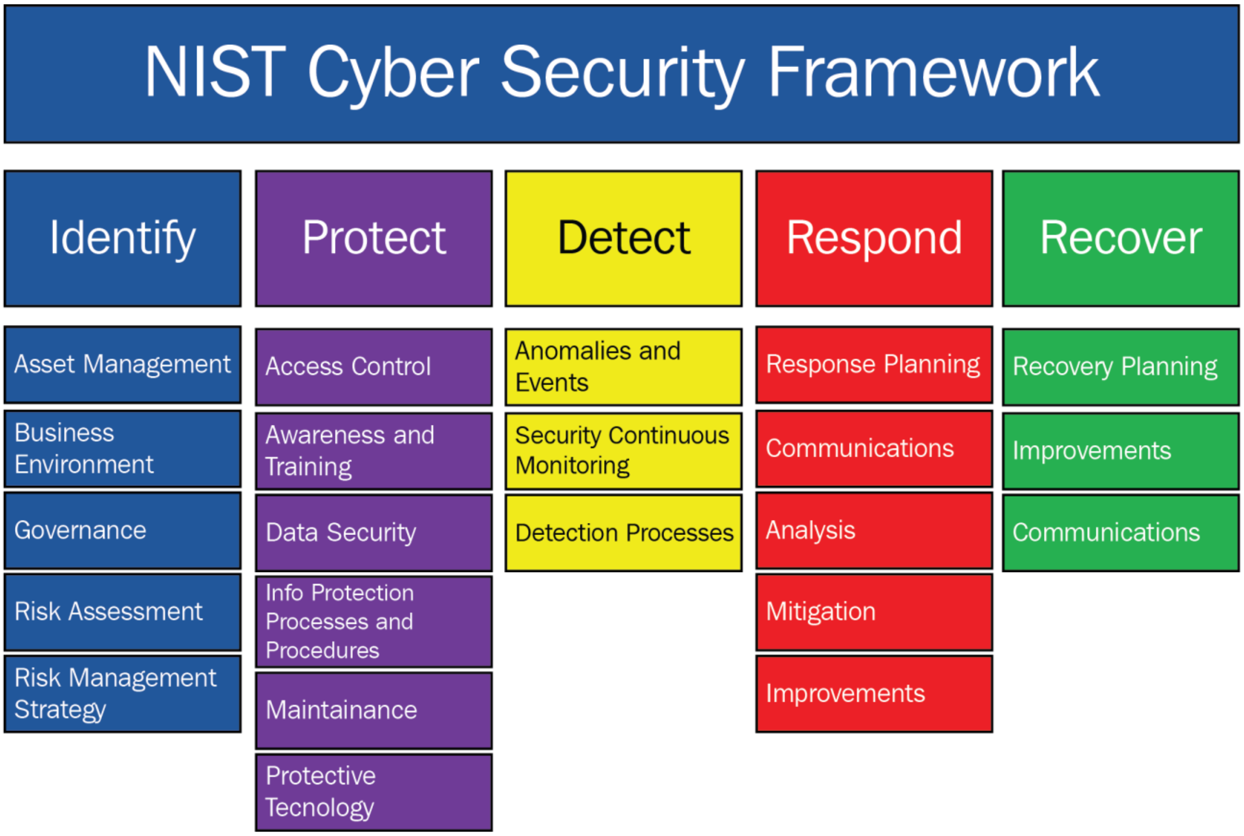
Chapter 3: The Role of the CRO in Cyber Resilience

No Images…

Chapter 4: Your CIO—Your Cyber Enabler

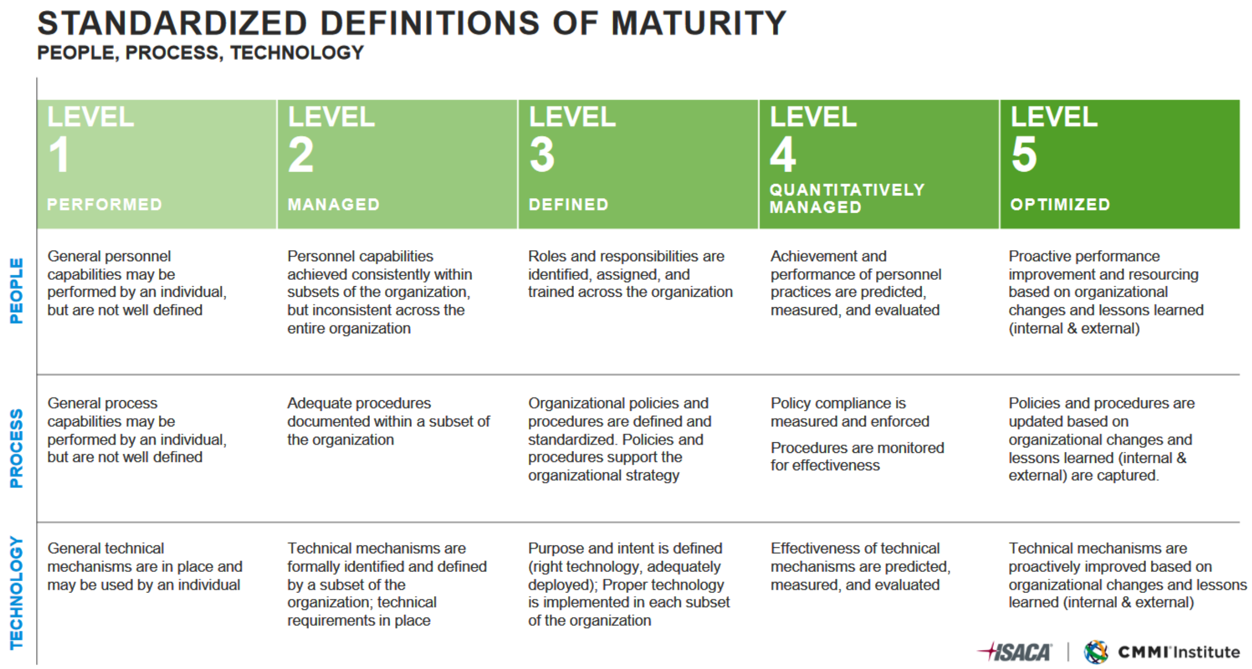
No Images…

Chapter 5: Working with Your CISO



NIST Cyber Security Framework

Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintainance		Improvements	
	Protective Tecnology			

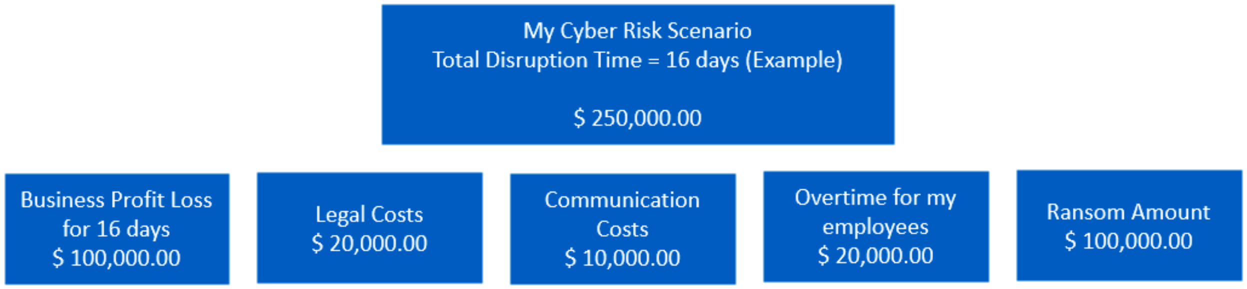


STANDARDIZED DEFINITIONS OF MATURITY

PEOPLE, PROCESS, TECHNOLOGY

	LEVEL 1 PERFORMED	LEVEL 2 MANAGED	LEVEL 3 DEFINED	LEVEL 4 QUANTITATIVELY MANAGED	LEVEL 5 OPTIMIZED
PEOPLE	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)
PROCESS	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 & external) are captured.
TECHNOLOGY	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)

ISACA | CMMI Institute



My Cyber Risk Scenario
Total Disruption Time = 16 days (Example)

$ 250,000.00

Business Profit Loss for 16 days
$ 100,000.00

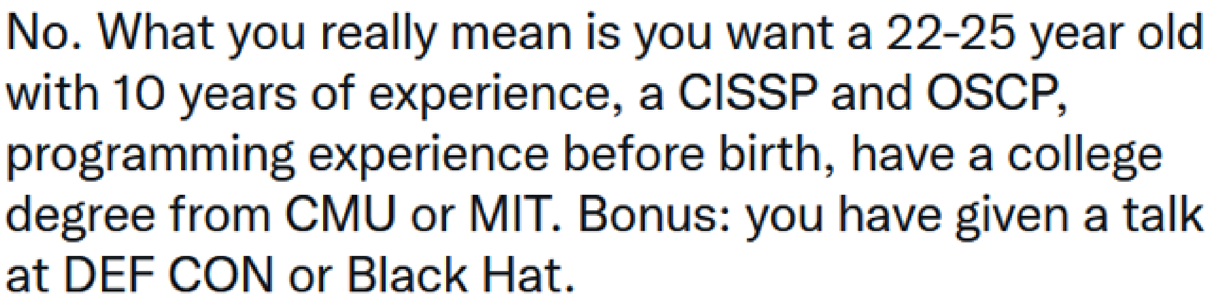
Legal Costs
$ 20,000.00

Communication Costs
$ 10,000.00

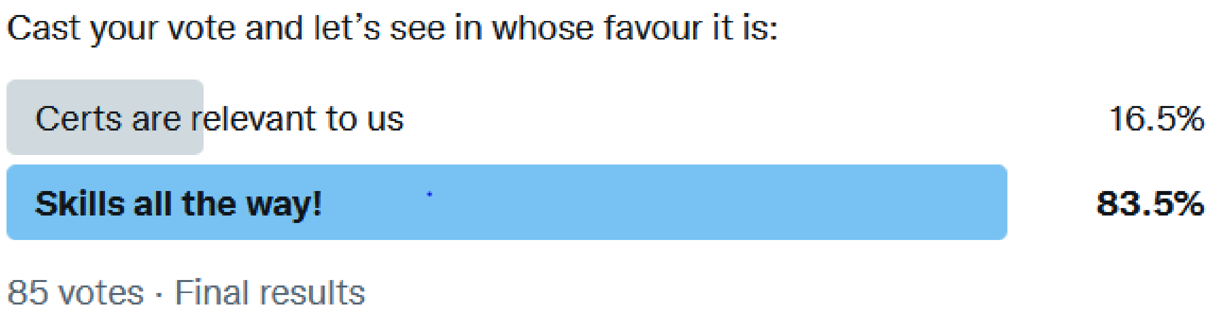
Overtime for my employees
$ 20,000.00

Ransom Amount
$ 100,000.00

Chapter 6: The Role of the CHRO in Reducing Cyber Risk



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.

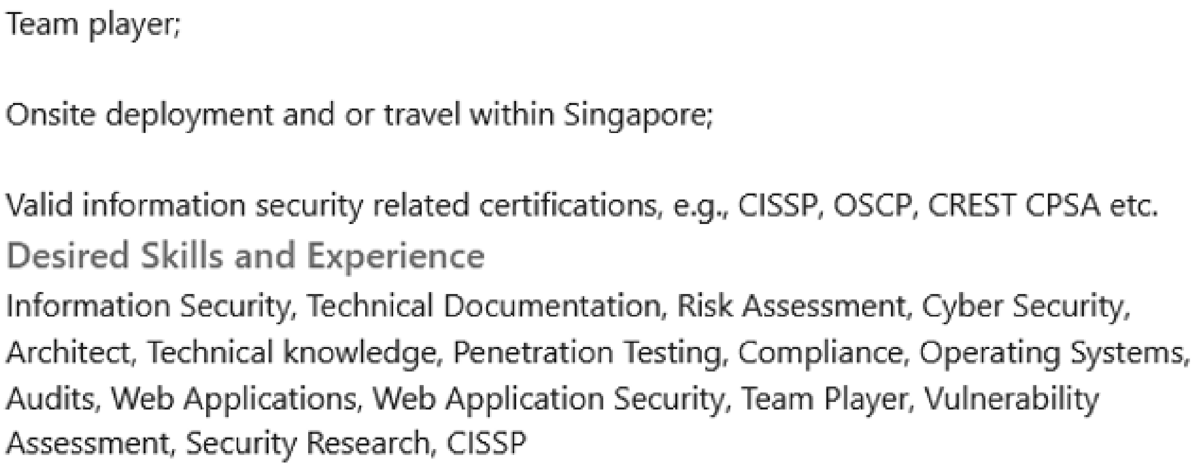


Cast your vote and let’s see in whose favour it is:

Certs are relevant to us	16.5%
Skills all the way!	**83.5%**

85 votes · Final results

Tweets commenting on the job posts and certifications’ values



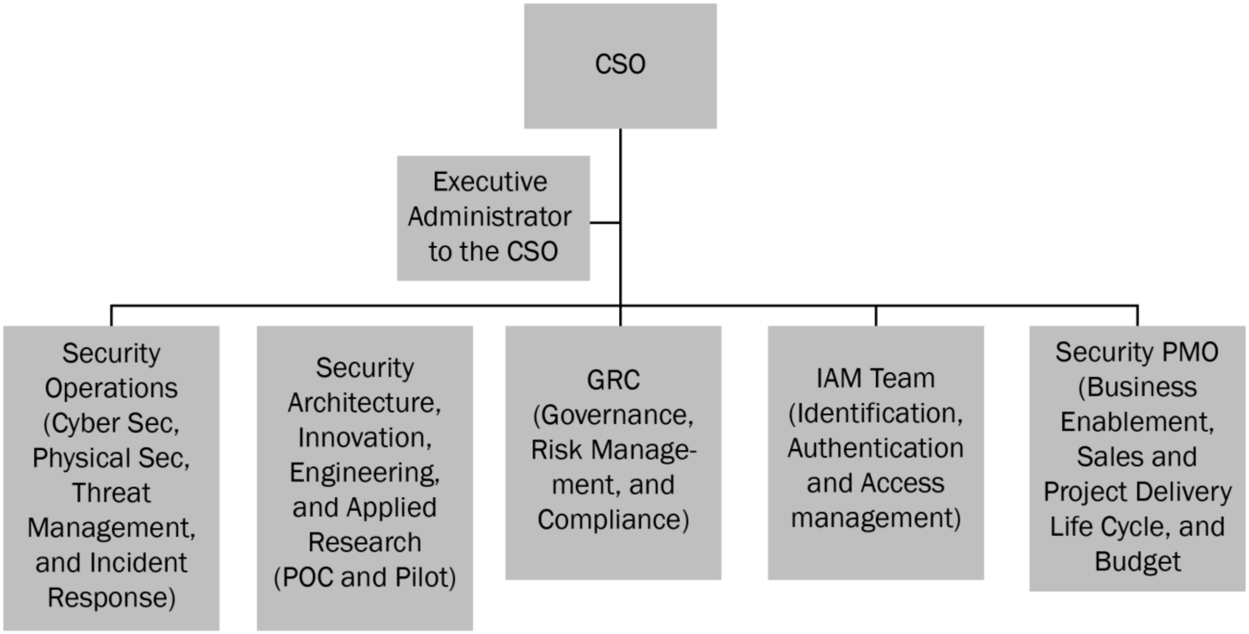
Team player;

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


CSO
Executive Administrator to the CSO
Security Operations (Cyber Sec, Physical Sec, Threat Management, and Incident Response)
Security Architecture, Innovation, Engineering, and Applied Research (POC and Pilot)
GRC (Governance, Risk Management, and Compliance)
IAM Team (Identification, Authentication and Access management)
Security PMO (Business Enablement, Sales and Project Delivery Life Cycle, and Budget

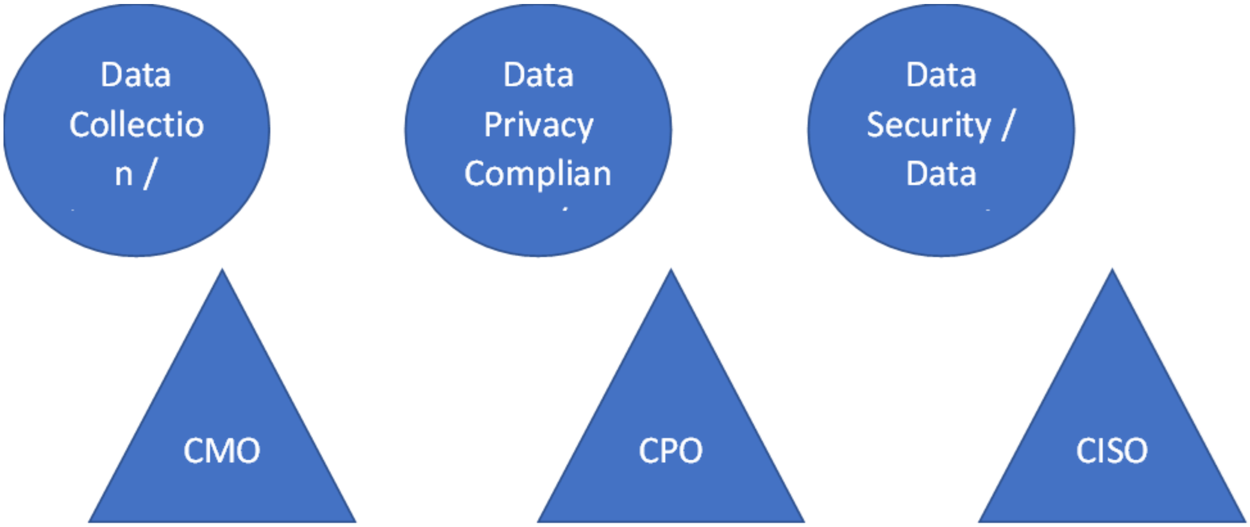
Chapter 7: The COO and Their Critical Role in Cyber Resilience

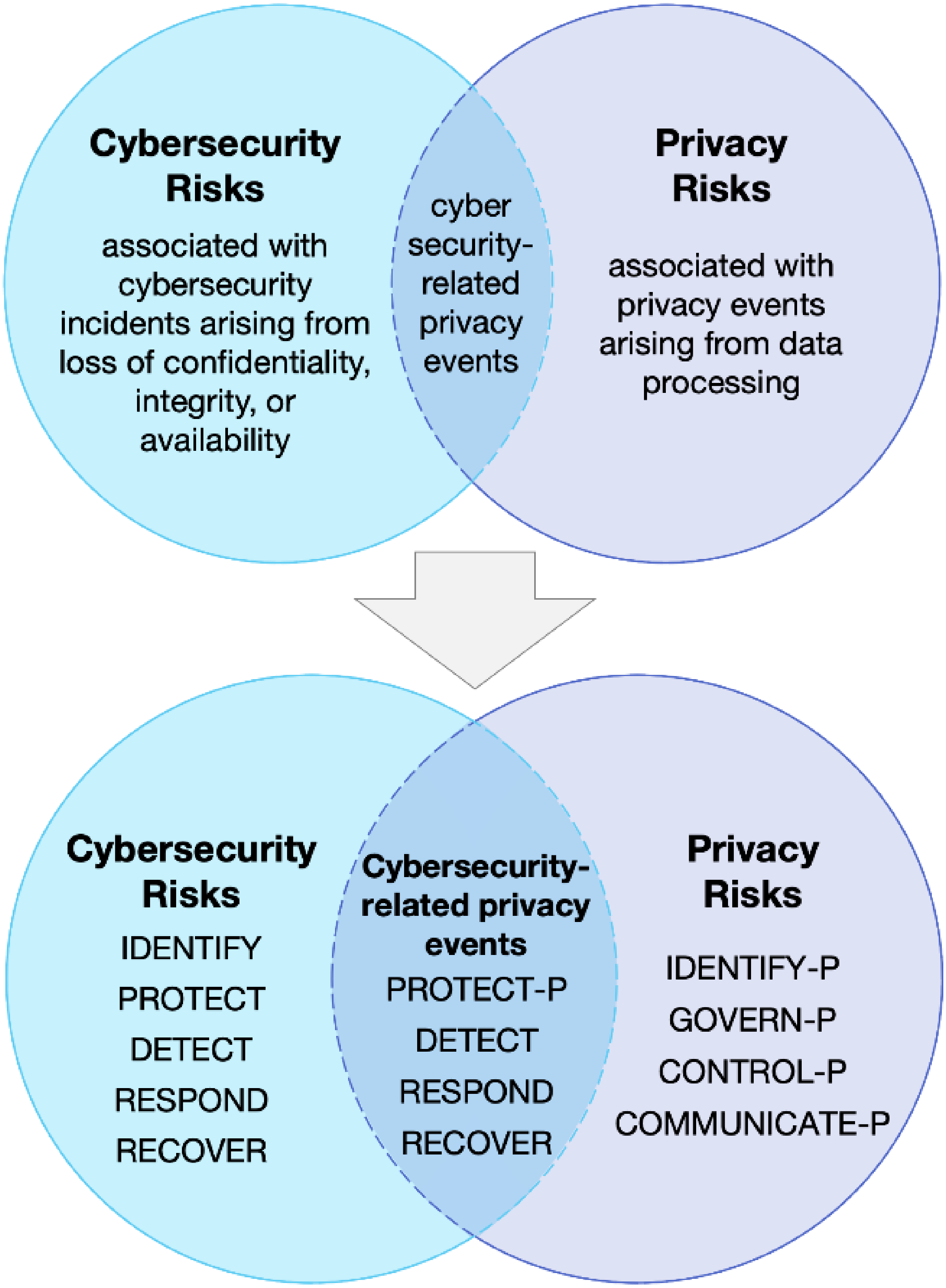
No Images…

Chapter 8: The CTO and Security by Design

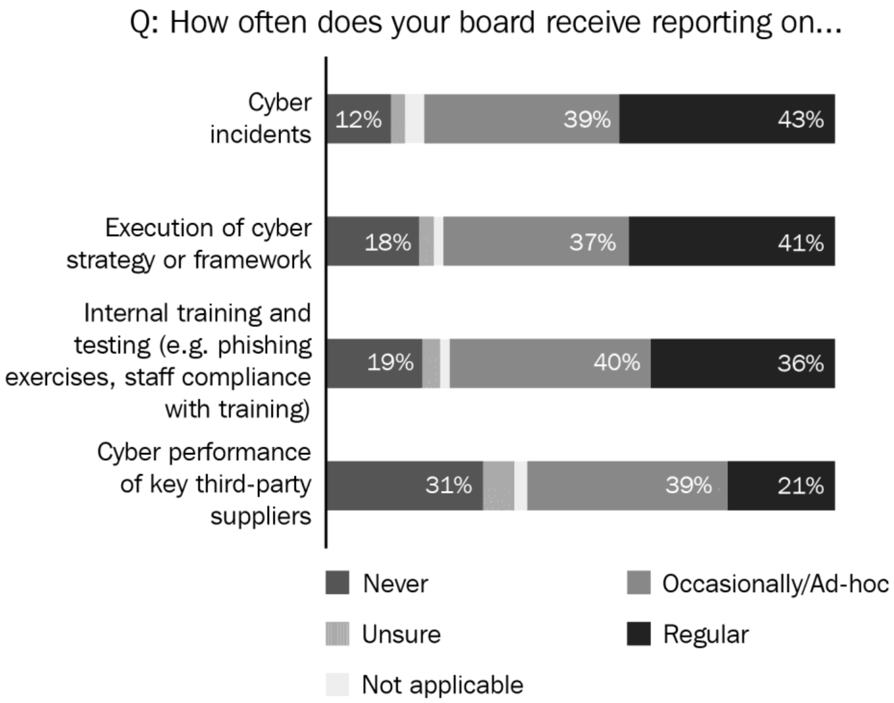
No Images…

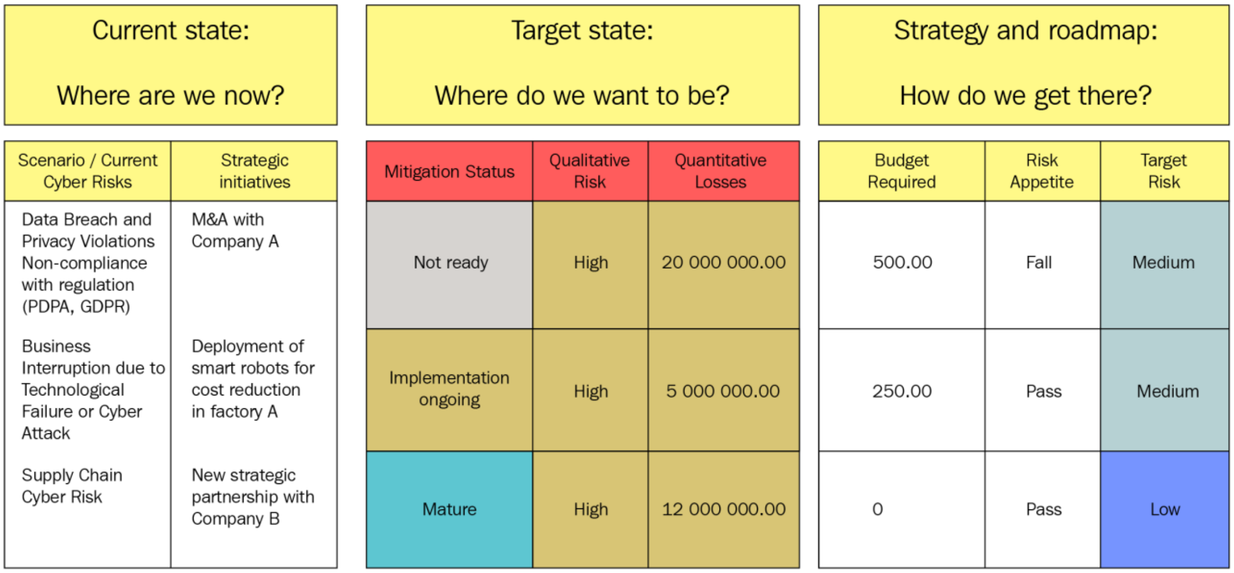
Chapter 9: The CMO and CPO—Convergence Between Privacy and Security




Cybersecurity Risks
associated with cybersecurity incidents arising from loss of confidentiality, integrity, or availability
cyber security-related privacy events
Privacy Risks
associated with privacy events arising from data processing
Cybersecurity Risks
IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER
Cybersecurity-related privacy events
PROTECT-P
DETECT
RESPOND
RECOVER
Privacy Risks
IDENTIFY-P
GOVERN-P
CONTROL-P
COMMUNICATE-P

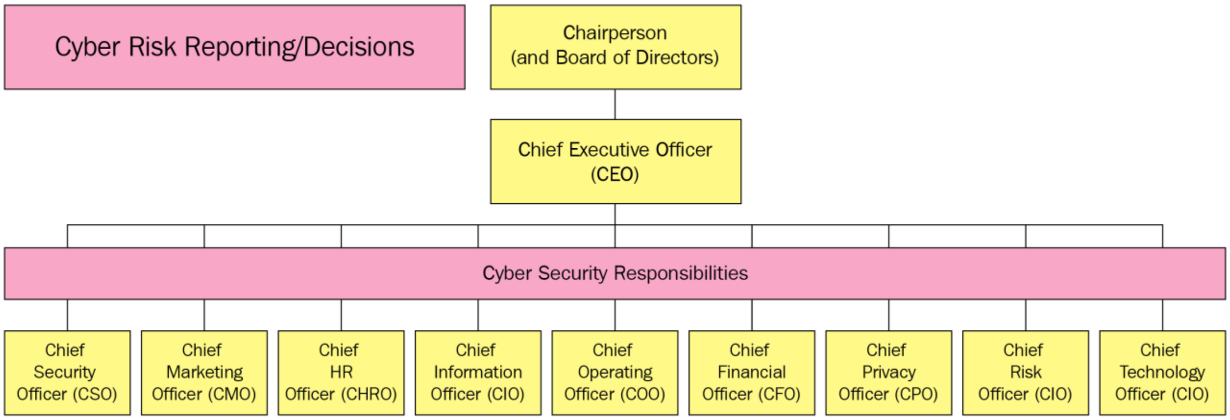
Chapter 10: The World of the Board

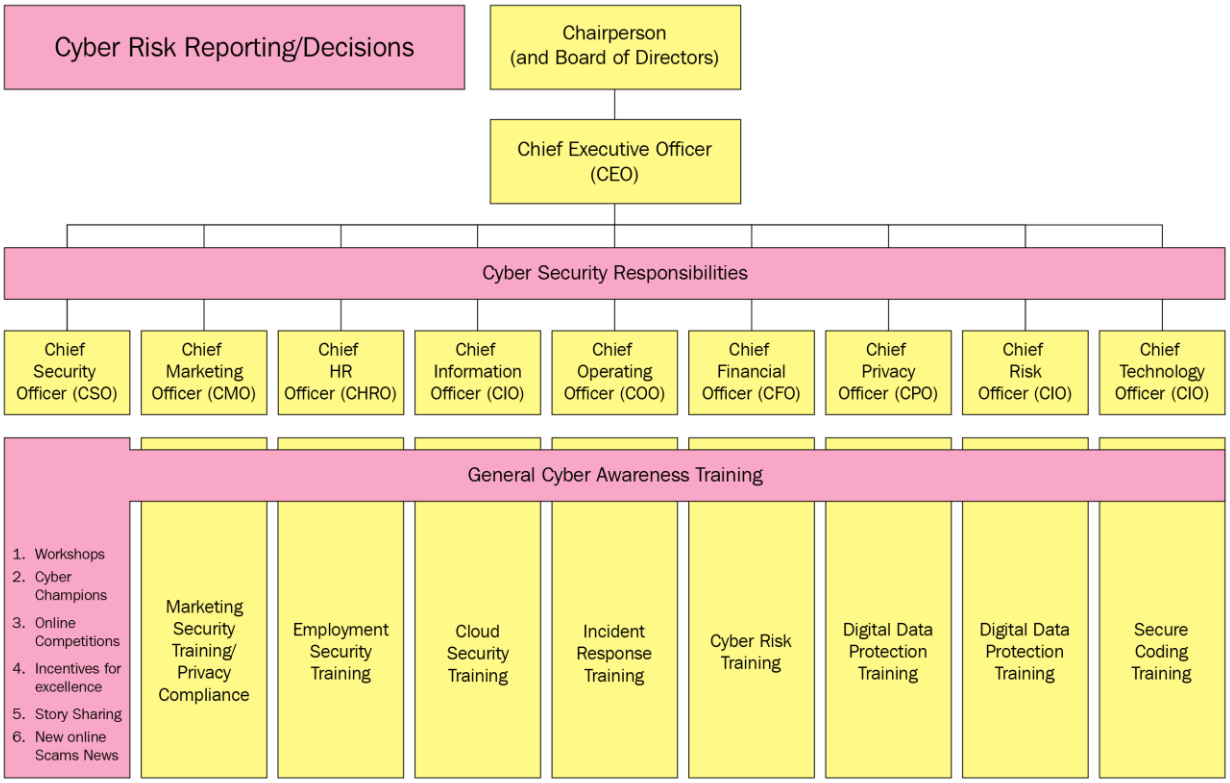




Current state: Where are we now?		Target state: Where do we want to be?			Strategy and roadmap: How do we get there?		
Scenario / Current Cyber Risks	Strategic initiatives	Mitigation Status	Qualitative Risk	Quantitative Losses	Budget Required	Risk Appetite	Target Risk
Data Breach and Privacy Violations Non-compliance with regulation (PDPA, GDPR)	M&A with Company A	Not ready	High	20 000 000.00	500.00	Fall	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

Chapter 11: The Recipe for Building a Strong Security Culture – Bringing It All Together


Cyber Risk Reporting/Decisions
Chairperson (and Board of Directors)
Chief Executive Officer (CEO)
Cyber Security Responsibilities
Chief Security Officer (CSO)
Chief Marketing Officer (CMO)
Chief HR Officer (CHRO)
Chief Information Officer (CIO)
Chief Operating Officer (COO)
Chief Financial Officer (CFO)
Chief Privacy Officer (CPO)
Chief Risk Officer (CIO)
Chief Technology Officer (CIO)


Cyber Risk Reporting/Decisions
Chairperson (and Board of Directors)
Chief Executive Officer (CEO)
Cyber Security Responsibilities
Chief Security Officer (CSO)
Chief Marketing Officer (CMO)
Chief HR Officer (CHRO)
Chief Information Officer (CIO)
Chief Operating Officer (COO)
Chief Financial Officer (CFO)
Chief Privacy Officer (CPO)
Chief Risk Officer (CIO)
Chief Technology Officer (CIO)
General Cyber Awareness Training
1. Workshops
2. Cyber Champions
3. Online Competitions
4. Incentives for excellence
5. Story Sharing
6. New online Scams News
Marketing Security Training/ Privacy Compliance
Employment Security Training
Cloud Security Training
Incident Response Training
Cyber Risk Training
Digital Data Protection Training
Digital Data Protection Training
Secure Coding Training