Cyber Resilience Strategy and Board Reporting

Presented by:

Roshan Daluwakgoda

Chief Information Security Officer

Corinium connected thinking | CISO Melbourne 2024

Ransomware continues to pose a significant risk to organizations.

- **Cyber extortion:** A hacker threatens to seize, damage or release electronic data owned by the victim. This often results in **double or triple extortion tactics**.
- The median dwell time between the first evidence of malicious activity and the deployment of ransomware is five days.

Source: Gartner

Process

Ransomware usually enters an organization’s system through:

a) Email phishing campaigns, prompting a user to click on a link, downloading the ransomware automatically, or

b) Exploiting vulnerabilities in an organization’s security and IT systems

The ransomware then spreads across all accessible IT systems, **encrypting the data,** and making it **inaccessible to users**

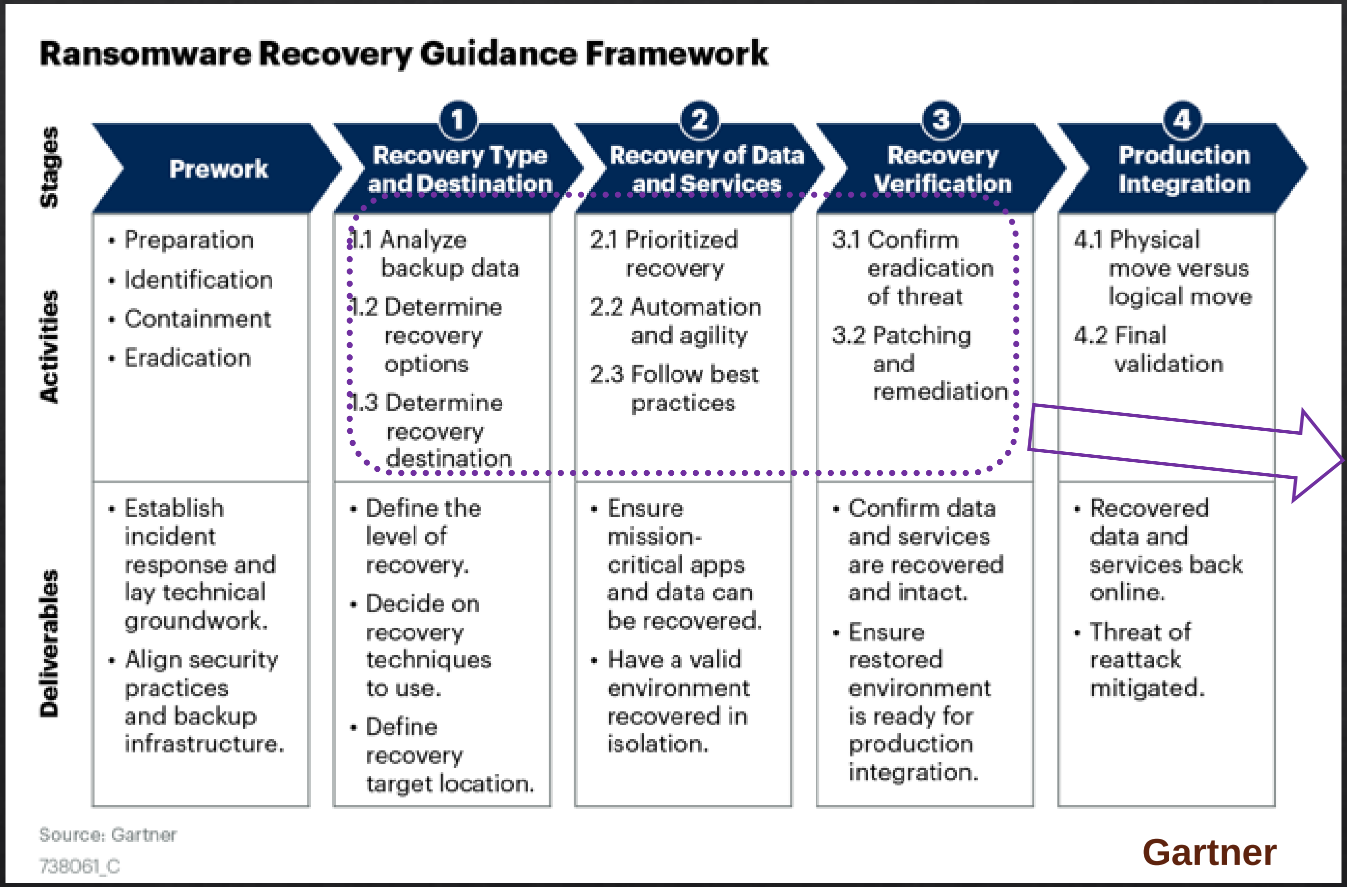
The cyber criminals then demand payment from the owners in return for access to the data or systems, in some form of **cryptocurrency**, usually bitcoin

Payment must then be made within a few hours or days, after which the data will be permanently lost or erased

Source: Gartner

CISO Leadership needs to adapt to these changes and look beyond just endpoint security controls to protect against ransomware

Build Your Recovery Capabilities - Adapt to Threat



Ransomware Recovery Guidance Framework

Stages	Prework	1 Recovery Type and Destination	2 Recovery of Data and Services	3 Recovery Verification	4 Production Integration
Activities	• Preparation • Identification • Containment • Eradication	1.1 Analyze backup data 1.2 Determine recovery options 1.3 Determine recovery destination	2.1 Prioritized recovery 2.2 Automation and agility 2.3 Follow best practices	3.1 Confirm eradication of threat 3.2 Patching and remediation	4.1 Physical move versus logical move 4.2 Final validation
Deliverables	• Establish incident response and lay technical groundwork. • Align security practices and backup infrastructure.	• Define the level of recovery. • Decide on recovery techniques to use. • Define recovery target location.	• Ensure mission-critical apps and data can be recovered. • Have a valid environment recovered in isolation.	• Confirm data and services are recovered and intact. • Ensure restored environment is ready for production integration.	• Recovered data and services back online. • Threat of reattack mitigated.

Source: Gartner

738061_C

Gartner

Recovery Time

- Do you have the ability to identify meta data associated with the threat actor in your environment?
- Timeline of Threat Actor Presence :How long has the threat actor been in your environment ?
- Have you identified all of the threat actor's C2 connections and remediated?

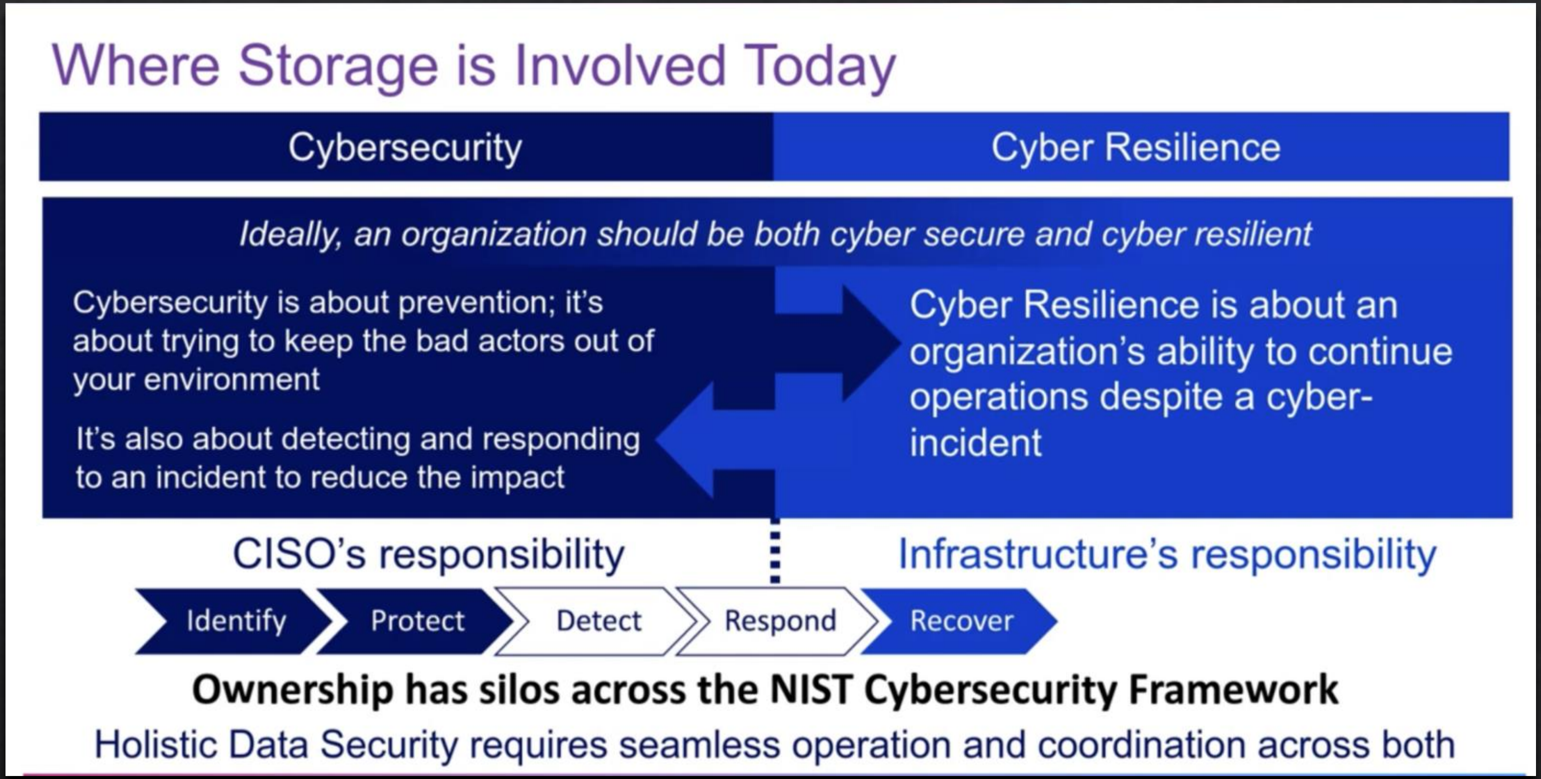
Recovery Options

- Has the threat actor left a back door open to your environment ? *(i.e: ransomware, extortions, data exfiltration etc.)*

Recovery Target Location

- Ensure your recovery target is sanitised.

Secure your Data – Architecture for Resilience



Where Storage is Involved Today

Cybersecurity	Cyber Resilience

Ideally, an organization should be both cyber secure and cyber resilient

Cybersecurity is about prevention; it's about trying to keep the bad actors out of your environment

It's also about detecting and responding to an incident to reduce the impact

Cyber Resilience is about an organization's ability to continue operations despite a cyber-incident

CISO's responsibility

Infrastructure's responsibility

Ownership has silos across the NIST Cybersecurity Framework

Holistic Data Security requires seamless operation and coordination across both

Source : SNIA CSTI

CISO is responsible for the Data Protection

- Data Privacy
- Data Security
- Secure Data Recovery

Who is responsible for detecting threats surfaced by storage ?

Data Storage ? *Implement Air Gapped storage (combination of effective IAM and Network Segregation)*

Immutable Data Archival ?
Your last hope

Cyber **resilience requires** the ability to **anticipate** and **adapt to adverse conditions and attacks**

Anticipated Threats

- Ransomware
- Data Related Threats
- Intrusion
- Supply Chain Attack
- DoS/DDoS/RDoS
- Malware
- Misconfiguration
- Poor Security Practice
- Social Engineering
- Misinformation/ Disinformation

Architect for Resilience

- Identify Attack Surface and Build a Defendable Environment
- Network Segmentation and Access Management
- Information Assets Protection and data Leak prevention
- Supply chain cyber risk reduction through collaborative procurement

Adapt to Threat

- Cybersecurity incident and contingency planning
- Establish vulnerability management
- Monitor for threats and respond

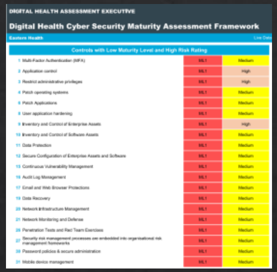
Cyber Resilience Strategy and Roadmap Development

High Value Cyber Resilience Strategy Development

Enabling Secure Digital Transformation with Trusted Services

Current state: Where are we now?

Threat & Risk Assessment



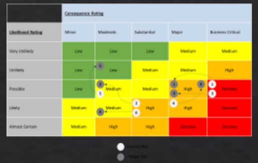
DIGITAL HEALTH ASSESSMENT EXECUTIVE

Digital Health Cyber Security Maturity Assessment Framework

Eastern Health

Controls with Low Maturity Level and High Risk Rating

1	Multi-Factor Authentication (MFA)	ML1	Medium
2	Application control	ML1	High
3	Restrict administrative privileges	ML1	High
4	Patch operating systems	ML1	Medium
5	Patch Applications	ML1	Medium
8	User application hardening	ML1	Medium
9	Inventory and Control of Enterprise Assets	ML1	High
10	Inventory and Control of Software Assets	ML1	Medium
11	Data Protection	ML1	Medium
12	Secure Configuration of Enterprise Assets and Software	ML1	Medium
15	Continuous Vulnerability Management	ML1	Medium
16	Audit Log Management	ML1	Medium
17	Email and Web Browser Protections	ML1	Medium
19	Data Recovery	ML1	Medium
20	Network Infrastructure Management	ML1	Medium
21	Network Monitoring and Defense	ML1	Medium
26	Penetration Tests and Red Team Exercises	ML1	Medium
27	Security risk management processes are embedded into organisational risk management frameworks	ML1	Medium
30	Password policies & secure administration	ML1	Medium
31	Mobile device management	ML1	Medium



Likelihood Rating	Consequence Rating Minor	Moderate	Substantial	Major	Business Critical
Very Unlikely	Low	Low	Low	Medium	Medium
Unlikely	Low	Low	Medium	Medium	High
Possible	Low	Medium	Medium	High	Extreme
Likely	Medium	Medium	High	High	Extreme
Almost Certain	Medium	High	High	Extreme	Extreme

Current State Capability Maturity Assessment

- Emerging Threat Landscape
- Increased Regulatory Compliance

Target state: Where do we want to be?

Target State Vision and Desired Capabilities

Careful profiling is done in defining the cyber security future state capabilities uplift with initiatives to be achieved in 3 years timeline

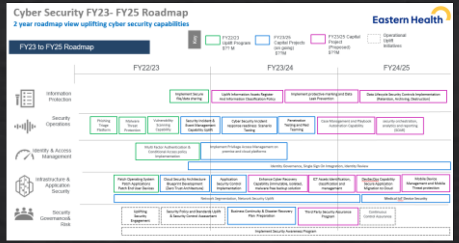
Eastern Health

Risk Reduction Target

- Enabling secure digital transformation
- Secure Data Driven Decision Making
- Secure Cloud Adaptation
- Improved Cyber Resiliency

Strategy & roadmap: How do we get there?

Prioritisation of Strategic Capabilities



Cyber Security FY23- FY25 Roadmap

2 year roadmap view uplifting cyber security capabilities

Eastern Health

FY23 to FY25 Roadmap

Key
FY22/23 Uplift Program
FY23/25 Capital Projects (on going)
FY23/25 Capital Project (Proposed)
Operational Uplift Initiatives
FY22/23
FY23/24
FY24/25
Information Protection
Security Operations
Identity & Access Management
Infrastructure & Application Security
Security Governance& Risk

Roadmap

Budget

- Information and Data Protection
- Detect, Response Respond and Recovery
- Digital Identity Trust
- Infrastructure and Cloud Security
- Security Governance

Strategy Planning Process and Current Status Analysis

Threat & Risk Assessment

Business Driver and strategic priorities

Strategy, budget , roadmap and Operating Model

Adapt Cyber Security Framework

Domains	Objectives	Information Security Capabilities | Services	Policies| Standards |Procedures |Plans
GOVERNANCE	• Ensure organisation understands and manages its cyber security risks and compliance obligations appropriately • Provide staff with cyber security knowledge to allow them to be able to protect our assets	• Information Security Reporting • Information Security Policy Governance • Information Security Risk Management • Information Security Awareness and Training • Third Party Security Risk Management	• Information Security Management Framework (ISMF) • Information Security Policy • Information Management Policy • Enterprise Risk Management Framework
PROTECT	• Ensure technology is consistently built with appropriate security levels • Ensure security technology provides the required level of security capability	• Identity and Access Management • Information and Data Protection • Infrastructure and Application Protection • End Point Protection • Security Design and Architecture	• Identity and Access Management standards • Information Security Classification and Handling Standards • Password and Privileged Account Management Standard • Communication and Networks Security Management Standards
DETECT	• Understand and manage perceived system vulnerabilities as well as align to risk averse strategy and compliance obligations	• Vulnerability & Threat Management • Managed Detect and Respond Service • Cyber Security Event Monitoring and alerting	• Threat and Vulnerability Management Standard • Security Event Logging and Monitoring Standard
RESPOND	• Contain or mitigate the impact of potential security threats and incidents	• Cyber Security Incident Management, Threat Hunting	• Information Security Incident Management Plan
RECOVER	• Efficiently recover normal business operations to reduce the overall impact of a security event	• Cyber Recovery Plan • ICT Business Continuity and Disaster Recovery • Crisis Management	• ICT Business Continuity and Disaster Recovery Plans • Crisis Management Plan

Aligned to VPDSF and VPDSS , PSPF , ASD-ISM, SOCI, NIST-CSF , ISO27001 , ISO22301, Privacy and Data Protection Act

Identify strategic initiatives to address control gaps

Focused strategies to remediate Risk and Delivery Business Outcome

Strategic initiatives have been identified to reduce the risk and address the controls gaps for each risk scenario, to guide the selection and prioritisation of the strategic initiatives to be included in the Strategy.

	Scenario	Current Risk	Strategic initiatives	Target Risk
RC.01	Data breach and loss through attacker.	High	Protective Marking and DLP	Medium
RC.02	Unauthorised privileged access by attacker	Medium	Network Access Control, SASE capability, Privileged Access Management	Low
RC.03	Exploit of vulnerabilities by external attack	High	Vulnerability and Threat Management	Medium
RC.04	Website comprise by external attacker.	Medium	SAST and DAST and DevSecOps Capability uplift	Low
RC.05	Unauthorized access to systems and platforms	High	Multifactor Authentication, SSO and Identity Governance	Low
RC.06	Rransomware attacks on crown jewel systems	Very High	SIEM and SOAR Capability, 24x7 cyber defence centre	Medium
RC.07	Advanced persistent cyber attack	Very High	Cyber Incident Response Plan, Simulation (Red/Blue team)	Medium
RC.08	Regulatory non-compliance	Medium	Partner Engagement , Leverage ICT team, skill uplift	Low
RC.09	External compromise through phishing email	High	Cyber Security Awareness and Training Program	Medium
RC.10	Exploitation of third party security weakness	High	Third Party Cyber Risk Management Capability	Medium

Regulatory Obligations : Australian Cyber Security Strategy Legislative Reform and Security of Critical Infrastructure (SOCI) Act

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Measure 1: Helping prevent cyber incidents secure-by design standards

Measure 2: Further understanding cyber incidents ransomware reporting

Measure 3: Encouraging engagement during cyber incidents limited use obligation on the ASD and the National Cyber Security Coordinator

Measure 4: Learning lessons after cyber incidents - Cyber Incident Review Board

Measure 5: Protecting critical infrastructure data storage systems

Measure 6: Improving our national response to the consequences of significant incidents consequence management powers

Measure 7: Simplifying how government and industry shares information in crisis situations – Protected information provisions

Measure 8: Enforcing critical infrastructure risk management obligations – Review and remedy powers

Measure 9: Consolidating telecommunication security requirements- Telecommunications sector security under the SOCI Act

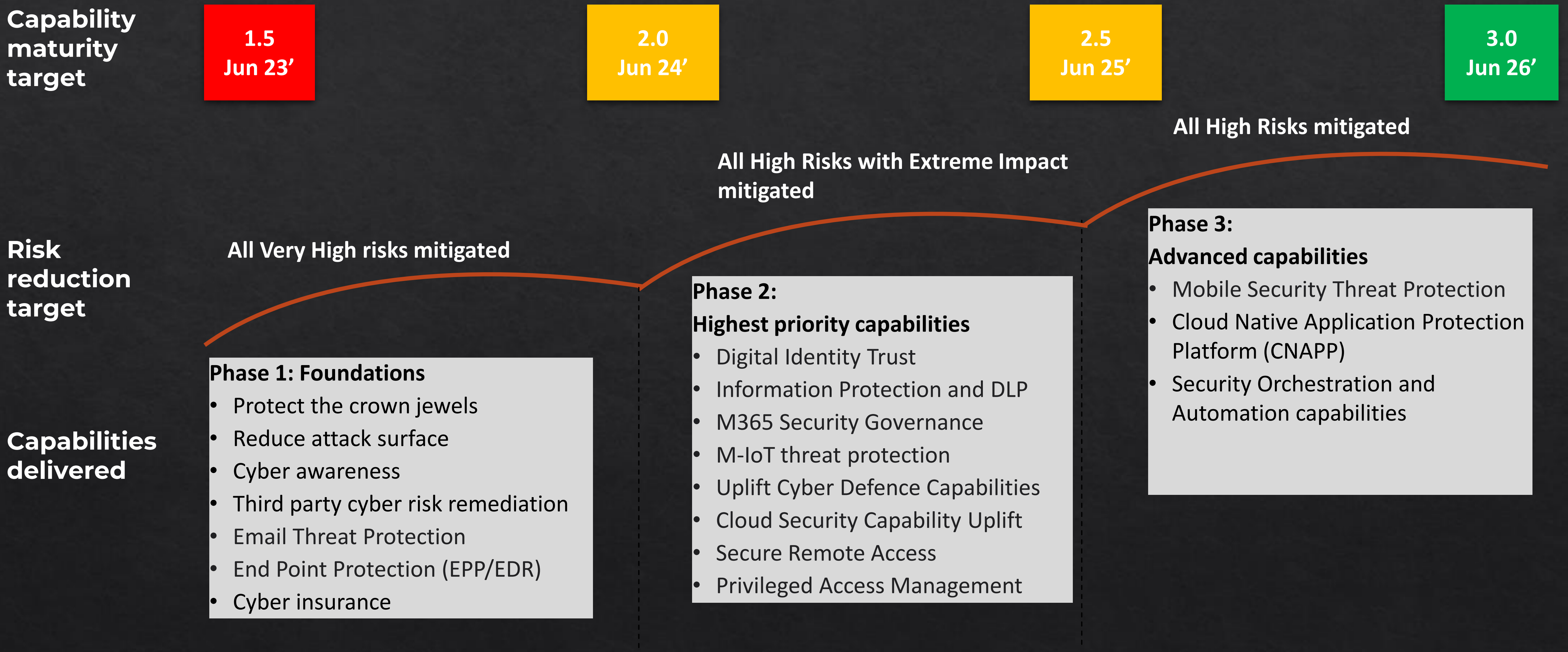
Systems of National Significance (SoNS), there are also four Enhanced Cyber Security Obligations (ECSO).

- Develop cyber security incident response plans to prepare for a cyber security incident.
- Undertake cyber security exercises to build cyber preparedness.
- Undertake vulnerability assessments to identify vulnerabilities for remediation.
- Provide system information to develop and maintain a near real-time threat picture.

You can read more about these additional obligations at Enhanced Cyber Security Obligations.

Cyber Resilience Strategy Roadmap

Progressive uplift of Cyber Resilience Capability and Risk Remediation



Capability maturity target

- 1.5 Jun 23’
- 2.0 Jun 24’
- 2.5 Jun 25’
- 3.0 Jun 26’

Risk reduction target

- All Very High risks mitigated
- All High Risks with Extreme Impact mitigated
- All High Risks mitigated

Capabilities delivered

Phase 1: Foundations

- Protect the crown jewels
- Reduce attack surface
- Cyber awareness
- Third party cyber risk remediation
- Email Threat Protection
- End Point Protection (EPP/EDR)
- Cyber insurance

Phase 2:

Highest priority capabilities

- Digital Identity Trust
- Information Protection and DLP
- M365 Security Governance
- M-IoT threat protection
- Uplift Cyber Defence Capabilities
- Cloud Security Capability Uplift
- Secure Remote Access
- Privileged Access Management

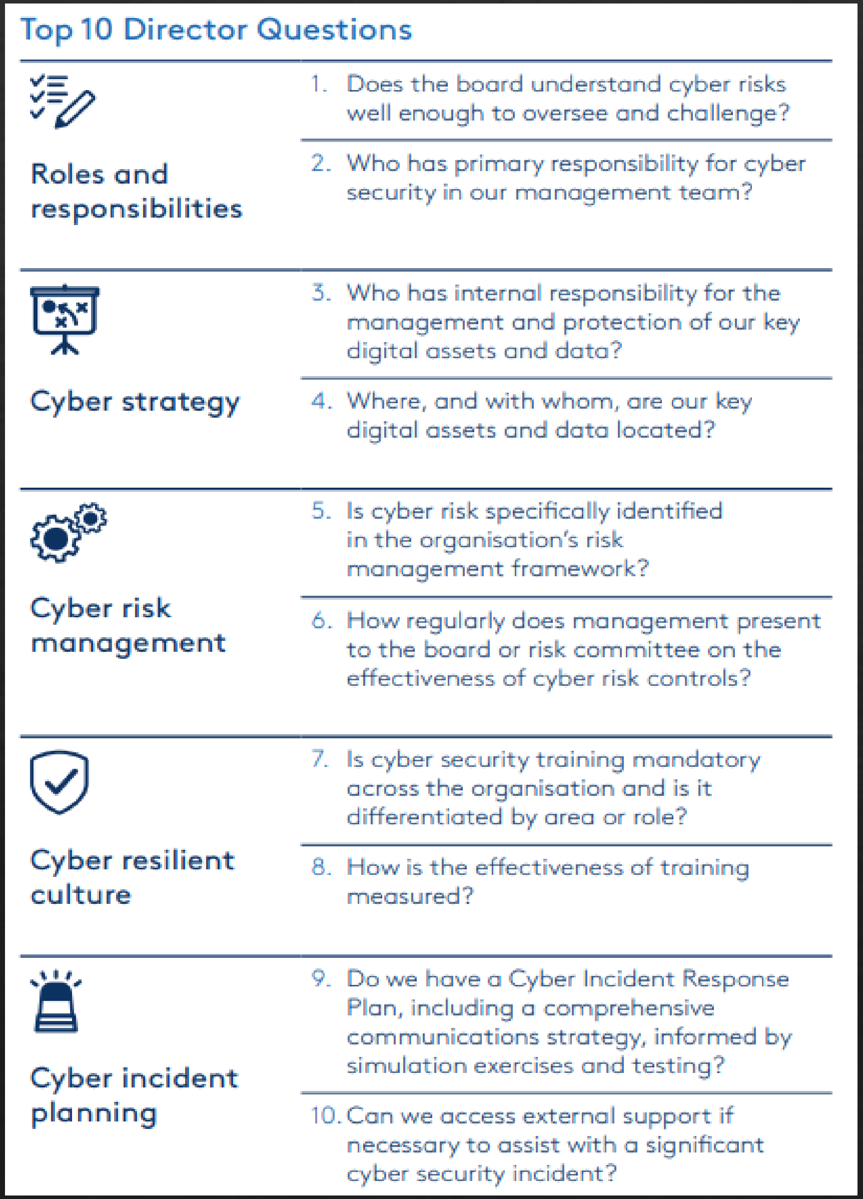
Phase 3:

Advanced capabilities

- Mobile Security Threat Protection
- Cloud Native Application Protection Platform (CNAPP)
- Security Orchestration and Automation capabilities

Board Reporting

Board Reporting – Cyber Security Governance Principles



Top 10 Director Questions

Roles and responsibilities	1. Does the board understand cyber risks well enough to oversee and challenge?
	2. Who has primary responsibility for cyber security in our management team?
Cyber strategy	3. Who has internal responsibility for the management and protection of our key digital assets and data?
	4. Where, and with whom, are our key digital assets and data located?
Cyber risk management	5. Is cyber risk specifically identified in the organisation's risk management framework?
	6. How regularly does management present to the board or risk committee on the effectiveness of cyber risk controls?
Cyber resilient culture	7. Is cyber security training mandatory across the organisation and is it differentiated by area or role?
	8. How is the effectiveness of training measured?
Cyber incident planning	9. Do we have a Cyber Incident Response Plan, including a comprehensive communications strategy, informed by simulation exercises and testing?
	10. Can we access external support if necessary to assist with a significant cyber security incident?

Source: Australian Institute of Company Directors

The Principles will enable directors of all sizes of organisations to ask the right questions of management, spot red flags in how cyber security risk is being managed, promote a culture of cyber security resilience and prepare and respond effectively to significant cyber security incidents

Source: Australian Institute of Company Directors

Publications:
Cyber Security Governance Principals
Cyber Incident Response and Recovery for Australian Directors

Summary

- Ransomware continues to pose a significant risk to organizations. Once inside, the attacker will move around the network, identify the valuable data, and assess the security controls used, often disabling endpoint protection tools, encrypting backups and exfiltrating the data.

Call for action

- Develop *Cyber Resilience capability* to continue business operations despite the cyber incident
    - Network Segmentation and Access Management
    - Identify Attack Surface and Build a Defendable Environment

- Establish *Cyber Recovery capabilities* and procedures beyond the traditional ICT disaster recovery plan
    - Implement air-gapped, immutable backup copies to recover fast from a cyber incident
    - Recover to a sanitised environment

- Simulate *Cyber Incident Response plan for IT and OT* environment

Thank you