

A JOINT PUBLICATION BY

Australian
Institute of
**Company
Directors**



CYBER SECURITY
COOPERATIVE
RESEARCH
CENTRE

Cyber Security Governance Principles

VERSION 2 | NOVEMBER 2024



Contents

Special Envoy's Foreword	4
AICD & CSCRC Foreword	5
Snapshot of the Principles	6
Top 10 director questions	8
Terminology	9
Introduction	10
Threat environment	11
Threat to SMEs and NPFs	12
Existing obligations and regulatory requirements	13
Key directors' duties and obligations	14
Cyber security specific regulatory requirements and standards	15

Principle 1:	
Set clear roles and responsibilities	18
Role of the board	19
Role of management	20
Whole of organisation	21
Board reporting	21
Role of external providers	22
Role of external experts	23
The role of insurance	26
Incident Response Case Study 1: Spirit Super	27
Principle 2:	
Develop, implement and evolve a comprehensive cyber strategy	28
Assessing and enhancing internal capability	29
Opportunities and risks with the use of external suppliers and partners	32
Ongoing evaluation and refinement	33
Director reflections: Third-party supplier risk	34
Incident Response Case Study 2: Ventia Services Group	35
Principle 3:	
Embed cyber security in existing risk management practices	36
Cyber-risk appetite	37
Developing and overseeing controls	37
Key cyber security risk approaches	39
Cyber supply chain risk	41
Director reflections: How to evolve effective cyber risk practices	44
Principle 4:	
Promote a culture of cyber resilience	45
Creating a cyber security mindset from the top down	46
Skills and training	48
Director reflections: A practical cyber security governance framework	50
Principle 5:	
Plan for a significant cyber security incident	51
Preparation	52
Recovery	59
Incident Response Case Study 3: Toll Group	63
Appendix A: Cyber extortion – Ransomware and data theft	64
Appendix B: Resources	67
Appendix C: Industry requirements and standards	69
Appendix D: SME and NFP director checklist	70
Appendix E: Glossary	72

Special Envoy's Foreword

The increasing uptake of digital technology and tools by Australian businesses is already a driver of productivity and economic growth, which will increase exponentially as the nature and use of technology expands.

These economic rewards, however, come with both legal and moral obligations for companies to keep their digital assets safe and secure. Strong cyber security is, and will continue to be, a cornerstone of Australia's digital resilience. This is why the Australian Government's *2023-2030 Australian Cyber Security Strategy (Cyber Security Strategy)* provides a pathway to Australia being a cyber security world-leader by the end of this decade.

A number of legal obligations imposed under various regulatory schemes, reflected in these Cyber Security Governance Principles, create the base-level standard for the cyber security of Australian companies.

However, strong cyber security cannot just be accomplished by regulation alone. Government needs to work together with Australian companies to provide the information, advice and other resources to uplift their cyber security. These Principles provide a path for companies to go beyond minimum compliance to make their best efforts on cyber security and meet their moral obligations to keep their digital assets and customers as safe and secure as possible.

This second edition of the Principles from the Australian Institute of Company Directors (AICD) and the Cyber Security Cooperative Research Centre (CSCRC) provides important updates on how companies can meet their cyber security obligations. Since the first iteration of the Principles was released in 2022 the world has changed

significantly – there have been marked geopolitical shifts that have seen the cyber threat environment alter and evolve. And domestically, there have been shifts too.

We have seen the introduction of the Cyber Security Strategy and associated *2023-2030 Australian Cyber Security Strategy: Action Plan*, a plan to enhance our nation's collective security into the future; the introduction of Australia's first standalone Cyber Security Bill, which proposes world-leading initiatives to counter cybercrime and make Australia a safer place to do business; and the enhanced Security of Critical Infrastructure regime has come online, helping ensure the amenities and services Australia relies upon for economic and social prosperity have adequate cyber security protections in place.

The updated Principles are an invaluable, best-practice guidance for Australian directors navigating this dynamic risk environment, taking into account new opportunities and risks, such as artificial intelligence, cyber-related regulatory and legislative developments, and insights from some of our nation's most experienced corporate leaders.

I commend the AICD and CSCRC for their commitment to keeping these Principles current and fit-for-purpose. By doing so, these Principles provide useful guidance to all Australian businesses to meet and exceed their cyber security obligations.



Dr Andrew Charlton MP
Special Envoy for Cyber Security and
Digital Resilience

AICD & CSCRC Foreword

Australian organisations are more connected than ever before.

Digital systems touch almost every facet of modern business operations, from payroll to production, and are therefore essential to continuity, reputation and efficacy. It is only when these systems become unavailable or compromised that we appreciate the fragility of the highly connected digital ecosystem that underpins modern business. Therefore, for all aspects of business operations cyber security is paramount.

Since 2022, when the AICD CSCRC Cyber Security Governance Principles were first published, much has changed. Australia has seen multiple significant cyber incidents, catapulting cyber security into the spotlight; global conflicts and the evolution of cybercrime have seen pernicious new threats emerge; and Australian regulators have made increasingly clear that organisational cyber security practices and accompanying board oversight will be placed under a microscope.

The cyber security challenge is real and, for directors, increasing in importance and in complexity. Establishing good governance as it relates to cyber security, developing an understanding of what cyber security is and what it does, and keeping abreast of new and emerging threats and risks is vital. Therefore, this update of the Principles is timely.

The first iteration of the Principles have been widely adopted as better practice in Australia and beyond. This update builds on the first iteration, reflecting regulatory and legislative shifts, the evolving threat environment and new case studies and insights from some of the Australia's leading directors.

We are confident the Principles will continue to be a rich source of information and guidance for Australian directors, helping enhance cyber security governance across all organisations, large and small.

We would like to acknowledge and thank AICD staff (Christian Gergis and Simon Mitchell) and CSCRC staff (Anne-Louise Brown) for their hard work to produce these Principles.



Mark Rigotti
Managing Director & CEO
Australian Institute of Company Directors



Rachael Falk
CEO
Cyber Security Cooperative
Research Centre

Snapshot of the Principles

PRINCIPLE 1: Set clear roles and responsibilities

KEY POINTS

1. Defining clear roles and responsibilities is a foundational component of building effective cyber resilience
2. Comprehensive and clear board reporting, including engagement with management and updates on emerging trends, is a key mechanism by which a board can assess the resilience of the organisation
3. External experts can play a role in providing advice and assurance to directors and identify areas for improvement

GOVERNANCE RED FLAGS

1. Cyber risk and cyber strategy not featuring regularly on board agendas
2. Board not annually reviewing skills to ensure that directors have a minimum understanding of cyber security risk
3. Board reporting on cyber risk is hard to digest and features excessive jargon with a reliance on technical solutions
4. Limited or no external review or assurance of cyber risk controls and strategy
5. No clear lines of management responsibility for cyber security

PRINCIPLE 2: Develop, implement and evolve a comprehensive cyber strategy

KEY POINTS

1. A cyber strategy, proactively overseen by the board, can be a business enabler by identifying opportunities for the organisation to build cyber resilience
2. Identifying the key digital assets and data of an organisation, including who has access to these assets, is core to understanding and enhancing cyber capability
3. A robust cyber strategy will account for the importance, and potential risks, associated with key third-party suppliers

GOVERNANCE RED FLAGS

1. Lack of formal documentation of the organisation's approach to cyber security
2. Limited understanding of the location of key digital assets and data, who has access and how they are protected
3. The cyber strategy and risk controls are not subject to internal and external evaluation and periodic refinement relative to evolving threats
4. Lack of data governance framework to guide how data is collected, held, protected and ultimately destroyed

PRINCIPLE 3:

Embed cyber security in existing risk management practices

KEY POINTS

1. Cyber risk is still an operational risk that fits within an organisation's existing approach to risk management
2. While cyber risk cannot be reduced to zero there are a number of accessible and low-cost controls that all organisations can utilise to mitigate the risk
3. The board should regularly assess the effectiveness of cyber controls to account for a changing threat environment, technological developments and the organisation's capabilities

PRINCIPLE 4:

Promote a culture of cyber resilience

KEY POINTS

1. A truly cyber resilient culture begins at the board and must flow through the organisation and extend to key suppliers
2. Regular, engaging and relevant training is a key tool to promote a cyber resilient culture, including specific training for directors
3. Incentivise and promote strong cyber security practices, including participating in phishing testing and penetration exercises

PRINCIPLE 5:

Plan for a significant cyber security incident

KEY POINTS

1. Directors and management should proactively plan for a significant cyber incident
2. Simulation exercises and scenario testing are key tools for the board and senior management to understand and refine roles and responsibilities
3. A clear and transparent approach to communications with key stakeholders in a significant cyber incident is critical in mitigating reputational damage and allowing for an effective recovery

GOVERNANCE RED FLAGS

1. Cyber risk and cyber strategy not reflected in existing risk management frameworks
2. High management confidence that cyber risk controls are effective without regular external validation
3. Over reliance on the cyber security controls of key service providers, such as cloud software providers
4. Cyber security controls and processes of potential vendors are not assessed in the procurement process for key goods and services
5. Prolonged vacancies in key cyber management roles

GOVERNANCE RED FLAGS

1. Board and executives do not undertake cyber security education nor participate in testing
2. Cyber security is not reflected in the role statements and KPIs of key leaders
3. Communication from leaders does not reinforce the importance of cyber resilience to staff (cyber is seen as an issue only for frontline staff to manage)
4. There is a culture of 'exceptions' or workarounds for board and management with respect to cyber hygiene and resilience

GOVERNANCE RED FLAGS

1. The board and senior staff have not undertaken scenario testing or incident simulations to test the Response Plan
2. Likely scenarios and consequences are undocumented with lessons from simulations not being captured
3. It is not clear how communications with key stakeholders will be managed in the event of an incident
4. No post incident review with board and management

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. Do we understand our current cyber security capability and have a plan to enhance this capability?
4. How does our approach to enhancing cyber security support our broader organisational strategy and strategic initiatives?

Cyber security risk management

5. Where, and with whom, are our key digital assets and data located?
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. Does the board and senior management reinforce the importance of cyber security and collective responsibility?

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?



Terminology

The technical language associated with cyber security need not be a barrier to directors governing cyber security risk. While directors should seek to educate themselves on relevant terms and concepts, they should also insist that management and external experts communicate in a clear way that demystifies the topic.

The Australian Signals Directorate (ASD) has comprehensive resources on terminology and key terms that will assist directors in keeping on top of the language of cyber security.

These Principles utilise a common set of terminology to assist directors in overcoming this barrier. This terminology is set out in the following diagram. An extensive glossary is also provided at [Appendix E](#).

Term	Definition
Cyber security	An overarching term that captures the steps, measures and processes used to protect the confidentiality, integrity, availability of data in an organisation's systems as well as protecting the systems themselves.
Cyber resilience	An organisation's posture or ability to defend, adapt, respond and recover from cyber threats and cyber incidents while maintaining continuous business operations. Cyber resilience includes the cyber culture of an organisation and how directors and employees take individual steps to build cyber resilience.
Cyber risk	The potential loss or harm to an organisation from a cyber incident. The loss covers technical systems and infrastructure, use of technology or reputation of an organisation.
Cyber threat	Any potential cyber event, including attack, that has the potential to harm an organisation's information systems and infrastructure.
Cyber incident	An unauthorised cyber security event, or a series of events, with the potential to compromise an organisation's business operations. Cyber incidents cover the spectrum of events from accidental significant data losses to criminal attacks.
Digital	Strategic steps or processes taken by an organisation to enable existing business models by integrating advanced technologies, including internet-facing systems. Data generated via digital strategies is increasingly seen as one of the key assets (and risks) for many organisations.

Introduction

Cyber threats are part of every organisation's risk landscape, particularly as organisations place more of their key assets and systems in internet-facing systems and expand digital-led growth strategies. The cyber threat environment is incredibly dynamic, and boards need to remain responsive to existing and emerging threats and have a good understanding of the cyber resilience of the organisations they govern.

Cyber incidents can have a significant – even existential – impact on an organisation. But their cause can be surprisingly simple. So simple, in fact, that it can be a singular security blind spot, one hacker gaining access to data or an employee misplacing a USB drive. Cyber security system weakness combined with human error often make it relatively easy for cyber threat actors to penetrate IT systems, access valuable data and severely impact an organisation's stakeholder trust and reputation. At its most significant, a cyber incident has the potential to cripple an organisation's operations. This is highlighted in **Incident Response Case Study 3** under **Principle 5**.

It is unsurprising that Australian directors consistently identify cyber security and data theft as the number one issue keeping them awake at night in Director Sentiment Index surveys.

These **Principles** provide a practical framework to help directors, governance professionals and their organisations proactively tackle oversight and

management of cyber risk. The purpose of the Principles is to illustrate what constitutes better practice oversight at the board level. The development of the Principles has been based on extensive consultation and feedback from senior directors, experts in cyber security, regulators and government agencies.

These Principles serve as a reminder to directors to be highly alert to cyber risk, have strong oversight of organisational cyber security risk management, to challenge management on cyber resilience and be well prepared in the event of a significant cyber incident.

Promoting a cyber resilience culture is key and this starts with the board setting the appropriate 'tone from the top'.

The references to legislation and key resources are accurate at the time of the publication in November 2024. However, cyber security obligations are rapidly evolving, and we recommend that readers keep up to date on key changes.

The Principles do not constitute legal advice and are produced as guidance only. The AICD and CSCRC recommend organisations seek independent advice regarding legal, regulatory and technical cyber security matters.

We are interested in hearing from users of the Principles about their experience and invite feedback by email to policy@aicd.com.au

Threat environment

Threat actors in cyber security can be bad-faith employees, individual criminals, issues-motivated groups, criminal syndicates and state-sponsored actors who undertake unauthorised activity on networks, generally for financial or strategic gain. Various typologies of threat actors have been developed, which classify them according to their cyber capabilities, levels of sophistication and motivation. Of these, ‘sophisticated state-based actors’ frequently demonstrate the highest level of scope, skills and resources. However, in recent years the tools created or used by state-based threat actors have also been increasingly available to cybercriminal syndicates. The theft of organisational data, including via ransomware, has emerged as a key cyber threat. Criminal groups steal an organisation’s valuable data and frequently render systems inoperable by encrypting the key data. They then extort their victims, demanding payment for the unlocking of systems and return of data. Ransomware and data theft is discussed in further detail at [Appendix A](#).

AUSTRALIAN TRENDS 2023/24

- Nearly 87,400 cybercrime reports – one every six minutes
- Top three self-reported crime types for business: email compromise, online banking fraud, business email compromise fraud
- The ASD notified critical infrastructure organisations over 90 times about potential malicious cyber activity
- The average self-reported cost of cybercrime for small business increased eight per cent to \$49,600

Source: *ASD Cyber Threat Report 2023–24*

Strategic disruption to critical infrastructure and supply chains remains a prominent target for threat actors, and a particular vulnerability for organisations, with potentially catastrophic effects for the Australian economy and society alike.

Organisations should appreciate that they may become a target for state-sponsored actors, not because of their own relations with a foreign government, but rather due to their strategic significance to Australia, for example as a critical asset owner.

The ASD has drawn particular attention to state-based actors carrying out Living Off the Land (**LOTL**) cyber incursions and activities. LOTL entails a threat actor being present or unobserved on a network and allows the actor to conduct their operations discretely as they can camouflage activity and look like a legitimate user of the network, potentially circumventing basic endpoint security capabilities. LOTL is particularly effective as:

- Many organisations lack effective security and network management practices (such as established baselines) that support detection of malicious LOTL activity. This makes it difficult for network defenders to discern legitimate behaviour from malicious behaviour and conduct behavioural analytics, anomaly detection, and proactive threat hunting.
- There is a general lack of conventional markers of malicious behaviour (known as ‘indicators of compromise’) associated with the activity, complicating network defenders’ efforts to identify, track, and categorise malicious behaviour.

The rapid development and deployment of sophisticated generative artificial intelligence (**GAI**) systems, like large language models (**LLMs**) over the past three years, has also created a range of new AI cyber security threats (**Box 0.1**).

Lastly, a board should also be aware that disgruntled employees and malicious insiders can pose a unique risk since they already have legitimate access to systems and may be intimately familiar with the organisation's security controls and valuable assets. These employees can act in concert with external threat actors and are often associated with the theft of intellectual property.

BOX 0.1: AI cyber threats

Cyber criminals and threat actors are increasingly using AI to enhance and scale their operations. These threats can include the use of synthetic content, such as deep fake visuals and visual cloning, to impersonate customers, external partners or senior management. Therefore, cyber security uplift should occur in lockstep with AI system implementation. The Australian Federal Police (AFP) has identified four key threats posed by AI affecting the criminal environment as:

- more frequent and widespread cyber-attacks, amplifying their impact;
- lowering the entry bar and cost for non-technical people to engage in malicious activities;
- exploitation of human-centric vulnerabilities; and
- deliberate sabotage of critical algorithms.

The AICD suite of resources, *Director's Guide to AI Governance*, developed with Human Technology Institute (HTI) at the University of Technology Sydney, has extensive guidance for directors on the governance of AI.

Threat to SMEs and NFPs



GUIDANCE FOR DIRECTORS OF SMES AND NFPs

- In each of the Principles there is a box highlighting practical cyber security steps for a director of a SME or NFP
- These steps are collated in a checklist **Appendix D**

While small and medium enterprises (**SMEs**) and not-for-profits (**NFPs**) comprise more than 90 per cent of Australian businesses by number, many struggle when it comes to cyber security. This is the result of a multitude of factors, including cost, resourcing and the perceived complexity of the risk.

However, as the economy becomes further digitised, cyber security needs to be a prime consideration for smaller organisations, which are key targets for cyber criminals due to their often-low cyber resilience. SMEs and NFPs, for instance, are frequently a target of low-cost malware or ransomware bots that scan the internet and networks identifying security gaps or weaknesses.

For a smaller organisation a cyber-attack can be crippling, impacting IT systems, websites, customer data and payment systems, severely impeding business continuity.

GOVERNING THROUGH A CYBER CRISIS

In February 2024 the AICD, in partnership with the CSCRC and Ashurst, published a new resource *Governing Through a Cyber Crisis*.

This resource builds off the guidance in the Principles and assists boards and directors with overseeing the effective response and recovery from a material cyber incident and emerge on the other side with a more cyber resilient organisation.

The resource is available [on the AICD website](#).

Existing obligations and regulatory requirements

Governing for cyber risks and building an organisation's cyber resilience forms part of directors' existing fiduciary duties owed to the company under both common law and the Corporations Act 2001 (Cth) (**Corporations Act**).

The AICD practice statement *Directors' oversight of company compliance obligations* and supporting legal opinion, published in October 2024, provides a valuable starting point for directors in understanding their duty of care and diligence. This duty is central to how a board oversees non-financial risk, including cyber security risk.

The next page provides a broader overview of the key duties and obligations that a director should be aware of in the oversight of cyber security risk and resilience.



Key directors' duties and obligations

DUTY TO ACT WITH CARE AND DILIGENCE

Directors have a duty to act with care and diligence to guard against key business risks. This includes being satisfied that appropriate systems are in place to bolster cyber resilience, as well as prevent and respond to cyber incidents.

DUTY TO ACT IN GOOD FAITH AND IN THE BEST INTERESTS OF THE CORPORATION

Directors must exercise their powers and discharge their duties in good faith in the best interests of the company, and for a proper purpose. In making decisions on cyber security on behalf of the company, directors must consider the impact of those decisions on shareholders/members and stakeholders including employees, customers, suppliers and the broader community.

RELIANCE ON INFORMATION AND ADVICE PROVIDED BY OTHERS

Just because a director does not have specialist knowledge about cyber security does not mean that the director's standard of care is reduced.

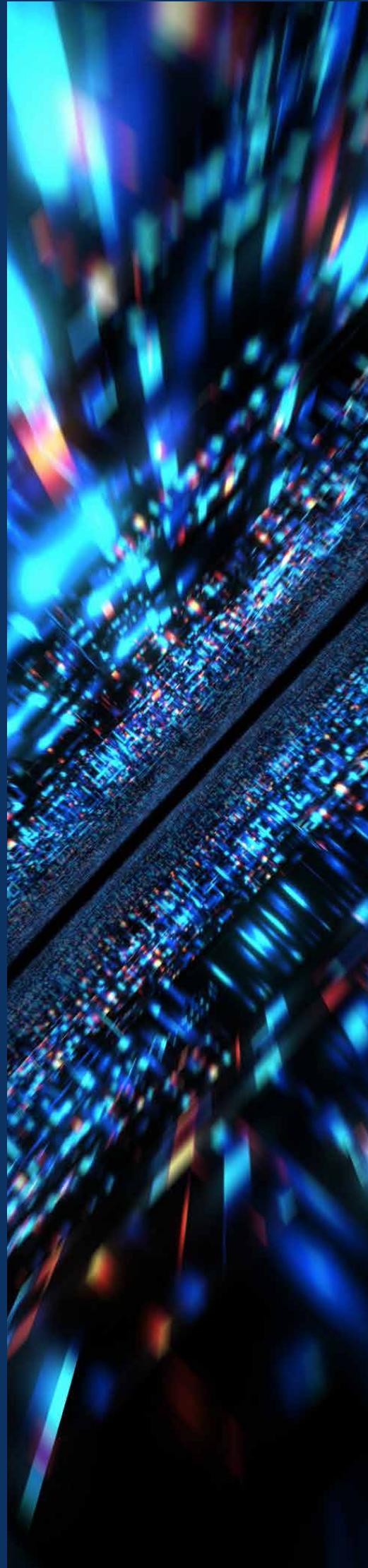
While in some circumstances, directors may rely on information or the advice of others, or delegate certain cyber matters to a board committee or management roles, this does not absolve directors of their accountability for decision-making.

OTHER STATUTORY OBLIGATIONS AND OTHER REGULATORS

Directors of entities that hold an Australian Financial Services License (AFSL) are also subject to general and specific obligations under the Corporations Act. The Federal Court of Australia consent orders in ASIC v RI Advice, confirmed this includes having in place risk management systems and controls to manage business risks. APRA regulated entities are also subject to extensive prudential obligations relevant to cyber security risk.

CONTINUOUS DISCLOSURE

For companies listed on the Australian Securities Exchange (ASX), directors must advise the market immediately if the company becomes aware of any information would have a material effect (positive or negative) on the company's share price. In the cyber context, this might apply in the event of customer data loss as a result of a significant cyber incident. This type of event may also expose a company and/or its directors to the risk of a class action.



Cyber security specific regulatory requirements and standards

Australian organisations are subject to a range of regulatory requirements and standards that are relevant to the governance of cyber risk and management of data. Depending on the industry, these obligations can be overlapping and complex.

The Department of Home Affairs' Cyber and Infrastructure Security Centre (**CISC**) publication *Overview of Cyber Security Obligations for Corporate Leaders* is a key source of information for directors in understanding cyber security relevant obligations.

Below is a high-level summary of key regulatory frameworks relevant to a board's oversight of cyber security and data management.

PRIVACY ACT

The *Privacy Act 1988 (Cth)* (**the Privacy Act**) – with its focus on how organisations collect, manage and dispose of personal information is a legislative framework relevant to the governance of cyber security.

Two regimes under the Privacy Act that directors should be aware of are:

- 1. Notifiable Data Breaches (NDB) scheme:** requires an organisation to notify affected individuals and the Office of the Australian Information Commissioner (**OAIC**) as soon as practicable of a material data breach.
- 2. Australian Privacy Principle 11: Security of Personal Information (APP 11)** – requires an organisation to take active measures to ensure the security of personal information it holds.

As detailed in **Table 1**, the Privacy Act is currently subject to reform.

OAIC V MEDIBANK PRIVATE LTD

In June 2024 the Office of the Australian Information Commissioner (OAIC) commenced civil proceedings against Medibank Private Ltd (Medibank) arising from an October 2022 data breach that impacted 9.7 million current and former customers.

The OAIC alleges that Medibank seriously interfered with the privacy of these customers by failing to take reasonable steps to protect their personal information from misuse and unauthorised access or disclosure in breach of the Privacy Act. Under Australian Privacy Principle 11 (Security of personal information) Medibank is required to take reasonable steps to protect the personal information it holds from misuse, interference and loss, as well as from unauthorised access, modification or disclosure.

The OAIC concise statement of claim for these proceedings alleges that in the context of Medibank's size, complexity and resources, it failed to implement appropriate cyber and data protection measures. These measures include allegedly not implementing internal multi-factor authentication at key high risk points, such as accessing sensitive information, implementing privileged access management controls that are monitored and regularly reviewed, and implementing password complexity requirements that are monitored and regularly reviewed.

In forming this view on appropriate measures for a business the size of Medibank, the OAIC cites the ASD Essential Eight, APRA Prudential Standard CPS 234 Information Security and the NIST Cyber Security Framework.

The OAIC claims before the court serve as an example of heightened regulator focus in Australia on cyber security and data governance and signal the cyber risk controls that are expected of large organisations.

Medibank is defending the OAIC allegations.

CRITICAL INFRASTRUCTURE

The *Security of Critical Infrastructure Act 2018* (Cth) (**SOCI Act**) applies to owners of critical assets in 11 key industry sectors and 22 distinct asset classes, imposing significant cyber risk management and reporting obligations – including a requirement for directors to annually attest that the organisation's risk management practices are up to date. Additionally, the SOCI Act provides the government with the ability to exercise significant directions and/or intervention powers where an asset owner is unwilling or unable to respond effectively to a significant cyber incident.

Smaller organisations may be indirectly impacted by the SOCI obligations by virtue of being in the supply chain of a SOCI entity.

APRA PRUDENTIAL REQUIREMENTS

Australian Prudential Regulation Authority (**APRA**) prudential requirements apply to banks, insurance companies and superannuation trustees. These requirements can also have a broader normative impact on Australian businesses through setting a benchmark for strong governance and risk management practices in key areas.

In cyber security, prudential standards CPS 234 *Information Security* (**CPS 234**) and CPS 230 *Operational Risk Management* (**CPS 230**) and the supporting guidance to these standards set key principles on the governance of cyber security risk, which can also assist across other sectors.

CPS 230 focuses on operational risk management and requires entities to maintain appropriate operational risk management frameworks. It sets a framework that assists a board identify, assess, and mitigate operational risks, including those related to information and cyber security.

CPS 234 mandates robust information security capabilities, including requiring regular testing and assurance of information security controls and oversight of the risk controls of material third-party suppliers and the key vendors of these third parties. It also emphasises the need for clear accountability and governance of information security.

For all organisations these standards and guidance provide a structured approach to managing information and cyber security risks, promote board-level engagement in cyber security matters and expect a culture of continuous improvement in cyber security and operational risk.

PENDING CYBER SECURITY & PRIVACY LEGISLATION

At the time of publication, the Federal Government has legislation before Parliament that would introduce specific standalone cyber security obligations in Australia. The reform package would also amend the SOCI Act. The key measures are outlined in **Table 1**.

The Department of Home Affairs has committed to publishing guidance materials to assist industry with understanding their obligations should the legislation be passed.

The Government has also introduced legislation to amend the Privacy Act. This is the first tranche of legislation to enact the proposals of the multi-year Privacy Act Review. The legislation would boost the powers of the OAIC, introduce new low and mid-tier penalties for a breach of the Privacy Act, require greater transparency of automated decision-making and introduce a statutory tort for privacy.

These Principles will be updated to reflect this legislation if, and when, they are passed by Parliament.

TABLE 1: Pending cyber security and critical infrastructure reforms

Reform	Detail
Cyber Security Act	
1. Mandatory cyber security standard for consumer-grade smart devices	Apply mandatory security standards on consumer Internet of Things devices consistent with international settings.
2. Ransomware payment reporting regime	An entity would report to Government if it makes a ransomware or extortion payment. The reporting obligation would apply to organisations above a certain revenue threshold (likely to be \$3 million as of November 2024).
3. Limited use obligation on the ASD and the National Cyber Security Coordinator (Coordinator)	The obligation restricts how cyber incident information, shared by victim organisations with the ASD and the Coordinator, is used by other Australian Government entities, including regulators.
4. Cyber Incident Review Board (CIRB)	Establish a CIRB (modelled off the Cyber Safety Review Board in the US) that would conduct no-fault, post-incident reviews of selected cyber incidents to enable root cause to be shared more widely across industry and relevant stakeholders.
SOCI Act	
5. Data storage systems and business critical data	Include data storage systems holding ‘business critical data’ in the definition of ‘asset’ under section 5 of the SOCI Act and separately amend the risk management rules to include risks to data storage systems holding ‘business critical data’ and the systems that access the data as ‘material risks’.
6. Consequence management powers	Additional powers for the Minister for Home Affairs to step in and direct a SOCI entity to do certain things associated with the consequence management of a critical asset incident.
7. Information sharing provisions	Amend the protected information framework to better support industry and enable a more agile response to attacks.
8. Risk management review and remedy powers	New directions power for the Secretary of Home Affairs where an entity can be directed to address seriously deficient elements of a risk management program.
9. Consolidating telecommunication security requirements	Consolidate security regulation for the telecommunications sector and bring this under the SOCI Act.

PRINCIPLE 1:

Set clear roles and responsibilities

KEY POINTS

1. Defining clear roles and responsibilities is a foundational component of building effective cyber resilience
2. Comprehensive and clear board reporting, including engagement with management and updates on emerging trends, is a key mechanism by which a board can assess the resilience of the organisation
3. External experts can play a role in providing advice and assurance to directors and identify areas for improvement

Role of the board

From the board's perspective, clearly defined roles and responsibilities assist directors in having effective oversight of cyber risk.

Irrespective of how large or resourced an organisation may be, the fast-paced and evolving nature of the cyber threat landscape will always present uncertainty for an organisation's operating environment, including staff and supply chains. As a result, directors need to become accustomed to accepting a certain level of ambiguity surrounding their organisation's cyber resilience.

While it is not the role of the board to directly manage cyber risk, the board does have ultimate accountability for how risks are governed and addressed. This includes being satisfied there are appropriate processes and delegations in place that provide directors with effective oversight of the actions of management.

The governance structures and allocation of roles and responsibilities when it comes to governing cyber security will vary by the size and nature of the organisation.



BOX 1.1: SMEs and NFPs – Roles and Responsibilities

- Document where possible who has responsibility for cyber security
- Appoint a cyber 'champion' to promote cyber resilience and respond to questions
- Consider whether a director, or group of directors, should have a more active role in cyber security oversight
- Identify our key digital providers and understand their cyber controls

At large organisations, the board may assign closer oversight of cyber security governance to a sub-committee of the board, such as the risk committee, audit committee or a technology committee. However, the dynamic and rapidly changing nature of cyber security, and the potential severity and velocity of the risk, may warrant cyber security being discussed

regularly at full board meetings. For example, as a standing item on IT infrastructure, digital initiatives or a component of risk or strategy. Board and committee charters should also be reviewed regularly to confirm that roles and responsibilities are clear, especially with respect to evolving risks such as cyber security.

This may necessitate joint meetings of relevant board committees where aspects of cyber oversight are split (e.g. cyber risk management may sit with the risk committee but technology and systems investment and maintenance lie under a technology committee).

Key to effective oversight of cyber risk is the board receiving regular reporting and engagement with management (discussed further below).

The delegation of cyber risk management or strategy to board committees, and ultimately management, should be detailed not only in the charter or governing documents of the respective committee, but also the organisation's overarching cyber strategy or policy.

To support the board's role in oversight and allow constructive challenge of management, directors should be equipped with appropriate skills and understanding of cyber risk. The importance of director training and upskilling on cyber is discussed at **Principle 4**. That said, directors should remember that the simplest questions are often the ones that are never asked – they should not be afraid to raise these with management. Equally important is the board seeking assistance from third-party experts, including external assurance and testing (detailed below).

Ultimately, one of the key roles directors can play in fostering a cyber resilient culture within the organisation is modelling effective cyber practices (discussed at **Principle 4**). Every director should take responsibility to enhance their own skills and knowledge on cyber security.

Boards may obtain insight in speaking to chairs/directors from other organisations with greater cyber sophistication (for example those that are APRA-regulated or critical infrastructure providers) to learn from their approach. This may be especially helpful where an entity has faced a major cyber incident and is willing to share their lessons learnt.

Role of management

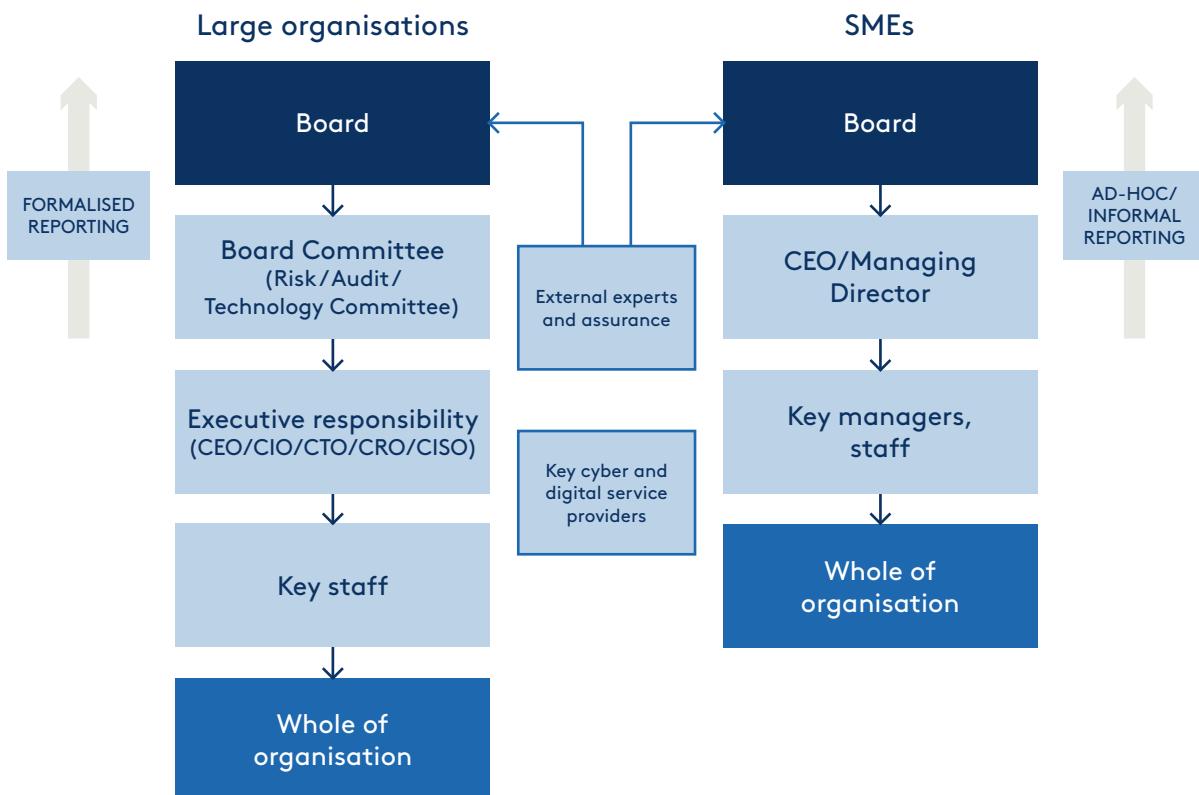
There is no strict rule on where responsibility for cyber security leadership should sit at the management level. As discussed in **Principle 4**, ultimately, cyber security is the responsibility of everyone in an organisation.

Direct management responsibility for cyber security must ultimately lie with the person who best understands cyber security, the threat landscape and the organisation's strategy and approach to mitigating risk. At large organisations, in some cases it may be appropriate for either the Chief Information Officer (**CIO**), Chief Technology Officer (**CTO**), Chief Information Security Officer (**CISO**) or Chief Risk Officer (**CRO**) to have responsibility for cyber security. In some cases, it may be appropriate for responsibility to be shared across key management personnel, for example the CRO and CIO. At smaller organisations, the Chief Executive Officer (**CEO**) may play a more hands-on role.

Regardless of who is allocated direct responsibility, it is critical that building the cyber security resilience of the organisation is central to all senior executive roles and responsibilities. It should be considered a shared enterprise risk and responsibility across the full executive team.

At larger organisations, responsibilities are cascaded from management through the organisation to particular individuals (**Figure 1**). In these circumstances, individual cyber responsibilities should be documented in position descriptions or role statements. Depending on the nature of the organisation it may be appropriate for each senior executive to have cyber security as a component of their responsibilities related to their business unit or division. To ensure that responsibilities remain current, there should be established processes to update responsibilities, including reflecting changes in the organisational structure or new information technology investment.

FIGURE 1: Cascading cyber security responsibilities at large organisations and SMEs



Internal audit may also have a role in providing assurance on the effectiveness of cyber security controls.

Where appropriate, key performance measures and components of variable remuneration may be linked to cyber resilience measures. Where this is the case, the board has a key role to play in setting appropriate incentives and a transparent framework for monitoring management's progress.

SHARED RESPONSIBILITIES

A challenge at many organisations is that core cyber security roles and responsibilities may be dispersed across different business areas or teams. For example, while the IT team may be responsible for maintaining IT equipment and software, a customer-facing team may have responsibility for how customer information is collected, stored and shared. Where responsibility is blurred or unclear it can result in a lack of ownership, ineffective oversight, and a weakening of the defences of the organisation to a cyber security incident.

The use of maps or other visual aids, as well as scenario testing or workshops on key cyber issues, may help staff better understand where responsibility for cyber sits across an organisation. The use of accountability maps and statements is utilised by APRA-regulated entities to meet Financial Accountability Regime requirements. These processes may also be useful for other organisations in defining and allocating responsibility for cyber security.

Additionally, a working group of key staff that meet regularly to discuss cyber risks and developments may be an effective ongoing mechanism to ensure coordination across different teams.

For most small organisations, formalised documentation of responsibilities for cyber security may not be necessary (exceptions would include organisations in certain industries, such as critical asset operators, health care or financial services). However, it is nonetheless essential that individuals within the organisation have a clear understanding of what is expected of them in terms of their contribution to organisational cyber resilience.



BOX 1.2: Questions for directors to ask

1. Do we understand cyber risks well enough to oversee and challenge?
2. Who has primary responsibility for cyber security in our management team?
3. Do we need a board committee to formally oversee cyber security governance?
4. What happens to cyber security risk responsibilities and management when key staff leave?
5. Are we insured for cyber risks, and do we understand our coverage and gaps?

Whole of organisation

Fundamentally, all staff members and key partners have a responsibility to enhance the cyber resilience of the organisation. This requires a whole-of-organisation approach to being vigilant to cyber threats, undertaking training and education, ensuring there is a cyber incident response plan, and that key defences, such as software updates, MFA and password security, are robust and up to date.

Building and promoting a culture of cyber resilience across an organisation is covered in detail in [Principle 4](#).

Board reporting

Robust board reporting on cyber security is a key tool by which directors will obtain insight into how controls, processes and the organisation's staff are contributing to the organisation's cyber resilience. Reports should be regularly presented by management and discussed at the board and/or board committee.

Reporting should align with the organisation's cyber strategy or policy and capture metrics that go beyond key measurable data points (e.g. anti-virus incidents) and traffic lights. Reports to the board should provide rich information about the internal and external threat environment, (e.g. risk management outcomes and broader cyber threats or developments relevant to that organisation). Trend data provides particular insight for directors.

At larger organisations, information may be presented as a series of dashboards or heatmaps that allows a holistic picture of the organisation's cyber posture and risk profile.

Directors should expect that board reporting is presented without complex technical language that may act as a barrier to assessing cyber risk and engaging with management.

BOX 1.3: Common board reporting metrics

Trend data, where available, is key to insightful board reporting:

- Cyber incident detection, prevention, and response, including incident trend analysis
- Cyber strategy performance, key initiatives, and progress to date
- Staff-related incidents, such as staff accessing or misusing data in breach of policies
- Internal audit activities, including outcomes of vulnerability and threat assessments
- External party assessments, including penetration testing results and benchmarking against peers and international standards
- Staff cyber training rates and completion
- Phishing exercise results
- Assessment of the broader threat environment, informed by vendor alerts, ASD alerts, intelligence shared by other organisations, and responses to threats

Role of external providers

Increasingly, organisations of all sizes use external providers to provide core business services and process and store key data. For example, the software and IT infrastructure of Software as a Service (**SaaS**) are commonly used to facilitate payment and invoice processing, internal payroll, accounting services, customer databases and word-processing software. SaaS providers will, in turn, utilise large cloud providers to host and store systems and data.

Documented roles and responsibilities should capture the key third-party suppliers and partners who support or manage the organisation's essential assets and data. An important consideration is the degree of dependency on a particular supplier and the role this supplier plays in the overall cyber security resilience of the organisation.

A board should also be aware that, generally, regulatory obligations hold the organisation itself responsible for failings of the supplier or vendor (i.e. an organisation cannot claim it was not at fault due to a failing of a contractor or supplier). Similarly, customers and other stakeholders expect organisations to effectively manage their supply chain.

Directors should have confidence that management, and the organisation more broadly, has the appropriate internal capabilities and risk-management processes in place to understand the role of key suppliers. The resilience of the organisation can be materially determined by the strength or otherwise of the cyber risk controls of the key suppliers.

Due diligence processes are critical in appointing and monitoring key external providers to ensure confidence that they are meeting contractual obligations and expectations around cyber security. To assist the board in overseeing the roles and responsibilities of key providers, the organisation should consider the following actions:

- Create and maintain a Supplier Classification Matrix categorising suppliers based on criticality and type of service/product provided. Categories should cover data storage and processing, software services and hardware providers;

- Create and maintain a service level agreement overview document that summarises key cyber responsibilities and metrics for each critical supplier, highlighting key responsibilities of the supplier and any shared responsibilities between the supplier and the organisation;
- Data flow diagrams: map how key data moves between the organisation and suppliers, including identification of controls and who access to data;
- Security control visualisation: map which security controls are implemented by suppliers versus internally with the goal of highlighting gaps or any overlaps; and
- Technology stack diagrams: highlights where each supplier's technology and services fits into the organisation's overall IT/digital architecture, including highlighting integration points and potential vulnerabilities.

Principle 3 provides further guidance on how a board can oversee risk in the cyber supply chain and put in place risk controls relevant to external vendors.

ROLE OF THIRD PARTIES IN A CYBER INCIDENT

Key suppliers and vendors are often critical to how an organisation prepares for and responds to a critical cyber security incident. Roles they can play include incident detection, threat analysis and eradication, system workarounds, repair and recovery.

The board-approved incident response plan should cover the role of these suppliers during a critical incident response, recovery and remediation phase, and how this is reflected in service agreements and contracts. The plan, and supporting documentation, should go down to the detail of having up-to-date contact details for key staff within the suppliers. The board should also be aware that service providers may impose additional charges when providing support during an incident response.

As discussed in greater detail in **Principle 5**, the Government through the ASD and Coordinator and industry specific regulators are often key third parties to a cyber incident. In addition to an organisation meeting its reporting and notification obligations, these bodies can provide support and advice to impacted entities.

Further guidance on preparing for a critical cyber incident is covered in **Principle 5** and in detail in *Governing Through a Cyber Crisis*.

Role of external experts

Given the board imperative to monitor and stay across evolving cyber risks and key capabilities, there can be a key role for independent external experts to provide an outside perspective. In the event of a cyber incident, external experts can be a valuable source of assistance for an organisation's immediate response and recovery. For large organisations, the board may want an external expert to report directly to the board. This step can assist the board obtain a more transparent view on the cyber security settings of the organisation, including the progress of management in addressing vulnerabilities.

That said, organisations should be cautious about being too reliant on external experts given the materiality of the risk to many organisations. Management capability uplift is critical, alongside education of directors to support their oversight function.



EXTERNAL AUDIT AND BENCHMARKING: COMPLIANCE DOES NOT EQUAL SECURITY

Independent experts can provide assessments of an organisation's risk management controls, and how they measure up across international standards frameworks (e.g. National Institute of Standards and Technology (NIST), International Standards Organization (ISO) 27001). This information provides the board with an understanding of the organisation's cyber risk maturity, which is an important input for developing the organisation's cyber risk strategy and cyber risk controls. It can also provide directors with a useful benchmark against the organisation's industry peers.

BOX 1.4: Key standards frameworks

The following table summarises key international standards frameworks that organisations utilise to build cyber security and data resilience and undertake reporting and benchmarking. Directors are not expected to have deep technical knowledge of each.

ISO 27001

Specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system

NIST Cybersecurity Framework

Provides a flexible, risk-based approach to managing cyber security risk across five core functions: Identify, Protect, Detect, Respond, and Recover

ISO 38500

A framework for effective governance of IT within organisations, defining how leaders should evaluate, direct, and monitor the use of information technology to ensure its alignment with overall business objectives and strategies

Essential Eight

Developed by the ASD it contains eight core mitigation strategies aligned to maturity levels and mitigate increasing levels of threat actor tradecraft

However, while compliance to a particular industry standard is important, it should not be misunderstood as placing an organisation in a sound position to defend attacks or a cyber incident. Compliance to an industry standard is just one part of a cyber strategy.

For some organisations it may be appropriate for an assessment of cyber resilience, including the performance of the cyber strategy, to be a component of the periodic audit program.

Factors that can be assessed within external cyber audit and benchmarking include:

- **Regulatory and standards compliance:** Does the organisation meet its domestic legal and regulatory requirements? Is data or information covered under privacy provisions stored appropriately? How does the organisation align or compare to key standards frameworks?
- **Data stocktake and access:** What is the key data that the organisation collects and stores? Who, and what partners, have access to this data? Is data or information stored appropriately and consistent with regulatory obligations? Does the organisation regularly undertake a thorough data stocktake and question whether all information needs to continue being held? Is there an overarching data governance strategy?
- **Technical compliance:** What software systems are used and how are they kept up to date? Is there a process for safely disposing of legacy systems and all data? Are there authentication systems in place? What controls ensure third parties cannot access internal systems without appropriate security measures? Are there logs for key systems so there is a record of who has accessed what data?
- **Continuous improvement:** Do core security measures align with best practice? Are there systems in place to deal with the contemporary threat landscape?

- **Awareness of threats:** What alerts or monitoring is in place to flag threats and breaches or respond to critical patching alerts? Are staff trained to respond appropriately and in a timely way?
- **Governance and strategy:** What are the systems and processes in place to manage and mitigate risk, or respond to threats or real events? How do individual responsibilities fall to each team? What approvals would they require, and to whom would they report?
- **Overall risk assessments:** How does the level of resilience across the organisation compare against industry peers in the context of alignment with standards and testing results? How does this resilience and risk posture align with the risk appetite and cyber strategy of the organisation?

BOX 1.5: Governance red flags

1. Cyber risk and cyber strategy not featuring regularly on board agendas
2. Board not annually reviewing skills to ensure that directors have an appropriate understanding of cyber security risk
3. Board reporting on cyber risk is hard to digest and features excessive jargon with a reliance on technical solutions
4. Limited or no external review or assurance of cyber risk controls and strategy
5. No clear lines of management responsibility for cyber security

The role of insurance

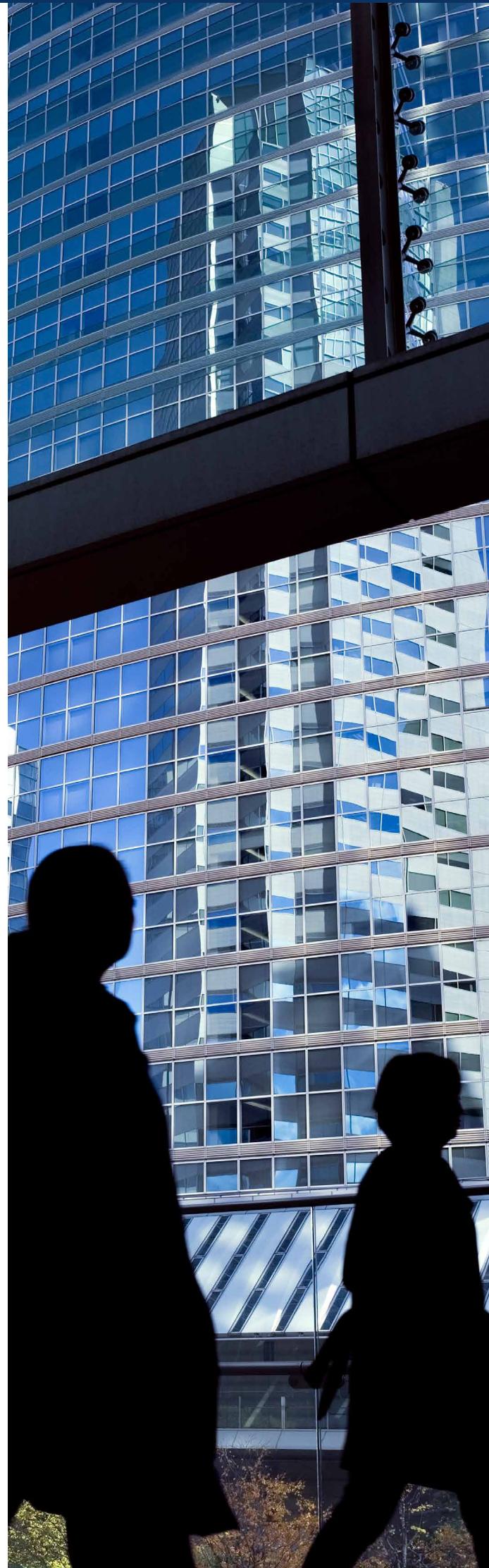
Organisations have the option of obtaining cyber insurance, which can provide a measure of protection in the event of a critical cyber incident. The board should carefully consider whether cyber insurance is appropriate for their organisation, accounting for the nature and scope of the coverage and the cost. It is also common for there to be a requirement to hold cyber insurance in certain procurement contracts, for example with Government agencies. Engagement with brokers can provide useful advice on the state of the market.

Prior to issuing a cyber insurance policy it is common for insurers to seek detailed information on an organisation's cyber posture and procedures. This underwriting process can be useful for organisations to assess their current resilience levels, as the questions asked by brokers/insurers will sometimes reveal previously unknown vulnerabilities.

In addition to financial compensation, often a key driver for holding a cyber insurance policy is access to expert advice and assistance in the event of a significant cyber incident. Either the insurer, or specific industry experts engaged by the insurer, will assist an organisation in the immediate response and recovery phase of a significant cyber incident.

There are often no standard terms and conditions for cyber policies. Therefore, directors should be aware of what is covered, including excluded events (e.g. a ransomware attack from a state-sponsored actor), and what assistance an insurer may provide in the event of a significant cyber incident. The board should also understand the level of protection provided under other insurance policies (e.g. business interruption), as it is common for these policies to exclude cyber-related claims.

The board should closely assess whether a cyber insurance policy provides sufficient mitigation from financial loss and access to support in the event of a cyber incident, relative to the cost. A board may form the view that in certain circumstances self-insurance is appropriate and choose to deploy the savings from not obtaining the policy to boosting cyber security controls.



INCIDENT RESPONSE CASE STUDY 1: Spirit Super

It only took one email. In May 2022 the email account of a single employee from Spirit Super was compromised through a sophisticated, but untargeted, phishing attack. Despite Spirit Super having multi-factor authentication and comprehensive cyber security training, the attacker was able to gain access to the mailbox. It set off a ripple of events that impacted the Australian superannuation trustee's members and sparked a rethink of its cyber defences. Cyber experts were critical to the handling of the incident, from discovering the extent of the data breach through to containing it.

For then Spirit Super Independent Chair Naomi Edwards, the incident highlighted the importance of sensitive data management and the specialist assistance of cyber experts.

"It was a cyber incident that was compounded by a weakness in the handling of sensitive information," she said.

"Even though we did all the things a board should do - overseeing the cyber strategy, setting the risk appetite, approving the policy framework, and monitoring our controls - it only takes a momentary lapse in a person's concentration. Then once they [the hackers] are through, it's all about how many layers of defences you have."

The company detected the breach quickly. Internal teams executed their technical incident response playbooks to isolate and contain the impact. As that happened, the board implemented its cyber incident plan, including advising key regulators. Transparency is key to member trust – so emails, SMS and letters were issued promptly advising them of the possibility their personal information was accessed.

Assistance was provided, included standing up a contact centre over the weekend and introducing personalised support for impacted members. In line with the plan, the board also called in external forensic experts to provide additional support to the Technology team. Unfortunately, they uncovered further sensitive information in the staff member's mailbox.

"With their specialist knowledge and toolsets, they were able to identify additional personal information that could potentially have been accessed," she said. "They had more technical ability in this area than we can resource internally. We did the right thing to have that on the plan, to have the third parties come in."

Ms Edwards said Spirit Super had only recently refreshed its cyber strategy and was investing in enhanced technologies and controls. But there was more to do, especially on how to safely handle the large volumes of sensitive information that staff must work with to fulfil their roles.

In addition to assisting with cyber incident response, Spirit Super also utilised independent experts to advise, review and test their cyber defences.

"The assessments conducted by experts are vital," she said. "They force you to put that list together and to understand their roles and when they need to be brought in. When you have an incident, you can refine the action plan from your learnings."

Provided by Naomi Edwards FAICD, former Chair of Spirit Super. Ms Edwards is the current Chair of the AICD, director of TAL, Propel Funeral Partners and Yarra Funds Management.

PRINCIPLE 2:

Develop, implement and evolve a comprehensive cyber strategy

KEY POINTS

1. A cyber strategy, proactively overseen by the board, can be a business enabler by identifying opportunities for the organisation to build cyber resilience
2. Identifying the key digital assets and data of an organisation, including who has access to these assets, is core to understanding and enhancing cyber capability
3. A robust cyber strategy will account for the importance, and potential risks, associated with key third-party suppliers

Assessing and enhancing internal capability

A cyber strategy is a plan for an organisation to enhance the security of its key digital assets, processes and people over time. An organisation's cyber strategy will be informed by the size and complexity of the organisation; its information technology infrastructure and systems; its key personnel and core competencies; the type and nature of information it holds; and stakeholder expectations, including regulatory and contractual obligations.

A further essential input is the organisation's cyber-risk appetite and controls, discussed in **Principle 3**, which will influence the choice of strategic options with respect to enhancing cyber resilience, including operating and capital investments.

Suggested key components of a cyber strategy are highlighted in **Box 2.1**. The discussion of these elements is covered in different sections of the Principles, with the relevant principles highlighted in the box.

A core element of a comprehensive cyber strategy is how an organisation will respond to a significant incident, including communicating with affected customers. This is discussed in detail in **Principle 5**.

A cyber strategy should be considered a 'living document' which the board receives regular updates on and reviews periodically.

For many SMEs and NFPs, a lengthy cyber strategy may be unnecessary and act as a barrier to nimble responses to cyber threats. However, for smaller organisations in industries such as healthcare or those that provide services to larger organisations, a documented cyber strategy will often be prudent. For these organisations the strategy will assist to ensure they comply with regulatory obligations relevant to the industry and/or demonstrate to partners how they are maintaining and enhancing cyber resilience, rather than being a weak link in the supply chain.

BOX 2.1: Key components of an effective cyber strategy

1. Governance arrangements

Promote effective governance of cyber security that is appropriate for the size and complexity of the organisation (**Principle 1**)

2. Identify and protect

Identify the key digital assets and data held by the organisation and how to comprehensively protect them (**Principle 2** and **Principle 3**)

3. Assess and enhance

Understand internal cyber capability, create a plan to enhance capability and promote a cyber resilient culture (**Principle 2** and **Principle 4**)

4. Detect, respond and recover

Have plans and processes to detect cyber incidents and respond and recover effectively (**Principle 5**)

5. Monitor and evaluate

Report and update the board to allow for ongoing assessment and refinement of the strategy (**Principle 2**)

INTERNAL CAPABILITY AND MATURITY

An equally important component of a cyber strategy is the assessment of the organisation's internal cyber capability and maturity. An accurate understanding of key personnel competencies, reporting chains, responsibilities and the IT infrastructure essential for business operations (for example, databases, servers and cloud software), provides the board with an overview of cyber security strengths, weaknesses and where enhancement is required.

Internal cyber capability often covers the following elements:

1. Adequacy of existing staffing, including the level of funding and the expertise of key cyber staff and the cyber knowledge of employees throughout the organisation;
2. Existing infrastructure and systems, for instance the key software or operating systems utilised by customers and staff;
3. The internal control environment for cyber, for instance the risk controls and reporting in respect of critical assets; and
4. Business continuity planning, covering how the organisation will respond in the event of a significant cyber incident.

For larger organisations, it is useful to conduct a benchmarking exercise against established maturity models or standards frameworks, ideally via an external expert. This review can help directors understand an organisation's internal capability and maturity. The results of the benchmarking are reported to the board and can inform discussions on enhancing specific capabilities. Where an external adviser is employed, it is useful for them to present to the board directly to reduce the risk that management may present an overly positive depiction of the results.

As detailed in **Principle 1**, common frameworks or maturity models that are utilised in benchmarking exercises can include NIST, ISO standards under the **ISO 27000 series** and **ISO 37000 series** and the ASD Essential Eight Maturity Model (**Box 1.4**).

ENHANCING CAPABILITY

A cyber strategy often encompasses steps an organisation will take over a certain period to enhance its cyber capabilities. These steps may be detailed in a roadmap, which can form the basis of progress reporting to the board.

The board may seek to align cyber enhancements, such as additional investment in new IT systems and infrastructure, with broader strategic planning for the organisation. An enhanced cyber posture will support broader digital or innovation focused strategies and can assist in enhancing reputation through being seen as a more cyber and digitally secure organisation.

Cyber enhancements do not always require significant capital expenditure. Rather, in most cases, enhancements are accessible for organisations of all sizes – being low cost, easy to implement and contribute to building a cyber resilient culture. **Box 2.2** lists a series of practical enhancements focused on smaller organisations drawn from ASD guidance, however, these are relevant to all organisations.



BOX 2.2: SMEs and NFPs – Practical cyber capability enhancements

1. Proactively identify opportunities to enhance cyber capability, including using external providers
2. Assess whether utilising reputable external providers will enhance cyber resilience over managing in-house
3. Identify key operational and customer data, who has access to the data and how it is protected
4. Limit access to key systems and data and regularly review access controls
5. Regularly repeat cyber security training and awareness among all employees
6. Promote strong email hygiene (e.g. avoid suspicious email addresses and requests for login or bank details)



Data governance and key digital assets

Every organisation holds key digital assets that, if damaged or lost in a significant cyber incident, would represent a significant threat to business continuity, reputation, or security.

For organisations of all sizes these 'crown jewels' digital assets include critical customer and employee related data, financial data and intellectual property (IP), as well as the technology infrastructure that underpins the ability to do business. In some cases, this might be the technology or systems supporting critical infrastructure and physical assets, such as power generation, water treatment or telecommunications. The loss or damage of this data or infrastructure can not only impact the business operations or continuity of services, but also the broader community – and in turn, severely damage an organisation's reputation.

Central to developing a strong cyber strategy is the comprehensive identification of the organisation's key digital assets and data. A board should have visibility over these key assets and receive regular updates from management as part of ongoing evaluation processes, guided by the questions in **Box 2.3**. Asking these questions will help directors better understand where cyber vulnerabilities may exist and will be a key input into risk management processes – discussed in **Principle 3**.



BOX 2.3: Questions for directors to ask

1. Who has internal responsibility for the management and protection of our key digital assets?
2. Who has access or decision-making rights to our key digital assets? For example, can all customer-facing staff access and change key databases?
3. What access to key digital assets is provided to third parties?
4. Where are our key digital assets located? Is this still appropriate given identified cyber risks?
5. What is the role of external providers in hosting and managing key digital assets?
6. What is the impact of the loss or compromise of any of our key digital assets?

DATA LIFECYCLE AND DATA GOVERNANCE FRAMEWORK

Data is valuable to cyber criminals not just your organisation. Therefore, collecting and storing large amounts of sensitive customer, employee and other organisational data (beyond legislative requirements) creates a significant risk to customers, employees and the organisation.

To help mitigate data-related risks, thorough, consistent and continuous data governance is required. This means directors should understand the extent of personal customer or employee data that is being stored and the legislative or regulatory reasons for doing so. To help ensure data governance is a top priority, all directors should expect of management, on a periodic basis, a 'map' of sensitive data the organisation holds. The map should include the nature of that data; where it is stored; who has access, who is protecting it; how well it is protected; and the business and legal reason for holding this data.

Lifecycle management of all data must be part of any organisation's cyber security strategy and should include secure destruction of all sensitive data. To minimise the risk of data theft or loss, organisations should only collect and store the minimum amount of personal information that is required for its relevant services or operations. For example, some data may be necessary for a 'point in time' only (e.g. onboarding or 'Know Your Client' verifications) and can be deleted after certain activities. There are specific requirements for some organisations to retain some identity documents (such as requirements in satisfaction of the telecommunications metadata obligations). In such cases, directors need to be satisfied that data obtained for a legislative obligation is both secure (as required by law) and has not been copied or stored for 'other reasons' within the organisation.

Furthermore, if there is an obligation to keep data, consideration should be given to storing it offline and, when there is no longer an obligation to retain it, it should be securely destroyed. This is a constant process and requires careful administration but should be a high priority for all organisations – especially those

required to retain significant amounts of personal data. All sensitive data should be encrypted while stored ('at rest') and access to such data strictly monitored.

Effective data governance is covered in more detail in *Governing Through a Cyber Crisis*.

Opportunities and risks with the use of external suppliers and partners

A comprehensive cyber strategy should account for the role of external suppliers and partners. For many Australian organisations, utilising external suppliers and partners is often a component of enhancing cyber security resilience.

Improvements to cyber security resilience associated with external partners include digital services and products that are more sophisticated and resilient to cyber threats, can be updated to respond to emerging threats, are subject to round-the-clock monitoring, and have access to a wide pool of expertise and intelligence. In many instances, outsourcing certain digital functions can bring cyber security benefits not available to an organisation were they to undertake the same function internally. However, in considering whether to outsource a particular function a board should balance the potential cyber and other strategic benefits (e.g. more innovative products) with the costs and any specific cyber and supply chain risks.

The board's oversight of due diligence, monitoring and reporting on key external providers is critical to understanding how a particular outsourced function impacts the cyber posture of an organisation.

In larger organisations, management should report regularly to the board on the cyber security capability and performance of key providers as a component of monitoring the cyber strategy. Obtaining a view of a provider's cyber security capability may be achieved through interviews, testing or certification checks.

The board may also obtain additional oversight on key providers through the provider itself presenting to the board and/or the use of independent assurance.

For smaller organisations, there may be barriers to obtaining specific information from large service providers about their cyber resilience due to differences in bargaining power and/or the provider offering standard terms and conditions. However, the organisation should still have a clear understanding of, or criteria for, what cyber resilient practices should be in place to provide confidence.

Principle 3 on supply chain risk provides additional guidance on how a board can oversee risk controls for key suppliers and take steps to build redundancy.

CORE ELEMENTS OF A DATA GOVERNANCE FRAMEWORK



Policies, procedures and training

Clear and comprehensive policies, procedures and training for how data is collected, used, stored, shared, and destroyed, how data quality is maintained and how data breaches are handled.



Accountability

Assignment of defined and documented responsibilities for data governance to individuals or teams, holding them accountable for ensuring compliance with the framework.



Data classification

Have a system for classifying data based on its sensitivity and importance. This will help to determine how the data should be protected and managed.



Internal controls and security

Include controls to ensure only authorised individuals have access to data, and that data is accessed for authorised purposes only.



Data quality

Determine definitions of data quality, set thresholds and tolerances for acceptable standards based on data classifications, and outline processes for ensuring that data is accurate, complete and up to date.

Ongoing evaluation and refinement

Ensuring the cyber strategy remains fit-for-purpose requires the board to periodically review performance against the strategy and identify opportunities for evolution and improvement. An evaluation or formal review of the cyber strategy at larger organisations may occur annually, in addition to regular monitoring via board reporting. At smaller organisations, an evaluation may be more ad-hoc or informal based on the complexity of the strategy.

There may be events or circumstances where it is appropriate for the board to review the strategy outside the annual process. For example, when an organisation experiences a significant cyber incident, a key component of recovering from the incident would be to reflect on whether the strategy requires amendment. In addition, a sudden change to the threat environment, for instance an industry peer experiencing a significant incident, may warrant the board reflecting on the organisation's strategy and cyber posture.

For larger organisations, it is better practice for the evaluation to be conducted by an external party, which is genuinely independent, and the report presented to the board unfiltered by management. This approach provides an impartial perspective that assists directors in assessing the performance of the strategy.

BOX 2.4: Governance red flags

1. Lack of formal documentation of the organisation's approach to cyber security
2. Limited understanding of the location of key digital assets and data, who has access and how they are protected
3. The cyber strategy and risk controls are not subject to internal and external evaluation and periodic refinement relative to evolving threats
4. Lack of data governance framework to guide how data is collected, held, protected and ultimately destroyed



DIRECTOR REFLECTIONS: Third-party supplier risk

The board must have a level of oversight of the processes for appointing and monitoring the third-party suppliers that store and manage an organisation's digital assets, according to director Catherine Brenner FAICD.

Central to ensuring the appropriate level of visibility at the board level is developing a strong data governance framework.

- As a first step, the board must understand what the organisation's key digital assets are (or 'crown jewels'), who has access to them and how that access is managed (including for example, what consent frameworks are in place).
- Secondly, the board needs to understand what privacy laws apply, and what obligations their organisation owes, in respect of the data it holds.

Ms Brenner says organisations often take comfort in storing key data with a third-party cloud-based provider, for example, but the board needs to understand how the organisation has confidence in the cyber and data management risk controls of both the provider and the organisation itself.

“So often I see, ‘It’s okay, they are managing that for us,’” Ms Brenner said. “But how do we have confidence that these key arrangements and controls are properly understood, overseen and governed?”

Ms Brenner advises directors to be aware of where, how and when data is collected by the organisation, its nature and volume, and where it is held, by whom and for how long. This can be done with summary dashboard reporting. Then, directors can question the risk controls behind that data management. Directors do not need to see granular data on provider performance but must be in a position to verify what is presented to the board.

“Ensuring compliance with privacy laws is a key part of the cyber piece,” Ms Brenner says. “If you’re getting the data governance and privacy piece right, then it is a great part of mitigating cyber security risk.”

Catherine Brenner FAICD is the Chair of Australian Payments Plus, Director of Scentre Group, Emmi and The George Institute for Global Health.

INCIDENT RESPONSE CASE STUDY 2: Ventia Services Group

What began as an unprompted cursor moving on a screen quickly escalated into a full-blown cyber incident for Australian critical infrastructure partner and service provider, Ventia Services Group Ltd (**Ventia**), in July 2023.

From the moment the anomaly was noticed by an observant employee it was all systems go, said Ventia Chair David Moffatt MAICD.

"Our CEO was overseas, I was overseas, and our new CIO was in her first few days of the job. We both returned immediately but were in a state of flux and it became evident we had to rally people from multiple locations to deal with this live threat, and quickly made the decision to shut down access to all our systems," Mr Moffatt said.

"This was a risk-based decision we took to prevent the attackers from getting further into our systems, and it was also a trust-based decision because to shut down our systems also meant pivoting to manual. We acted quickly and decisively and, as a result, were able to keep the threat out."

The decision was guided by Ventia's role as a key partner and service provider to critical government functions and private sector infrastructure owners, and its organisational value that the security of these clients and the broader community was paramount.

Mr Moffatt added that moving to a secure messaging platform and manual based operating model relied not only on the courage of management, endorsed and supported by the board, but also the trust and support of employees.

Close collaboration and alignment between the executive and the board was also pivotal to Ventia's response, said Mr Moffatt, which he described as "not a two-step governance process, but an integrated process".

He also reflected that from the outset, transparency with government, clients, employees and other key stakeholders was fundamental to Ventia's approach.

"Transparency can't be overstated in terms of the trust you build with all of the organisations you're working with. The trusted relationships with our customers, and ultimately their support, was fundamental to us successfully managing the scenario," Mr Moffatt said.

"We made the call with limited information to be totally transparent with the world at large and we would say we were under attack. We put that on our website so everybody knew – employees, customers, media, investors etc – and said we would periodically update this information."

While Ventia was able to keep threat actors out of its systems as a result of its fast response, one thing they had underestimated was the time to reconnect and recover post incident. There was also an overreliance on too small a group of people to return operations to business as usual. The human impact of these events on employees was significant.

As a result, Ventia has taken steps to implement new recovery procedures and processes that would help ensure the organisation recovered more effectively, including appropriate employee support and resourcing. Ventia has also implemented a multi-year strategy to maintain and uplift its cyber security posture, including substantial operational and capital expenditure on cyber security controls.

David Moffatt MAICD is the Chair of Ventia Services Group and Chair of Apollo Global Management Australia & New Zealand.

PRINCIPLE 3:

Embed cyber security in existing risk management practices

KEY POINTS

1. Cyber risk, despite its prominence and velocity, is still an operational risk that fits within an organisation's existing approach to risk management
2. While cyber risk cannot be reduced to zero there are a number of accessible and low-cost controls that all organisations can utilise
3. The board should regularly assess the effectiveness of cyber controls to account for a changing threat environment, technological developments and the organisation's capabilities

Cyber-risk appetite

Cyber-risk appetite is, in broad terms, the risk an organisation is willing to take in its digital activities to achieve its strategic objectives and business plans. Importantly, an organisation's cyber-risk appetite is distinct from its cyber-risk profile, which commonly represents an organisation's 'point in time' position with respect to cyber risk once controls have been factored in (discussed below).

A clear cyber-risk appetite can be used as an input by directors and management to inform current and future business activities, as well as overall strategic decision-making and the allocation of resources. For example, a cyber-risk appetite would inform whether an organisation partners with a third-party, particularly if the arrangement involves the third-party utilising or handling the key digital assets of the organisation. Further, it may assist in investment decision-making and where a board should prioritise additional resources for cyber security controls.

Larger organisations may have a board-approved risk-appetite statement that incorporates all relevant risks, including cyber, to present the organisation's holistic risk appetite.

For smaller organisations, documenting a cyber-risk appetite in detail may not be necessary. Rather, directors should determine the level of risk the organisation will tolerate in undertaking its business activities and objectives.

Having a zero or very low cyber-risk appetite is unlikely to be appropriate or achievable in an increasingly digitally connected economy. A balanced cyber-risk appetite would recognise the inherent risk that comes with doing business in a digital economy, while taking a pragmatic approach to managing this risk in the context of business opportunities. For example, a SME may identify that there are cyber risks associated with outsourcing website payment processing to a cloud provider, however this strategy may outweigh the cyber risks associated with managing payments in-house.



BOX 3.1: Questions for directors to ask

- Does the organisation have a cyber-risk appetite and is it being utilised in strategic decision-making?
- Is cyber risk specifically identified in the organisation's risk management framework?
- How regularly does management present to the Board or risk committee on the effectiveness of cyber risk controls?
- For a larger organisation, is there external review or assurance of cyber risk controls?

Developing and overseeing controls

Where possible, it is appropriate to embed the management of cyber risk into existing risk-management controls and processes. For larger organisations this may be ensuring cyber risk is reflected in the enterprise risk management framework. An embedded approach can enable directors to assess the interaction or impact of other risks on cyber and vice versa.

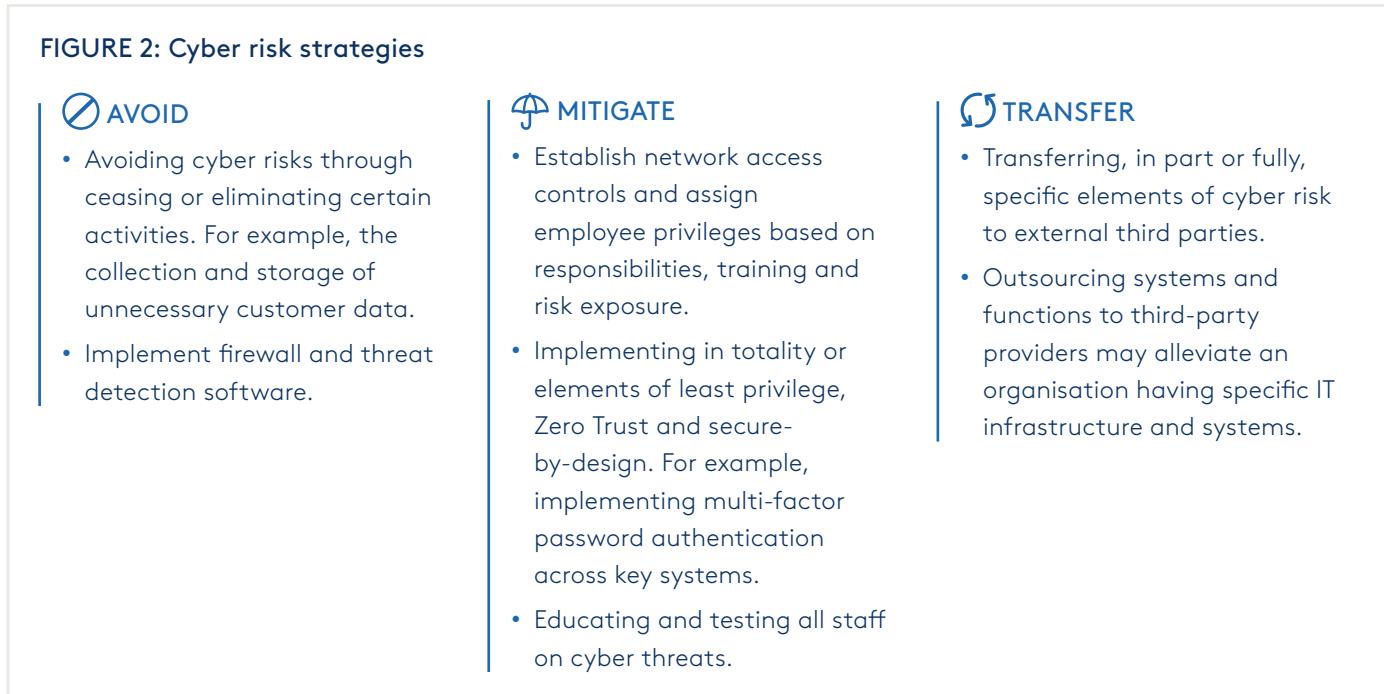
Risk controls or strategies are the mechanisms by which an organisation seeks to avoid, mitigate or transfer cyber-risk (see [Figure 2](#)).

BOX 3.2: Evolution of password controls

There has been a significant shift away from traditional password-based authentication towards more secure and user-friendly alternatives. This trend is driven by the increasing sophistication of cyber threats and the inherent vulnerabilities of password systems.

Organisations are increasingly adopting MFA, biometric methods (such as fingerprint or facial recognition), and passwordless solutions like security keys or mobile-based authentication. These methods not only enhance security by reducing the risk of credential theft and unauthorised access but also improve user experience by eliminating the need to remember passwords.

FIGURE 2: Cyber risk strategies



In general, management is responsible for developing, implementing and managing risk controls. In larger organisations, a dedicated risk/audit or technology committee allows directors to more closely oversee management. For smaller organisations, this oversight may occur in an informal manner, for example through conversations with key personnel. However, central to sound risk governance is an understanding by directors of what cyber risks exist, what controls are in place to reduce or mitigate those risks, and how those controls are performing.

Cyber-risk controls will ultimately depend on an organisation's size, complexity, information systems and infrastructure and cyber-risk appetite. However, there are common stages of risk control that can be applied in organisations of all sizes to manage cyber risks.

For all organisations, the ASD's **Strategies to Mitigate Cyber Security Incidents** provides a comprehensive resource for operationally focused cyber-risk controls, including a number of practical steps smaller organisations can take to mitigate cyber risks.

For larger organisations, traditional risk-control frameworks, such as the three lines of defence, can be readily utilised for managing cyber risk. The advantage of utilising embedded risk frameworks is that they are understood across an organisation and draw upon the expertise of key risk and compliance staff, reducing the likelihood that cyber risk remains the sole responsibility of IT or digital teams.

Risk controls should also account for insider threats from disgruntled or malicious employee activity, which can lead to data theft, system compromise and the theft of intellectual property. Implementing key elements of 'least privilege' or 'Zero Trust', as discussed below, can assist in addressing this risk along with broader employee risk processes. These processes can include prompt deactivation of credentials when employees depart, segregation of duties and access for critical functions and two-person controls for sensitive operations.

Key cyber security risk approaches

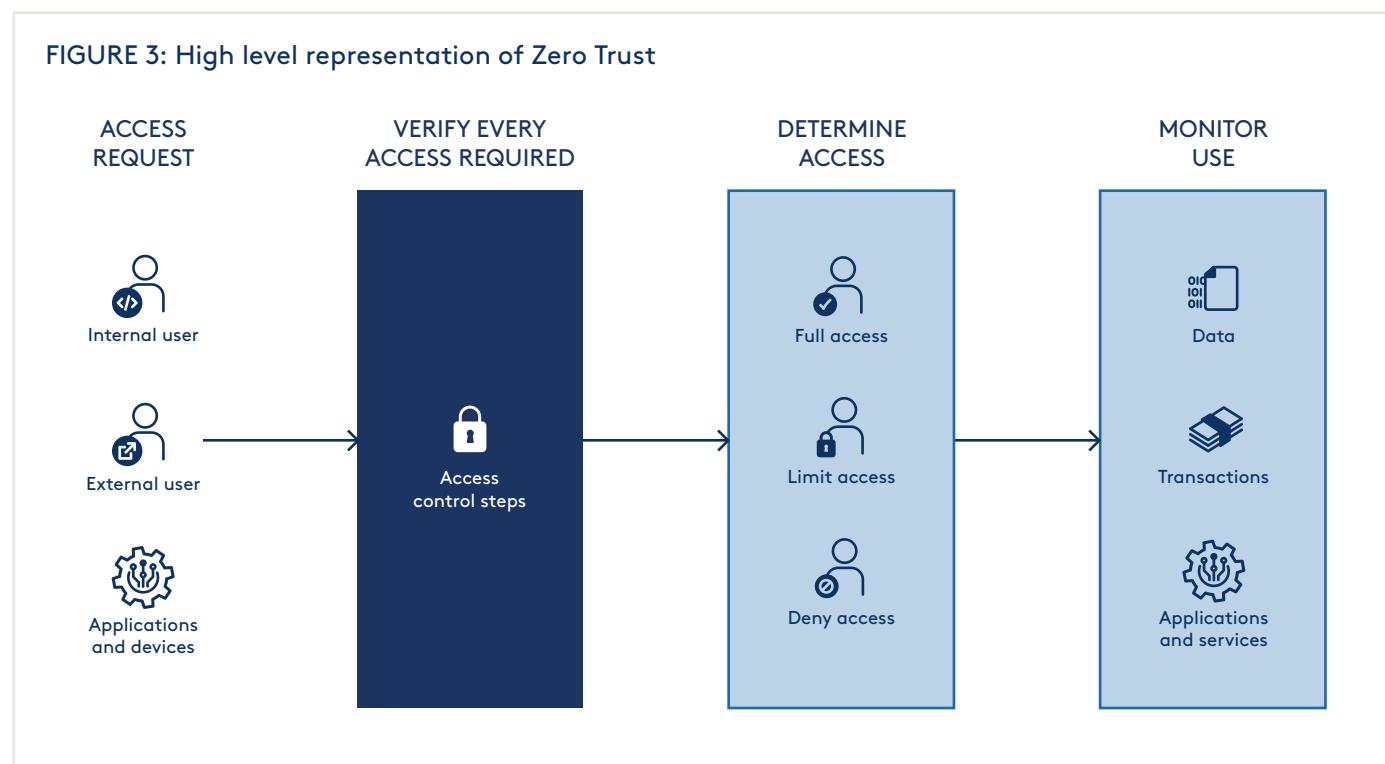
The cyber security models or philosophies of 'least privilege', 'Zero Trust' and 'secure by design' are increasingly central to how organisations are approaching building cyber security resilience and moving away from traditional perimeter-based defences.

Although primarily the domain of management to implement, there is value in directors having an understanding of these approaches as a starting point in engaging with executives, vendors and experts on the effectiveness of risk controls, and how these approaches could assist.

Implementing these approaches or philosophies in totality can be complex and resource intensive. For example, it can necessitate the encryption of data both in storage and also in transit and may require significant investment in new IT infrastructure and software (e.g. to allow for segmenting a network into smaller security zones).

Nonetheless, implementation of elements of these concepts or philosophies may result in enhancements in cyber security resilience and demonstrate to partners and customers a commitment to a secure cyber environment ([Figure 3](#)).

FIGURE 3: High level representation of Zero Trust



LEAST PRIVILEGE

Least privilege is a core concept that is reflected across various traditional cyber security frameworks, including NIST and ISO 27001. The implementation of least privilege will vary across organisations, however common or key features can include:

- **Minimal Access Rights:** Users are given the minimum levels of access necessary to perform their job functions.
- **Role Based Access Control:** Access rights are assigned based on roles within the organisation.
- **Separation of Duties:** Critical tasks are divided among multiple users to prevent conflicts of interest or opportunities for fraud.
- **Privileged Access Management:** Strict control and monitoring of accounts with elevated privileges.
- **Just-In-Time Access:** Providing elevated permissions only when needed and for a limited time.
- **Regular Access Review:** Periodic audits and recertification of user access rights.

ZERO TRUST

Zero Trust is a model or framework for cyber security risk management that is centred on the principle of 'never trust, always verify'. Zero Trust is seen as more suitable to the greater use of cloud computing, remote work and mobile devices to access systems and data. Notably, the Government has committed under the *2023-2030 Australian Cyber Security Strategy* to develop a whole-of-government Zero Trust culture.

The key principles of Zero Trust are:

- Never trust any entity by default, regardless of whether it is inside or outside the network perimeter;
- Enforce strict identity verification for every person and device trying to access data, transactions and applications or services;
- Implement least privilege access, limiting user permissions to only what is absolutely required to achieve the organisation's objectives;
- Assume that breaches are inevitable and segment access to restrict movement; and
- Continuously monitor, inspect and log all traffic, activity and behaviour for anomalies.

SECURE-BY-DESIGN

Secure-by-design emphasises building security into systems and software from the ground up, rather than adding it as an afterthought. This approach involves considering potential security threats and vulnerabilities throughout the entire development lifecycle, from initial planning and design through to implementation and maintenance. By prioritising security at every stage, organisation can create more resilient digital infrastructure that is inherently resistant to cyber-attacks.

By adopting secure-by-design principles, organisations of any size can enhance their security posture, reduce the risk of costly breaches, and demonstrate a commitment to protecting sensitive data.



Cyber supply chain risk

WHAT IS A CYBER SUPPLY CHAIN?

The interconnected network of hardware, software, personnel and data flows, often originating from third parties, that is involved in delivering digital products or services, from development through deployment and ongoing support.

As discussed in [Principle 1](#) and [Principle 2](#), organisations of all sizes increasingly rely upon third parties, such as SaaS providers, to supply key digital and IT services and capabilities that are central to business operations. This approach can bring financial, innovation and cyber security benefits. However, it can also result in discrete risks, including through an overreliance on a particular provider or providers. The result is that many organisations of all sizes have a cyber supply chain where goods and services that are essential to the operation of the organisation can be jeopardised by an external cyber failure or event.

The risk posed by cyber-related supply chain failures is an increasing focus of Government, including via SOCI obligations and APRA prudential requirements. For instance, the SOCI Act Rules specifically require a critical asset owner to develop and provide a Critical Infrastructure Risk Management Program, aimed at eliminating or minimising material risks in the supply chain.

Box 3.3 provides an overview of how an organisation can map its cyber supply chain and identify key providers. It is important to identify where possible third parties that may present an elevated risk due to the nature of the services they provide, for instance managed IT service providers and vendors of critical security or network architecture elements.

BOX 3.3: Mapping and identifying the cyber supply chain

The extent of an organisation's cyber supply chain is contextual. You should consider the essential digital goods and services required by the business to deliver goods and services to customers and clients.

The key question is: Who are the providers that supply the digital services and products your business relies upon to operate? There is also value in highlighting the key and high-risk suppliers.

A map of the cyber supply chain would comprehensively highlight key suppliers, the flow of products, services and data and any interdependencies.

ASD GUIDANCE

The ASD guidance on [Cyber Supply Chain Risk Management](#) is a useful starting point for additional resources on the management of cyber supply chain risks.

For a board, key components of the oversight of cyber supply chain risk can include:

- Understanding the location and ownership structure of the provider, including interdependencies with other IT systems and infrastructure providers (e.g. the software may be hosted within a cloud system of another company – e.g. AWS, Azure), shareholdings, links or cooperation arrangements with foreign governments and foreign intelligence agencies;
- Understanding and monitoring the cyber security posture and settings of the partner, encompassing what contractual obligations it must meet in respect of cyber security and adherence to standards benchmarks (e.g. NIST). For providers that have a higher risk or provide critical services it may be appropriate for the organisation to undertake a vendor security risk assessment;
- Visibility of how a key provider utilises subcontractors or partners to provide the services and notification obligations when these subcontracting arrangements change;
- Security considerations are appropriately captured in contractual obligations and oversight arrangements, for example reporting by the provider and notification settings for incidents of supply failures;
- The role of these providers is appropriately reflected in the Response Plan; and
- Direct engagement by the board with key supplier representatives, including interviews or presentations.

For larger organisations, it is often better practice for the Risk/Audit Committee to have oversight of the risks associated with key supplier relationships, including cyber risks. For smaller organisations the board should have direct oversight.

The CrowdStrike incident in mid-2024 demonstrated the risks with supply chain vulnerabilities. While not a cyber security incident, it did highlight for many boards how the interdependent and layered nature of critical vendors in digital and cyber supply chains can result in significant operational risks. In the wake of CrowdStrike, prominent directors reflected publicly on how the incident was a wake-up call on critical vulnerabilities and how boards and organisations must plan for these events. Better practice on a cyber incident response plan is detailed in **Principle 5**.

Where possible, and resources allow, it may be appropriate for the organisation to have a level of redundancy for particular key services or products. An organisation can implement different forms of redundancy to mitigate risks in the cyber supply chain, including:

- Supplier diversification: Using multiple suppliers for critical products or services;
- Geographic distribution: Spreading suppliers across different regions or countries to reduce location specific risks;
- Data backups: Maintaining copies of crucial data and system in separate, secure physical or virtual locations; and
- Stockpiling: Maintaining an inventory of critical hardware or software.

A comprehensive approach to redundancy is often resource intensive and may not be appropriate or feasible for many SMEs. However, smaller organisations should be maintaining backups (and testing restoration from backups) as a key cyber control and important component of redundancy. Further, it may be appropriate for a small organisation to consider how it could readily switch to alternative suppliers of critical digital services, such as payment processing or internet connectivity.

MEASURING AND EVALUATING INTERNAL CONTROLS

Periodic reporting and regular engagement with management on the performance of risk controls can provide directors with meaningful insights.

However, it may be challenging for directors alone to assess the effectiveness of risk controls, in part due to the rapidly evolving nature of cyber risk and the lack of established metrics for cyber performance.

In practice, effective cyber controls could mean that attempted cyber threats or incidents have little to no impact on business operations or key assets, due to the effectiveness of the measures put in place to mitigate the threat. While this is a good outcome, it may not accurately reveal the underlying role of controls in preventing incidents. The absence of no or few reports of cyber incidents should have directors on notice to engage regularly with management to understand what inputs are informing the level of risk assessment.



BOX 3.4: SMEs and NFPs – Risk controls

1. Patch and update applications and anti-virus software
2. User application hardening – limit interaction between internet applications and business systems
3. Limit or restrict access to social media and external email accounts
4. Restrict use of USBs or external hard drives
5. Restrict operating system and software administrative privileges
6. Implement multi-factor authentication
7. Maintain and regularly test offline backups of key data
8. Ensure that departing employees and volunteers no longer have access to systems and passwords, or physical access to sites or sensitive data

Directors should also assess whether prominent cyber incidents that impact other organisations warrant an evaluation of risk controls, including asking management whether a similar incident would inflict damage upon the organisation and what steps need to be taken to mitigate against a similar incident. All directors should treat other incidents as simulations.

As discussed in **Principle 2**, at least annually, directors should reflect on the cyber risk controls of the organisation and whether the cyber-risk appetite remains appropriate, having regard to the evolving external threat environment and internal capabilities.

For larger organisations, it may be appropriate to have an annual external audit or assurance of cyber risk controls.



BOX 3.5: Governance red flags

1. Cyber risk and cyber strategy not reflected in existing risk management frameworks
2. High management confidence that cyber risk controls are effective without regular external validation
3. Over reliance on the cyber security controls of key service providers, such as cloud software providers
4. Cyber security controls of potential vendors are not assessed in the procurement process for key goods and services
5. Prolonged vacancies in key cyber management roles

DIRECTOR REFLECTIONS: How to evolve effective cyber risk practices

Reflecting on how boards should approach cyber risk management, experienced non-executive director, Melinda Conrad FAICD, noted that while cyber risk is an operational risk, it is not a static risk.

The cyber threat environment is dynamic and constantly evolving, often at a much faster pace than other operational risks an organisation faces. It is for this reason that oversight of cyber risk warrants an elevated focus by the board, and directors should be continuously looking for ways to uplift their skills and knowledge and identify where external help may be needed.

In Ms Conrad's view, effective levers to assist a board's oversight of cyber risk management within an organisation include:

- **Setting a cyber-risk appetite** as a tool to guide investment decision-making and evaluating the adequacy of risk controls. In determining the cyber-risk appetite, boards should take the time to understand the organisation's 'crown jewels' (or key digital assets) which could be most impacted by a cyber event.
- **Map critical services and infrastructure** to provide visibility of key providers and potential vulnerabilities. This assists a board in understanding where it needs greater oversight on the cyber resilience of key providers and where alternatives, backups or redundancies to critical services should be considered.
- **Regular reporting to the board** using both lead and lag metrics. In addition to reporting on the technical aspects, such as patching and perimeter protection practices, the board should also focus on how 'cyber hygiene' is being practiced across the company — what is the percentage of staff who have completed cyber awareness training? What is the staff phishing failure rate? The outcomes of these metrics can then be assessed against the board's risk appetite so that there is alignment with management on what is an acceptable cyber risk position for the company.
- **External audit, review and penetration testing** which are conducted by rotating providers to ensure they are 'not marking their own homework'. This overlay allows directors to test what management is reporting to the board and provides visibility of how an organisation is benchmarked against industry peers and standards frameworks.

Melinda Conrad FAICD is a Director of ASX Limited, Ampol Australia, Stockland, Penten and The Centre for Independent Studies.

PRINCIPLE 4:

Promote a culture of cyber resilience



① KEY POINTS

1. A truly cyber resilient culture begins at the board and must flow through the organisation and extend to key suppliers
2. Regular, engaging and relevant training is a key tool to promote a cyber resilient culture, including specific training for directors
3. Incentivise and promote strong cyber security practices, including participating in phishing testing and penetration exercises



Creating a cyber security mindset from the top down

Building a cyber resilient culture is the responsibility of everyone, however the board and senior management have a leading role to play in promoting and modelling a cyber security mindset and this should also flow through to what is expected of suppliers. Governance decisions, and the oversight of cyber security risk management, should promote a culture of cyber resilience across the organisation – that is, the day-to-day attitudes and conduct of staff in their interactions with the digital world.

Directors can demonstrate a commitment to a culture of cyber resilience through seeking opportunities to build their personal knowledge of digital products and services, data governance, and market-leading cyber security settings. This commitment not only sets a tone from the top but also positions the board in a strong position to assess the resilience of the organisation, make investments to boost resilience and engage with management and experts. A commitment to ongoing education and building knowledge is also consistent with a director meeting their directors' duties.

Frequently, significant cyber incidents have an element of human error (e.g. an employee opening a malicious email). Therefore, a genuine culture of cyber resilience is a crucial – and often overlooked – cyber control. Building cyber resilience in staff will both improve cyber resilience in workplace settings as well as when staff use work devices in home settings. Initiatives that directors can require of management fall into three main categories, as shown in [Figure 4](#).

FIGURE 4: Features of a cyber resilient organisational culture

 **BEHAVIOUR AND LANGUAGE**

- Board and senior management communications reinforce importance of cyber security and shared responsibility of all staff
- Regular ongoing cyber awareness training is completed by all employees, including by directors and senior management
- Embedding a common and accessible language when talking about cyber security, with updated information provided about new and emerging threats
- Being open and honest about cyber risks to the organisation and encouraging all staff to play their part in promoting cyber resilience
- Cyber training and phishing exercises promote a culture of continuous learning rather than criticising employees for poor understanding
- Consider building a team of 'cyber champions' across the organisation, who staff can go to for advice and guidance
- Careful handling of post incident review processes to avoid blame culture while maintaining appropriate accountability.

 **GOVERNANCE**

- Cyber security resilience is integrated into established risk management processes and reporting and are reflected in the organisation's risk appetite
- Clearly defining key roles and responsibilities for cyber security management right across the organisation
- Ensuring cyber security strategy and risk management are standing items for the board or meetings of the board audit/risk/technology committee
- Developing a comprehensive Response Plan in the event of a cyber security incident (see **Principle 5**)
- Ongoing board training and expert briefings to sharpen skills and maintain currency of understanding.

 **INCENTIVES**

- Developing KPIs and incentives for management, key personnel, and/or where appropriate, all staff, to ensure cyber security performance, including both sound cyber risk management practices and execution of the cyber strategy
- Encouraging conduct such as transparency and early reporting of cyber breaches (or attempted breaches such as phishing)
- Regularly communicating to all employees about cyber hygiene performance with strong team performance highlighted and rewarded.

Skills and training

Effective cyber security policies alone are not sufficient to promote cyber resilience across the organisation. While policies may explain where risks lie, ongoing training and education is necessary.

It is critical that cyber security training is implemented beyond the induction or orientation process for new staff, including directors. Engaging and relevant training will reinforce sound cyber hygiene practices and an overall culture of cyber resilience. Cyber training should take place at least annually, and through management reporting, the board should have visibility of training results, including differences between business areas.

External training providers can assist with technical ‘deep dives’ appropriate for specific cohorts of staff, or even directors where the board would benefit from a more comprehensive understanding.

PAYING ATTENTION TO KEY STAFF AND CONTRACTORS

In larger organisations, close attention should be paid to business functions or key personnel that have greater access to and control of key digital assets, systems and infrastructure. This heightened focus can entail internal and external security operation centres (SOCs), additional security controls for these individuals, and more in-depth training around being aware of their heightened security risk profile.

Increasingly, these staff or third-party contractors are being targeted by external threat actors precisely because they do have widespread, high-level access to many systems. If threat actors can access the credentials of someone who has ‘system administration’ across many key systems within an organisation, it means they can gain a foothold and move around as if they are a legitimate user, evade normal detection mechanisms and then carry out reconnaissance and large-scale data theft.

BOX 4.1 QUESTIONS FOR DIRECTORS TO ASK

1. Is cyber security training mandatory across the organisation?
2. How often is training undertaken, including by directors?
3. Is training differentiated by area or role?
4. How is the effectiveness of training measured?
5. What is the plan for building the cyber security understanding of directors and senior executives?

DIRECTOR EDUCATION

For organisations where cyber security risk is highly material and/or tied to an ambitious strategic agenda (e.g. digital transformation) it may be appropriate for a director to hold specific cyber security or digital skills. In such cases, having a director with deeper knowledge may provide the full board with additional insight. It is critical that remaining board members do not abdicate responsibility for cyber security to that individual, nor should it be considered a substitute for management level capability.

Becoming cyber literate can help directors gain confidence in their understanding of the cyber threat landscape, the potential impacts that cyber failings can have on the organisation, strategies for improving cyber resilience, as well as response and recovery in the event of cyber incidences. It can also have broader educational benefits in assisting board decision-making on digital and information technology strategies, including new capital investments.

Directors should also keep across the evolving cyber security regulatory landscape, including legal obligations that may apply to their organisation. Critically, this requires an understanding of the organisation’s notification requirements to regulatory and reporting bodies such as the OAIC, APRA, the CISC and the ASD in the event of a cyber incident.

COLLABORATION

Directors can also instil an outward and proactive focus on the cyber threat landscape by encouraging management to participate in information sharing and collaboration with government and industry peers, within legal constraints.

Directors should test whether their organisation is contributing to formal intelligence exchanges, such as threat information, and whether this network is providing timely updates on emerging threats.

Large organisations, for example, are encouraged to participate in the **ASD's Cyber Security Partnership Program** which enables participating organisations to share, and obtain insight, and intelligence on cyber security threats with the ASD.

Management should also be encouraged to contribute to collaborative industry fora that can share information on effective risk control and may be able to assist in cyber incident recovery, for example through pooling of resources to support impacted organisations.



BOX 4.2: SMEs and NFPs – Cyber resilient culture

1. Mandatory training and phishing testing for all employees, and volunteers where appropriate
2. Regular communications to employees on promoting strong cyber practices, including email hygiene. The communications could be electronic (e.g. email reminders) or physical (e.g. signage in the workplace)
3. Incentivise strong cyber practices, for example small rewards for performance on phishing exercises
4. Pick a staff member to be a 'cyber security leader' to promote strong cyber practices and respond to questions from other staff
5. Subscribe to ASD alerts to stay across emerging cyber threats



BOX 4.3: Governance red flags

1. Board and executives do not undertake cyber security education nor participate in testing
2. Cyber security is not reflected in the role statements and KPIs of key leaders
3. Communication from leaders does not reinforce the importance of cyber resilience to staff – cyber is seen as an issue for frontline staff to manage
4. There is a culture of 'exceptions' or workarounds for board and management with respect to cyber hygiene and resilience

DIRECTOR REFLECTIONS: A practical cyber security governance framework

Andy Penn has a four-point framework he has developed as a practical and pragmatic way for boards to approach cyber security governance and build cyber security resilience.

1. You cannot protect what you do not know you have.

- Build an inventory of digital assets.
- Complete and maintain a thorough inventory of all your digital assets – this will take time and be more challenging than it sounds but it is an essential foundation for good cyber security. The inventory can be independently verified for additional diligence.
- Use the process as an opportunity to consider how to simplify your technology environment, approach to collecting and storing data, and your digital footprint. Dispose of digital assets and data that no longer need to be retained.

2. Not all digital assets are equal, but they are all defendable.

- By undertaking a thorough inventory of digital assets, you will be able to triage them in terms of their criticality and determine a security posture appropriate for each.
- Pick the appropriate framework against which to measure the security posture you will take – the Essential Eight is a very good model depending on the type of asset. For applications, data sets, encryption keys, AI instances, and hardware/endpoint, additional security steps may also be required.
- Identify security gaps and agree an approach, timeline and resources for addressing those gaps. This will form the foundation of the company's cyber security improvement program.

- Legacy systems remain a big problem for many organisations but, by knowing where they are and the vulnerabilities they may present, they can be better defended. Furthermore, a solid plan to replace legacy systems based on risk can be implemented.

3. The worst time to develop a crisis management plan is in the middle of a crisis.

- Make sure your organisation has a well-established cyber-specific crisis management plan, including playbooks, clear lines of accountability and pre-prepared communications.
- Scenario testing is essential. Pressure testing the response of the executive leadership team and the board in an environment that is as realistic as possible will help identify any weaknesses or missing elements.
- Pre-plan how key issues such as continuous disclosure obligations and ransomware demands are going to be dealt with to the point of even getting legal advice on scenarios tested.
- The board is unlikely to be best placed to make fast decisions on the intricate and technical complexities of a real-life incident.

4. What is safe today may not be safe tomorrow.

- Cyber security and cyber threats are constantly evolving with new innovations and new technologies – AI and Quantum for example can introduce new vulnerabilities into encryption systems that do not exist today. Therefore, it's the responsibility of directors to stay up to date with new threats and potential vulnerabilities.

Andy Penn AO is a director of Coles Group, Chair of Visit Victoria, a Senior Advisor to McKinsey and TPG Private Equity and is a member of the Council of Trustees of the National Gallery of Victoria. Mr Penn was Chair of the Expert Advisory Board on the development of both the 2023-2030 Australian Cyber Security Strategy and the 2020 Strategy and is the former Chief Executive Officer of Telstra.

PRINCIPLE 5:

Plan for a significant cyber security incident

KEY POINTS

1. Directors and management should proactively plan for a significant cyber incident
2. Simulation exercises and scenario testing are key tools for the board and senior management to understand and refine roles and responsibilities
3. A clear and transparent approach to communications with key stakeholders in a significant cyber incident is critical in mitigating reputational damage and allowing for an effective recovery



Preparation

A board and organisation that is well prepared for a significant cyber incident will be in a stronger position to mitigate impacts to its business operations, reputation and stakeholders, as well as recover in a timely manner. Directors should appreciate that, following a significant cyber incident, information may be fluid and there may be inaccurate or unverified material being spread via media, chat forums and elsewhere on the Internet. Such information may be disseminated by the actual perpetrator of the attack or others impersonating them to create confusion or profit opportunistically. The board should also be aware that in some circumstances directors and senior management can be personally targeted by threat actors during the incident as a mechanism to increase pressure on decision-making, for instance the payment of a ransom.

For this reason, communications during a 'live' cyber incident must be planned beforehand so there is a consistent approach as to how the organisation will manage the incident, who their external Incident Responders will be, and which experts will be critical in developing communications. This way, irrespective of the media attention and counter narratives that may circulate during the incident, the organisation will be able to respond to all stakeholders in a constructive and measured way.

ROLES AND RESPONSIBILITIES IN A CYBER INCIDENT

The nature of a cyber crisis requires organisations to have clearly defined roles and responsibilities that are articulated before an incident to ensure a prompt and effective response. These roles and responsibilities should be documented in plans and practised as part of training and simulations that include the board.

Figure 5 highlights key roles and responsibilities across three levels, starting with the role of the board. External support, including from key suppliers, is often critical in the cyber incident response and recovery phases and this role should also be documented.

FIGURE 5: Documenting key roles and responsibilities for cyber incident response

Board Board sub-committee	CEO	Incident response team
	Key senior management	IT security and infrastructure teams
	Senior IT staff	Frontline customer service
	Human Resources and Legal	Ongoing business operations and finance
	External support and advice	On the ground external support
	KEY RESPONSIBILITIES	KEY RESPONSIBILITIES
<ul style="list-style-type: none"> • Approve major decisions related to crisis response • Approve new resources and spending • Monitor response and provide high level guidance and support • Approve key communications 	<ul style="list-style-type: none"> • Activate the Response Plan and lead response • Coordinate actions across teams • Oversee and approve immediate security and recovery actions • Understand and fulfill legal and regulatory obligations • Communicate regularly and openly with staff, customers and other stakeholders • Support frontline employees • Call on external support and advice 	<ul style="list-style-type: none"> • Undertake immediate triage and implement security measures • Safeguard sensitive and data and systems • Access and rebuild systems from backups once safe to do so • Communicate and support stakeholders and customers • Report back to management • Participate in post-crisis briefings



CYBER INCIDENT RESPONSE PLAN

A documented cyber incident response plan (**Response Plan**) is a key tool in ensuring an organisation is well placed to respond effectively to a critical cyber incident.

Significant cyber incidents can be incredibly complex with a high number of variables that make comprehensive planning challenging. However, developing a Response Plan is a key tool in ensuring that those involved at the board and operational level have a clear understanding of their respective roles and responsibilities.

The Response Plan is a core component of an organisation's broader cyber strategy or policy. For larger organisations, the Response Plan may also be a component of broader business continuity and crisis management planning.

The Response Plan would seek to cover a series of potential incidents (e.g. ransomware, denial-of-service, failure of a critical supplier or service) and be informed by scenario and simulation exercises, discussed below.

Appendix A provides a summary of the threat of data theft, including ransomware, and a high-level decision tree for how a board may approach a data extortion event.

Table 2 details the core elements of a comprehensive Response Plan. **Figure 6** illustrates where the cyber strategy and Response Plan fit within the cyber incident lifecycle.

TABLE 2: Core elements of a comprehensive Response Plan

Element	Detail
Roles and responsibilities	What business functions and personnel will be responsible for implementing key steps in the Response Plan, including the role of the board or board committee. For larger organisations it should detail the immediate response/crisis management team (CMT) and include staff from IT, communications, human resources, legal and senior executive representatives. It should also include any third-party external experts who could assist in the event of an incident.
Resources	What resources will the incident response team require? This should cover physical resources (e.g. computer assets, data back-ups), key internal expertise (e.g. cyber security, legal) and external expertise and support (e.g. crisis advisers, legal advisers, cyber insurer support, communications support). It should also identify where possible where the board may need to approve the procurement of additional resources.
Common security incidents and responses	Detail common threat vectors, common cyber incidents and the response to those incidents. For instance, the plan would detail how the organisation would respond to a denial of service, phishing, ransomware, malware and data loss/breaches incidents.
Triage and immediate response	How the organisation will identify a cyber incident is occurring, assess its severity and understand the impact on business operations and internal and external stakeholders.
Containment and eradication	Strategies and actions for limiting the severity and scope of the cyber incident. Steps for containing and eradicating an attack may include taking affected systems offline or isolating unaffected systems to prevent spread of malware.
Communications	Specific communication approaches for staff and impacted customers, suppliers/external partners as well as the broader public. It should be clear who will be responsible for communicating with which stakeholders, including coordination with Government agencies (e.g. ASD and Coordinator) Communications is expanded on in further detail below.
Notification and reporting	Identification of regulatory, market and customer/supplier reporting and notification obligations. For larger organisations these requirements can be numerous depending on the nature of the incident. The ASD's ReportCyber tool is a valuable starting point for understanding and meeting this requirement.
Recovery and remediation	Steps for not only rebuilding systems and infrastructure, including new investment in IT systems, if necessary, but also for examining 'lessons learnt' and identifying strategies to minimise the risk of a similar incident occurring in the future.
Supporting procedures and playbooks	For larger organisations it is often good practice to have specific playbooks on common or high impact incidents. In effect, a playbook is a detailed response plan covering the immediate response steps to a particular incident, such as ransomware, denial of service, loss of critical external service/product.

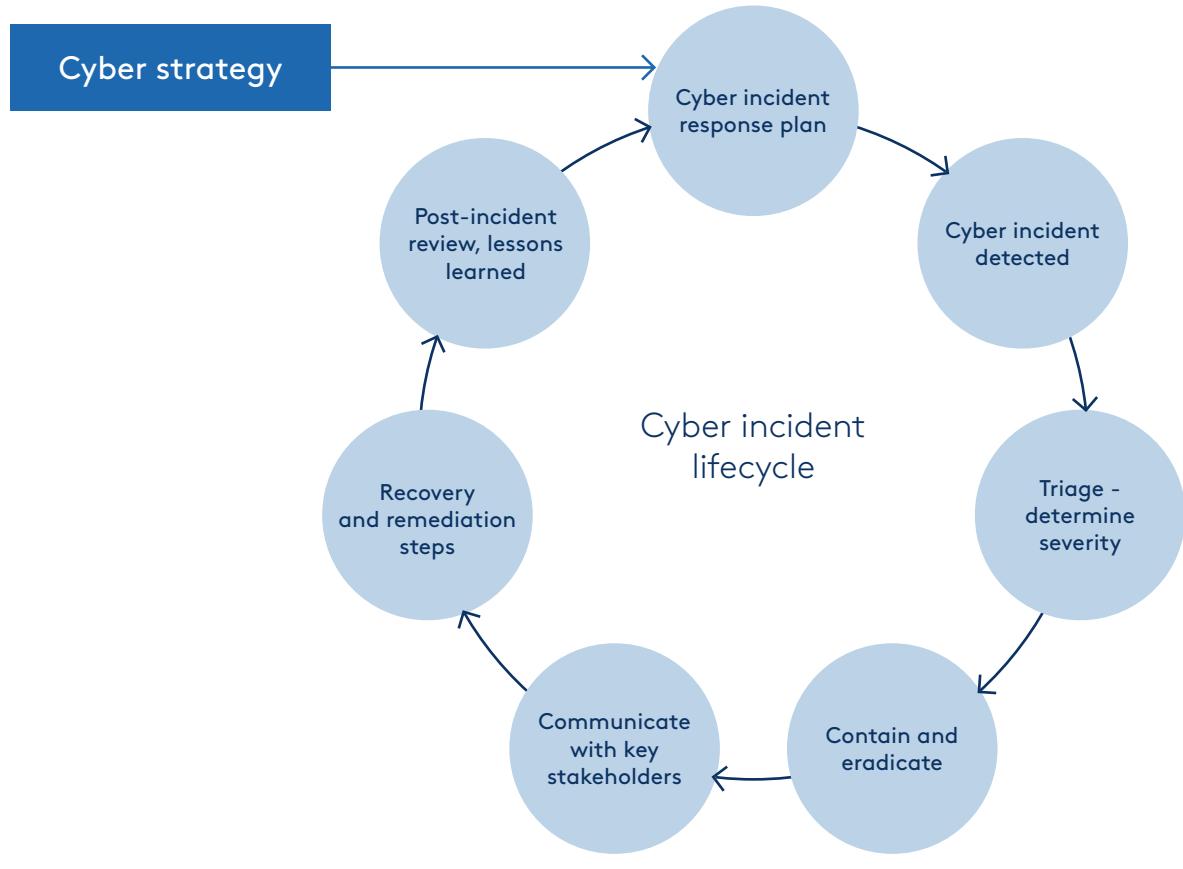
Directors should approve the Response Plan and have an understanding of the responsibilities of the board and/or specific directors in the event of an incident. The Response Plan should be cascaded through the organisation to promote key staff awareness, including understanding their roles and responsibilities.

The Response Plan should be reviewed on a regular basis and be updated based on changes in environmental factors (e.g. emerging threats), organisational structure and any changes to the organisation's key digital assets.

Maintaining hard copies of cyber incident response plan documents – and other key documents like contact details – is essential. In the event of an incident, the organisation's systems may be inaccessible.

While a Response Plan will need to be tailored to each organisation and its personnel and assets, a range of templates are available, including the ASD's *Cyber Incident Response Plan – Guidance*.

FIGURE 6: The cyber incident lifecycle



TRAINING AND TESTING

The board must be satisfied an organisation is prepared to quickly and effectively respond to a significant cyber incident. A program of regular testing and continuous improvement of the Response Plan is the most-effective way to establish this confidence and build the essential muscle memory that teams, including boards, need to exercise.

A program of training and testing should include:

1. Regular technical and physical penetration testing:

For more mature organisations, penetration testing ('pen testing') should also include testing based on the assumption of compromise, both technical and physical (e.g. allowing testers entry to an IT environment to determine how secure it is beyond the perimeter). Boards should be briefed on the scope and results of penetration testing, including understanding what controls and systems are tested and the remediation timetable in relation to high-risk vulnerabilities.

2. Desktop scenario-based exercises:

Desktop exercises provide a valuable platform for teams to step through an escalating series of technical and non-technical scenarios and discuss how the current plans and resources would respond. Such exercises are designed to build a common understanding of roles and responsibilities and to identify gaps in current planning and resources. They can be undertaken at the multi-disciplinary leadership and board levels and can also be used within discrete teams to refine specific response actions. For example, there is significant value in a crisis communications scenario test.

3. Testing an organisation's response through simulations:

Simulation exercises are a key tool for the board, senior management team and operational teams to test their knowledge of plans and processes and their roles and responsibilities during an incident. They differ from desktop exercises in that their purpose is to test people, processes and plans.

Organisations will adopt a program of training that is relevant for their scale, complexity and risk profile.

For larger organisations, good practice is to run simulation testing at least twice a year, using different scenarios, supported with focused desktop training sessions throughout the year. Critical infrastructure entities, or those at higher risk due to the nature of their industry, operations, or the data they hold, should look to run simulations on a quarterly basis, if possible. Response plans should be updated to reflect lessons learned during the simulations.

It is important that simulations test the organisation's response to incidents that are credible or likely – but may be lower impact – as well as those that would have an extreme impact. Plans should be tested across all levels of the organisation. Simulations should support the board and senior management team to voice concerns, learn from mistakes and improve critical skills.



BOX 5.1: Questions for directors to ask

1. Do we have a Response Plan informed by simulation exercises and testing?
2. What role does the board have in communications and/or public announcements?
3. In the event of data loss or theft what is the plan for communicating with customers and employees?
4. Are we aware of our regulatory obligations to notify or report the incident?
5. How will we support employees who are responding to the incident and ensure they have the necessary resources?
6. Can we access external support if necessary to assist with response?

RESPONSE AND RECOVERY

COMMUNICATIONS

A clear and comprehensive approach to communications during a significant cyber incident is critical. Many organisations have experienced greater reputational damage from poor communications rather than the incident itself.

While generally the responsibility of senior management, the board will often have close involvement in the approach to communications due to its importance to stakeholder relationships, including with government, regulators, customers and staff. It is vitally important that an organisation communicates as transparently as possible with key stakeholders (most importantly customers) on the nature and potential impact of the cyber incident.

However, assessing the full extent and severity of a cyber incident can take some time and raise complex questions regarding materiality, especially for listed entities. In some cases, it may be appropriate to acknowledge that the direct cause of the incident and its impact on business operations and stakeholders are not yet known and may remain uncertain for some time, with updates provided to stakeholders as the situation evolves. Organisations should be mindful that what may appear to be a 'fact' early on can sometimes be false. Therefore, 'facts' can change, and communications will need to acknowledge that cyber incidents can often evolve. In doing so, organisations should be clear on what facts are known, and unknown, so that there is appropriate transparency and stakeholder expectations can be managed.

Where there has been a significant incident, in addition to any regulatory notification obligations, it is important that those whose data has been compromised (most importantly customers) are advised promptly. Directors of ASX listed organisations should also bear in mind their continuous disclosure obligations under the ASX Listing Rules and Corporations Act. In May 2024 the ASX updated its [Guidance Note 8](#) to assist listed companies make disclosures in respect of cyber incidents.

The changes to the Guidance Note highlight that directors will need to promptly consider whether the cyber incident is likely to have an operational or reputational impact that materially affects the company's share price and if so, disclose this information to the market as soon as possible after becoming aware of the incident. The Guidance Note also sets the expectation that listed companies should have draft announcements and comprehensive response plans in place for potential cyber incidents to ensure adherence to disclosure obligations.

More broadly, regulators, investors and other stakeholders may expect listed company directors to disclose cyber security risks as part of other regulatory disclosures such as the Operating and Financial Review, which outline material business risks. It is important these disclosures are accurate and reflect the significance of any cyber incident the organisation has experienced and simply not a cut and paste from previous disclosures. However, companies should be careful that disclosures (say of risk controls) do not compromise cyber resilience.



BOX 5.2: Governance red flags

1. The board and senior staff have not undertaken scenario testing or incident simulations to test the Response Plan
2. Likely scenarios and consequences are undocumented with lessons from simulations not being captured
3. It is not clear how communications with key stakeholders will be managed in the event of an incident
4. No post incident reviews with board and management

ENGAGEMENT WITH GOVERNMENT AND REGULATORS

The Response Plan should be clear on responsibilities for real time management and engagement with government agencies and regulators. Depending on the organisation and the incident, notification requirements may include the OAIC under the Notifiable Data Breaches scheme in the Privacy Act, ASD and Home Affairs under the SOCI Act, financial regulators APRA and ASIC, and state government departments and agencies.

If the organisation is particularly large or systemically important, the organisation should liaise with the National Cyber Security Coordinator (**Coordinator**). One of the roles of the Coordinator is to work across the Commonwealth Government to bring together expertise and resources from departments and agencies and work with the victim organisation to lessen the consequences of a cyber incident. Where the scale of an incident is significant, it may also warrant direct contact with relevant ministerial offices.

In general, a posture of collaboration and transparency with key arms of the Government is likely to assist in effective incident response and recovery. The ASD, for example, may be able to assist in the technical recovery, including the triage of systems and expelling threat actors. Actively engaging with the Coordinator and ASD may result in a more efficient and effective response from the Government that will ultimately benefit impacted customers.

As noted in **Table 1**, under proposed legislative reforms, the ASD and Coordinator would be bound by a ‘limited use obligation’ that would limit how information that is shared with these bodies during a critical cyber incident can be used by other regulators or law enforcement bodies. It is hoped these reforms will encourage greater trust and collaboration between industry and government.

Recovery

A comprehensive Response Plan should also address what happens once the immediate crisis has passed, outlining the process for recovery. Operationally, this can include the approach to recovering IT networks, systems and applications to ensure business continuity. This may be done in partnership with external IT advisers.

THE BOARD’S ROLE IN RECOVERY AND REMEDIATION

The recovery phase begins when the crisis has been contained and no longer represents an immediate risk to an organisation’s data, systems, people and customers, with systems operating at a level that enables BAU (business as usual) activity to resume. The role of the board in the recovery phase is to oversee and assist management to secure systems, understand the impact and what went wrong, and returning the organisation to business as usual. It is also critical to assess where improvements and investment may be required to an organisation’s risk management controls and cyber strategy.



BOX 5.3: SMEs and NFPs – Plan and respond

1. Prepare a Response Plan utilising online templates if appropriate.
2. If practical, conduct a simulation exercise or test various scenarios against the incident response plan.
3. Ensure physical back-ups of key data and systems are regularly updated, tested and securely stored.
4. Maintain offline lists of who may assist in the event of a significant cyber security incident and which key stakeholders to communicate with.

For larger organisations, a post-incident review may assist in identifying lessons learned and ultimately promote a cyber resilient culture. Key questions or issues that might be covered in a post-incident review are highlighted in **Box 5.4**.

The board also has a key role in the remediation phase of a cyber crisis where the organisation is seeking to rebuild stakeholder trust and make investments to strengthen its cyber defences (see **Figure 7** for the main features of this phase).

The board should expect a clear plan for each of these key activities, with regular reporting and updates. In particular, the board should be satisfied with the speed of the recovery and remediation program and the adequacy of resources to support each activity.

② **BOX 5.4: Key post-incident review questions**

1. What have we learnt about our existing systems, controls and cyber behaviour, including weaknesses?
2. Did everyone know their respective roles and follow them? How did they perform individually and collectively?
3. Did the organisation become aware of the incident within an appropriate timeframe? Was the incident reported to us by a third-party like a vendor or the media? What does this tell us about monitoring and reporting controls?
4. Was the board appropriately briefed about the incident? Did we have sufficient oversight and visibility of management actions?
5. Did we appropriately support the employees who were at the front line of responding to the incident?
6. What improvements could be made to communication plans?
7. How have we sought to rebuild relationships with impacted stakeholders?

SECURITY UPLIFT IN THE RECOVERY PHASE

A significant cyber incident will often precipitate the need for a significant security remediation program. However, immediately, the board will need to be satisfied there are appropriate measures in place to ensure that as systems are restored, they remain secure and that appropriate short-term investments and measures to secure data and systems have been adopted.

Boards should look to their internal IT and security teams and their external security providers and forensics experts to address the following questions:

- What is the level of confidence that the systems are now secure?
- What is the risk and likelihood of a secondary attack, and what measures are in place to rapidly identify and contain any attempts?
- What tools, systems, monitoring and processes have been implemented to immediately uplift security? Are these partially or fully implemented and functional?
- Do we have sufficient monitoring, protection and visibility of the organisation's digital assets?
- Are there any critical vulnerabilities that require further immediate remediation?

The security uplift phase can also be examined as a component of any post-incident review.

WELLBEING OF EMPLOYEES

A cyber incident can be a highly stressful event for those impacted, and for those tasked with responding to the incident. Those involved in directly responding to the incident, including senior management, frontline technical staff and those handling customer queries, will be working long hours and be under intense pressure for an extended period. In addition, many employees not directly involved in the response may have changed work patterns and experience increased pressure. For instance, taking over the responsibilities of staff involved in the direct response or facing customer queries and complaints.

The wellbeing of staff should be a key consideration in the recovery period, with a supportive, team-focused culture central to effective recovery and rebuild.

Concrete steps a board could oversee and prompt management to implement include:

- Regular communications and briefings;
- Assistance with identity theft concerns; and
- Acknowledgement of and rewarding efforts.

Where employee error has caused or contributed to the incident, the board should satisfy itself that consequence management is appropriate and that individual scapegoating does not occur which could gloss over systemic failures.

ReportCyber

Organisations of all sizes are encouraged to report significant cyber incidents to the ASD. Reporting can assist an organisation receive support and also provides visibility to the ASD of current threats to Australian organisations.

Reporting can be done via the ASD website's [ReportCyber portal](#).

The 24-hour Cyber Security Hotline (1300 CYBER1) is a key source of advice for individuals and SMEs.

CUSTOMER REMEDIATION AND COMPENSATION

An effective remediation, compensation and complaints-handling process actively contributes to restoring customer and regulator trust, and can mitigate future litigation risks. Boards should consider compensation from the perspective of the customer and not just a legal baseline of what is 'legally necessary'.

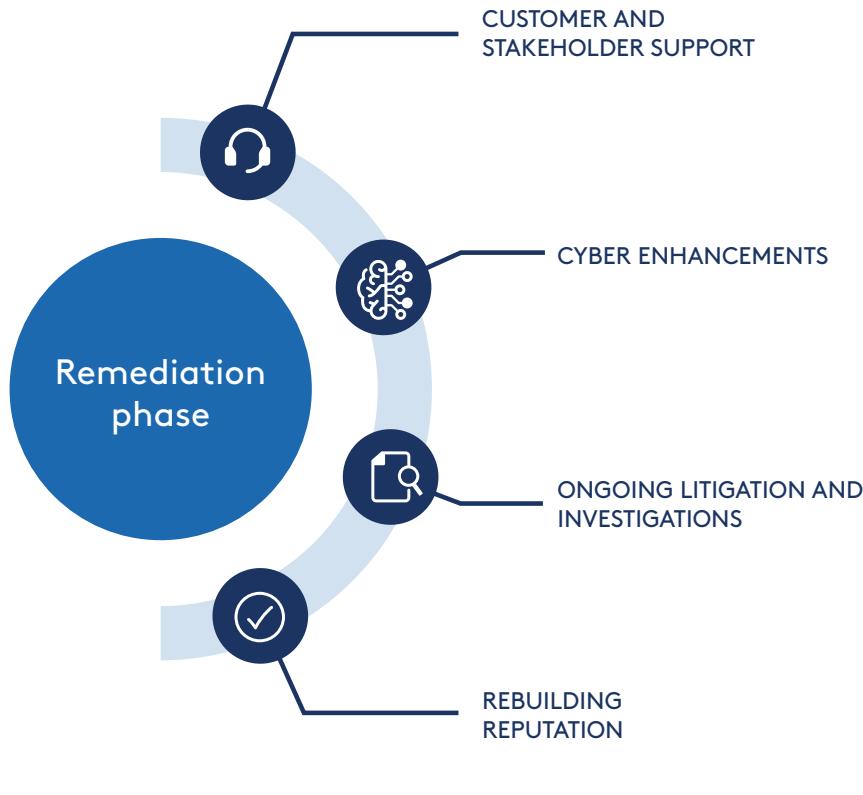
The board should approve, or delegate the approval of, customer-remediation and compensation plans, based on a thorough assessment of the financial and non-financial risk of harm and any consequential loss.

Customer-remediation plans should consider the following:

- The provision of specific advice and access to resources for individuals whose personal data may have been stolen, including access to credit monitoring and dark web monitoring, where appropriate.
- Advice to individuals regarding actions they can take to limit their risk of identity theft and fraud following a data breach, including contacting banks and government agencies to ensure additional monitoring can be put in place and utilising the services of IDCARE.
- Providing advice on the necessity of replacing identity documents, the costs (and any reimbursement) of replacement, and the process for replacing documents, while working closely with relevant government departments.
- Providing access to appropriate counselling or other support services.
- The need to reimburse or compensate impacted individuals or businesses for particular types of harm or damage.

REBUILDING REPUTATION

FIGURE 7: Key elements of the cyber incident remediation phase



Significant cyber incidents are often seen as a breach of customer, employee and community trust, and can cause considerable ongoing reputational damage. The board will need to oversee management's steps to rebuild the organisation's reputation consistent with its established organisational values and objectives.

It is important that the organisation takes appropriate action to demonstrate that it accepts accountability for the incident, notwithstanding the actions of malicious actors.

Accepting accountability can be demonstrated through a clear public acknowledgement, tangible material improvements to the organisation's security program,

removing personal data that is not required to be retained, remaining relentlessly customer focused and escalating complaints rapidly.

The board plays an important 'check-and-challenge' function, determining that the organisation can deliver on commitments to customers and impacted parties in the weeks and months following a cyber incident.

The board should also expect that communications are well-planned, appropriately frequent, take into account the 'voice of the customer' and are aligned with the organisation's long-term remediation objectives.

INCIDENT RESPONSE CASE STUDY 3: Toll Group

In early 2020 Toll Group, one of Australia's largest logistics providers, suffered significant cyber incidents that crippled its business operations and ultimately threatened its solvency.

For John Mullen, then Chair of Toll Group, the ransomware attacks were both an existential IT crisis and a profound challenge to the company's ongoing operations.

"It rapidly moved, for me as Chairman, from being an issue of what is our IT preparedness and what is our strategy, through to a potential insolvency issue," Mr Mullen said. "We had over 50,000 employees around the world who we pay every week, and we couldn't collect cash from our customers.

"That became my major preoccupation."

The Toll Group cyber-attacks have become one of Australia's most high-profile incidents.

Mr Mullen said the attacks highlighted to companies and directors the potential for significant damage that successful ransomware attacks can wreak on a company.

"We had no reason to believe that something of that magnitude would happen," he said. "We had done all the right things. But that was a lesson. Do the right thing and you can still be in trouble."

Mr Mullen credits the Toll executive team for providing detailed and timely information throughout the crisis. Directors were also able to access external advisers, separate from management.

But the challenge was inherent in the complexity of the event, he said, requiring communications to be constantly updated and refined as further details were uncovered.

"As a board we got far more involved [in cyber resilience] following the incidents," he said. **"It really, really sharpens your focus. It's such a complex and fast-moving area that it can be challenging for directors to stay on top of the risk. We went back to square one assuming we were more vulnerable."**

He said for all those reasons, directors should seek independent oversight on a regular basis, comparing cyber assurance to an auditor's review of financials.

"It needs to be regular," he said. "You don't say, 'We're not going to do an audit this year, we did that last year', you just wouldn't do that with finances. You need to systematise [cyber] as well."

Mr Mullen said the incidents were a warning to all organisations – especially small and medium businesses – to be aware of the profound risks of cyber security incidents and take actions to mitigate them. "Do not think you're immune," he said.

John Mullen is a former Chair of Toll and Telstra. He is the current Chair of Qantas, Brambles, Treasury Wine Estates and the Australian National Maritime Museum.

APPENDIX A:

Cyber extortion – Ransomware and data theft



The ASD has identified ransomware as the most destructive cybercrime threat facing Australians due to its high financial and operational cost and other disruptive impacts to victims and the broader Australian community. As highlighted in **Incident Response Case Study 3**, such is the impact of ransomware that it can imperil the ongoing solvency of an organisation.

RANSOMWARE AND DATA THEFT

Ransomware and data theft involves cyber criminals accessing an organisation's systems to gain access to high value systems, data or targets.

LEGALITY OF RANSOMWARE PAYMENTS IN AUSTRALIA

Australia does not currently have any laws that explicitly prohibit the payment of ransom demands. However, the ASD has clear advice for organisations not to pay a ransom as, among other issues, there is no guarantee it will regain an organisation's access to their data, and it may incentivise future attacks.

Although there is no express prohibition on the payment of cyber ransoms in Australia, there are certain laws in place that mean doing so could amount to a criminal offence depending on the facts. These laws include the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) and the *Criminal Code Act 1995* (Cth).

As of November 2024 there is legislation before Parliament that would require the reporting of ransomware payments by businesses above a certain revenue threshold to the Department of Home Affairs.

An organisation experiencing a data theft event should obtain legal advice on paying a ransom or extortion.

The most common form or method of data theft is ransomware – a form of malware designed to seek out vulnerabilities in the computer systems of organisations, both large and small, locking up, stealing and encrypting data, and rendering computers and their files unusable. The ransomware attack is accompanied by a demand for ransom to be paid, often in cryptocurrency, in return for decrypting and unlocking systems.

Cyber criminals may draw on a number of techniques to extract payment from victims, including employing multiple techniques at once – known as double or multiple extortion. While ransomware is a well-known technique, cyber criminals can monetise access to compromised data or systems in many different ways. They may extort victims in return for decrypting data or non-publication of data, on-sell compromised data or systems access for profit, or exploit compromised data or systems for future use.

BOARD DECISION-MAKING

Whether to pay a ransomware or data theft extortion raises difficult legal and ethical questions for directors, including whether a payment promotes further attacks on the organisation. Obtaining external legal advice will often be necessary.

It is important to remember that even if an organisation pays the ransom, it does not guarantee full recovery of their data or that the actor will not retain a copy of the data and continue to access and use that data.

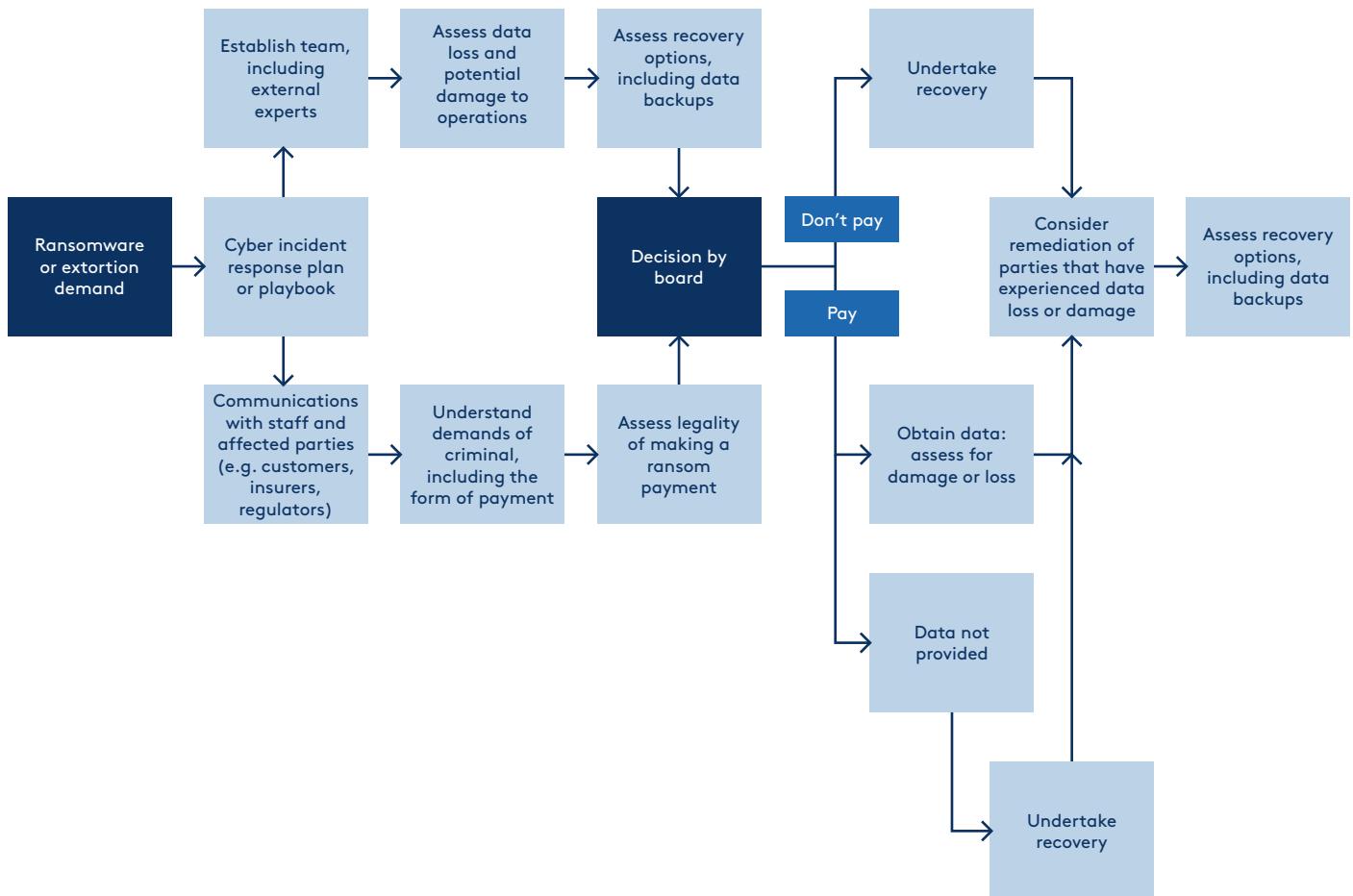
The effectiveness of an organisation's response to an extortion event involving ransomware and/or data theft will depend on how prepared both management and the immediate response team are for such an incident. Developing a Response Plan and the board undertaking simulations (including ransomware and data theft war game exercises) together with management are key steps directors can take. **Principle 5** discusses preparation and recovery in further detail.

Nonetheless, directors should recognise that data theft incidents can be highly complex, with events moving rapidly and information or facts difficult to determine. In addition, communicating and negotiating with criminal threat actors adds significant unreliability and limited trust, including whether the stolen data will be deleted and not otherwise exploited.

Key to board decision-making in a data theft event is obtaining expert external advice, this will likely include cyber security expertise, legal advice, communications or public relations support and close communication with cyber insurers (if applicable). For many organisations, including those under the SOCI Act, there are often obligations to notify regulators and impacted individuals within a specified time frame. In the future, there is likely to be a broader ransomware payment reporting requirement that will apply to organisations above a certain revenue threshold. This is detailed further in **Existing obligations and regulatory requirements**.

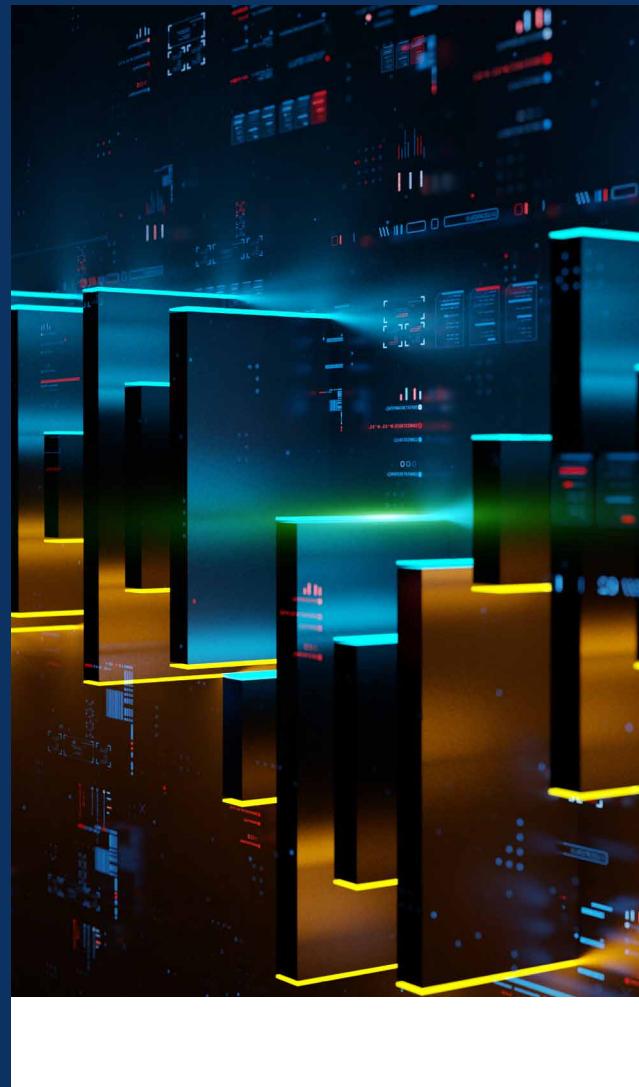
The decision tree below provides a high-level overview of steps and factors directors should consider in the event of a significant data theft event or ransomware attack.

DECISION TREE



Note: The decision tree presents a linear and binary set of events and decisions of one particular form of a data theft incident. However, in practice a data theft event often presents complex decision-making challenges for the board and management based on imprecise, unreliable and fast changing information. It is strongly recommended that appropriate external expertise is obtained to support sound decision-making.

APPENDIX B: Resources



1. Government and industry resources
 - a. ASD, including:
 - i. [Practical Cyber Security Tips for Business Leaders](#)
 - ii. [Ten Things to Know About Data Security](#)
 - iii. [Small business cyber security guide](#)
 - iv. [Cyber supply chains](#)
 - v. [Strategies to Mitigate Cyber Security Incidents, including the Essential Eight Maturity Model](#)
 - vi. [Cyber Incident Response Plan](#)
 - vii. [Cyber Security Partnership Program](#)
 - viii. [ReportCyber](#)
 - ix. [Alerts](#)
 - a. Cyber and Infrastructure Security Centre: [Overview of Cyber Security Obligations for Corporate Leaders](#)
 - i. [National Office of Cyber Security: HWL Ebsworth Cyber Security Incident Lessons Learned](#)
 - c. ASIC, including:
 - i. [Cyber resilience good practices](#)
 - ii. [Key questions for an organisation's board of directors](#)
 - iii. [Market integrity rules for market operators and participants](#)
 - d. APRA, including
 - i. [Prudential Standard CPS 234 Information Security](#)
 - ii. [Prudential Practice Guide CPG 234 Information Security](#)
 - iii. [Prudential Standard CPS 230 Operational Risk Management](#)
 - iv. [Prudential Practice Guide CPG 230 Operational Risk Management](#)
 - v. [Letter \(August 2024\): Additional insights on common cyber resilience weaknesses](#)
 - vi. [Insight article \(November 2021\): Improving cyber resilience: the role boards have to play](#)

- e. Australian Charities and Not-for-profits Commission: Governance Toolkit - Cyber Security
 - f. OAIC, including
 - i. Australian Privacy Principles guidelines: Chapter 11: APP 11 – Security of personal information
 - ii. Notifiable Data Breaches
 - iii. CDR Privacy Guidelines
 - iv. My Health Record
 - g. IDCARE
 - h. Council of Small Business Organisations of Australia:
 - i. Cyber Wardens
 - ii. Cyber Security Resources
 - 2. International standards frameworks
 - a. NIST Cybersecurity Framework
 - b. NIST Zero Trust Architecture
 - c. ISO/IEC 27001 Information Security Management
 - 3. AICD resources
 - a. Course: The Board's Role in Cyber
 - b. AICD publications:
 - i. AICD CSCRC Ashurst Governing Through a Cyber Crisis
 - ii. AICD AISA Cyber Security Handbook for Small Business and Not-for-Profit Directors
 - iii. Directors' Guide to AI Governance
 - c. Director tools:
 - i. Information technology guidance
 - ii. Managing a data breach: Ten oversight questions for directors
 - iii. Data and privacy governance
4. Research and reports
 - a. CSCRC:
 - i. Smaller but Stronger: Lifting SME Cyber Security in South Australia (2022)
 - ii. Case Studies
 - b. Actuaries Institute: Cyber Risk and the role of insurance (2022)
 - c. Insurance Council of Australia: Cyber Insurance: Protecting our way of life, in a digital world (2022)
 - d. National Cyber Security Centre (UK): Cyber Security Toolkit for Boards
 - e. World Economic Forum: Principles for Board Governance of Cyber Risk (2021)

APPENDIX C: Industry requirements and standards



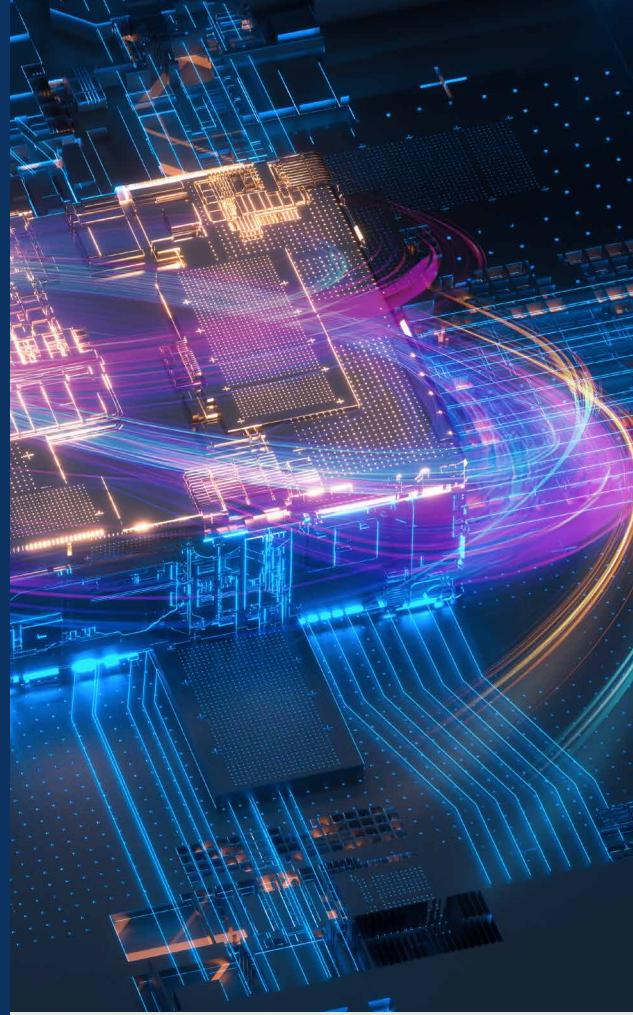
Regulatory obligations on a particular organisation will differ based on its size, industry and jurisdictions in which it operates. In many cases an organisation will have to meet both Commonwealth and state-based obligations, including reporting and notification requirements.

The Cyber Infrastructure and Security Centre publication *Overview of Cyber Security Obligations for Corporate Leaders* is a key source of information on the key Commonwealth cyber security regulatory obligations relevant to the governance of cyber security risk.

Key Commonwealth regulatory frameworks include:

- *Security of Critical Infrastructure Act 2018*
- *Privacy Act 1988 (Cth)*, including Australian Privacy Principles and Notifiable Data Breaches scheme
- APRA prudential standards, including CPS 234 Information Security and CPS 230 Operational Risk Management
- *My Health Records Act 2012*
- Consumer Data Right under the *Competition and Consumer Act 2010*
- ASIC Market Integrity Rules
- Australian Energy Sector Cyber Security Framework
- *Telecommunications Act 1997*

APPENDIX D: SME and NFP director checklist



PRINCIPLE 1:

Set clear roles and responsibilities

- Document, where possible, who has responsibility for cyber security
- Appoint a cyber 'champion' to promote cyber resilience and respond to questions
- Consider whether a director, or group of directors, should have a more active role in cyber security oversight
- Identify our key digital providers and understand their cyber controls

PRINCIPLE 2:

Develop, implement and evolve a comprehensive cyber strategy

- Proactively identify low-cost opportunities to enhance cyber capability
- Assess whether utilising reputable external providers will enhance cyber resilience compared with managing in-house
- Identify key operational and customer data, who has access to the data and how it is protected
- Limit access to key systems and data and regularly review access controls
- Regularly repeat cyber security training and awareness among all employees
- Promote strong email hygiene (e.g. avoid suspicious email addresses and requests for login or bank details)

PRINCIPLE 3:

Embed cyber security in existing risk management practices

- Patch and update applications and anti-virus software
- User application hardening – limit interaction between internet applications and business systems
- Limit or restrict access to social media and external email accounts
- Restrict use of USBs or external hard drives
- Restrict operating system and software administrative privileges
- Implement multi-factor authentication
- Maintain and regularly test offline backups of critical data
- Ensure that departing employees and volunteers no longer have access to systems and passwords, or physical access to sites or sensitive data

PRINCIPLE 4:

Promote a culture of cyber resilience

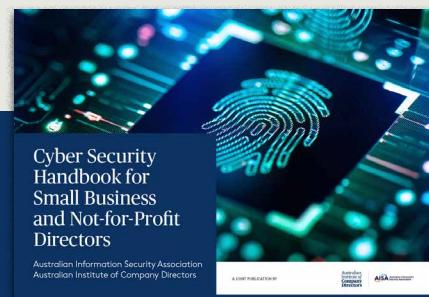
- Mandatory training and phishing testing for all employees, and volunteers where appropriate
- Regular communications to employees on promoting strong cyber practices, including email hygiene. The communications could be electronic (e.g. email reminders) or physical (e.g. signage in the workplace)
- Incentivise strong cyber practices, for example small rewards for performance on phishing exercises
- Pick a staff member to be a ‘cyber security leader’ to promote strong cyber practices and respond to questions from other staff
- Subscribe to ASD alerts to stay across emerging cyber threats

PRINCIPLE 5:

Plan for a significant cyber security incident

- Prepare a Response Plan, utilising online templates if appropriate
- If practical, conduct a simulation exercise or test various scenarios against the incident response plan
- Ensure physical back-ups of key data and systems are regularly updated, tested and securely stored
- Maintain offline lists of who may assist in the event of a significant cyber security incident and which key stakeholders to communicate with

Comprehensive guidance for directors of SMEs and NFPs is contained in this guide from the AICD and the Australian Information Security Association



APPENDIX E: Glossary

The ASD has an extensive online glossary of cyber security relevant terms available on their [website](#).

Term	Definition
AFSL	Australian Financial Services License
APRA	Australian Prudential Regulation Authority
ASD	Australian Signals Directorate
ASIC	Australian Securities and Investments Commission
ASX	Australian Securities Exchange
Cloud computing	A service model that enables network access to a shared pool of computing resources such as data storage, servers, software applications and services
Cloud service provider	A company that offers some component of cloud computing to other organisations or individuals
Cyber and Infrastructure Security Centre (CISC)	The regulator of the SOCI Act, contained in the Department of Home Affairs
Essential Eight	The eight essential mitigation strategies that the ASD recommends organisations implement as a baseline to make it much harder for adversaries to compromise their systems
Generative artificial intelligence	Deep-learning models that can generate high-quality text, images, and other content based on the data they were trained on
IDCARE	Australia and New Zealand non-government identity and cyber support service
ISO 27001	International Standard Organization 27001 Information Security Management
Least privilege	A security model in which users, processes, and systems are granted only the minimum permissions necessary to perform their required functions
LLMs	Large language models are generative AI systems capable of understanding and generating human language by processing vast amounts of data
Malware	Malicious software used to gain unauthorised access to computers, steal information and disrupt or disable networks. Types of malware include Trojans, viruses and worms

Term	Definition
Multi-factor authentication (MFA)	A method of computer access control in which a user is granted access only after successfully presenting several separate pieces of evidence to an authentication mechanism – typically at least two of the following categories: knowledge (something they know), possession (something they have), and inherence (something they are)
NDB scheme	Notifiable Data Breaches scheme
NIST	National Institute of Standards and Technology (US)
NFP	Not-for-profit; an organisation that does not operate for private benefit
OAIC	Office of the Australian Information Commissioner
Penetration testing	A method of evaluating the security of an ICT system by seeking to identify and exploit vulnerabilities to gain access to systems and data. Also called a 'pen test'
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (such as bank details), encouraging them to open a malicious attachment, or visit a fake website that will ask the user to provide sensitive information or download malicious content
Ransomware	Malicious software that makes data or systems unusable until the victim makes a payment
Secure by design	An approach to software and hardware development that builds security into the architecture and design from the start, rather than adding it as an afterthought
SME	Small-to-medium enterprise
SOCI Act	Security of Critical Infrastructure Act 2018
Zero Trust	A security model that requires strict identity verification and continuous authentication for every user, device, and application attempting to access resources within a network

ACKNOWLEDGEMENT OF COUNTRY

The Australian Institute of Company Directors acknowledges the First Nations people across this Country. We acknowledge the Traditional Custodians of the Lands on which our organisation is located and where we conduct our business. We pay our respects to the Elders, past and present, and recognise those who continue to promote and protect First Nations cultures. The Australian Institute of Company Directors is committed to honouring First Nations peoples' unique cultural and spiritual relationships to the Skies, Lands, Waters, and Seas, and their rich contribution to society. We acknowledge the past and stand together for our future.

ABOUT CSCRC

The CSCRC develops cyber security capability and capacity to help keep Australia safe. We do this by developing innovative, real-world research and cultivating outstanding talent to solve pressing cyber security challenges for the nation.

ABOUT AICD

The Australian Institute of Company Directors is committed to strengthening society through world-class governance. We aim to be the independent and trusted voice of governance, building the capability of a community of leaders for the benefit of society. Our membership includes directors and senior leaders from business, government and not-for-profit sectors.

DISCLAIMER

The material in this publication does not constitute legal, accounting or other professional advice. While reasonable care has been taken in its preparation, the AICD and CSCRC do not make any express or implied representations or warranties as to the completeness, reliability or accuracy of the material in this publication. This publication should not be used or relied upon as a substitute for professional advice or as a basis for formulating business decisions. To the extent permitted by law, the AICD and CSCRC exclude all liability for any loss or damage arising out of the use of the material in the publication. Any links to third-party websites are provided for convenience only and do not represent endorsement, sponsorship or approval of those third parties, any products and services offered by third parties, or as to the accuracy or currency of the information included in third-party websites. The opinions of those quoted do not necessarily represent the view of the AICD and CSCRC. All details were accurate at the time of printing. The AICD and CSCRC reserve the right to make changes without notice, where necessary.

COPYRIGHT

Copyright strictly reserved. The text, graphics and layout of this guide are protected by Australian copyright law and the comparable law of other countries. The copyright of this material is vested in the AICD and CSCRC. No part of this material can be reproduced or transmitted in any form, or by any means electronic or mechanical, including photocopying, recording or by any information storage and retrieval systems without the written permission of the AICD and CSCRC.

**For more information about Cyber Security Governance Principles Version 2,
please contact:**

E: policy@aicd.com.au

 JOIN OUR SOCIAL COMMUNITY

aicd.com.au