Australian Institute *of* **Company Directors**

CYBER SECURITY COOPERATIVE RESEARCH CENTRE

Cyber Security Governance Principles

October 2022

Table of Contents

Foreword

> "Directors have a critical role to play and must seek to lift their own cyber literacy levels, recognising that this is a key risk that can never be eliminated but can be effectively managed."

— **Hon Clare O'Neil MP**
Minister for Home Affairs and Minister for Cyber Security

As Australians entrust their most sensitive data to organisations, there is a legitimate expectation that it will be protected. Keeping Australians' data safe requires strong collaboration between government, business and industry. Australia must work as one team to build up the defences we need to protect our society and economy. It is the responsibility of all organisations across Australia to make stronger cyber security practices a priority and make the necessary investments where needed. There is much that even small business and not-for-profits can do to ensure that the data they use and store is securely protected.

I am therefore delighted to see the Australian Institute of Company Directors (AICD) and the Cyber Security Cooperative Research Centre (CSCRC) partnering to publish a set of Cyber Security Governance Principles. These Principles provide a clear and practical framework for organisations to build stronger cyber resilience. Directors have a critical role to play and must seek to lift their own cyber literacy levels, recognising that this is a key risk that can never be eliminated but can be effectively managed.

I commend the Principles to Australian organisations of all sizes and reinforce the Australian Government's commitment to work hand in glove with business and industry to develop world class cyber security practices.

Hon Clare O'Neil MP
Minister for Home Affairs and Minister
for Cyber Security

Snapshot of the Principles

1. Set clear roles and responsibilities

Defining clear roles and responsibilities is a foundational component of building effective cyber resilience

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

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 periodically on board agendas
2. Chair and 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

2. Develop, implement and evolve a comprehensive cyber strategy

A cyber strategy, proactively overseen by the board, can be a business enabler by identifying opportunities for the organisation to build cyber resilience

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

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 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

3. Embed cyber security in existing risk management practices

Cyber risk is an operational risk that fits within an organisation's existing approach to risk management

While cyber risk cannot be reduced to zero there are a number of accessible and low-cost controls that all organisations can utilise

The board should regularly assess the effectiveness of cyber controls to account for a changing threat environment, technology developments and the organisation's capabilities

GOVERNANCE RED FLAGS:

1. Cyber risk 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

4. Promote a culture of cyber resilience

A cyber strategy, proactively overseen by the board, can be a business enabler by identifying opportunities for the organisation to build cyber resilience

Regular, engaging and relevant training is a key tool to promote a cyber resilient culture, including specific training for directors

Incentivise and promote strong cyber security practices, including participating in phishing testing and penetration exercises

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

5. Plan for a significant cyber security incident

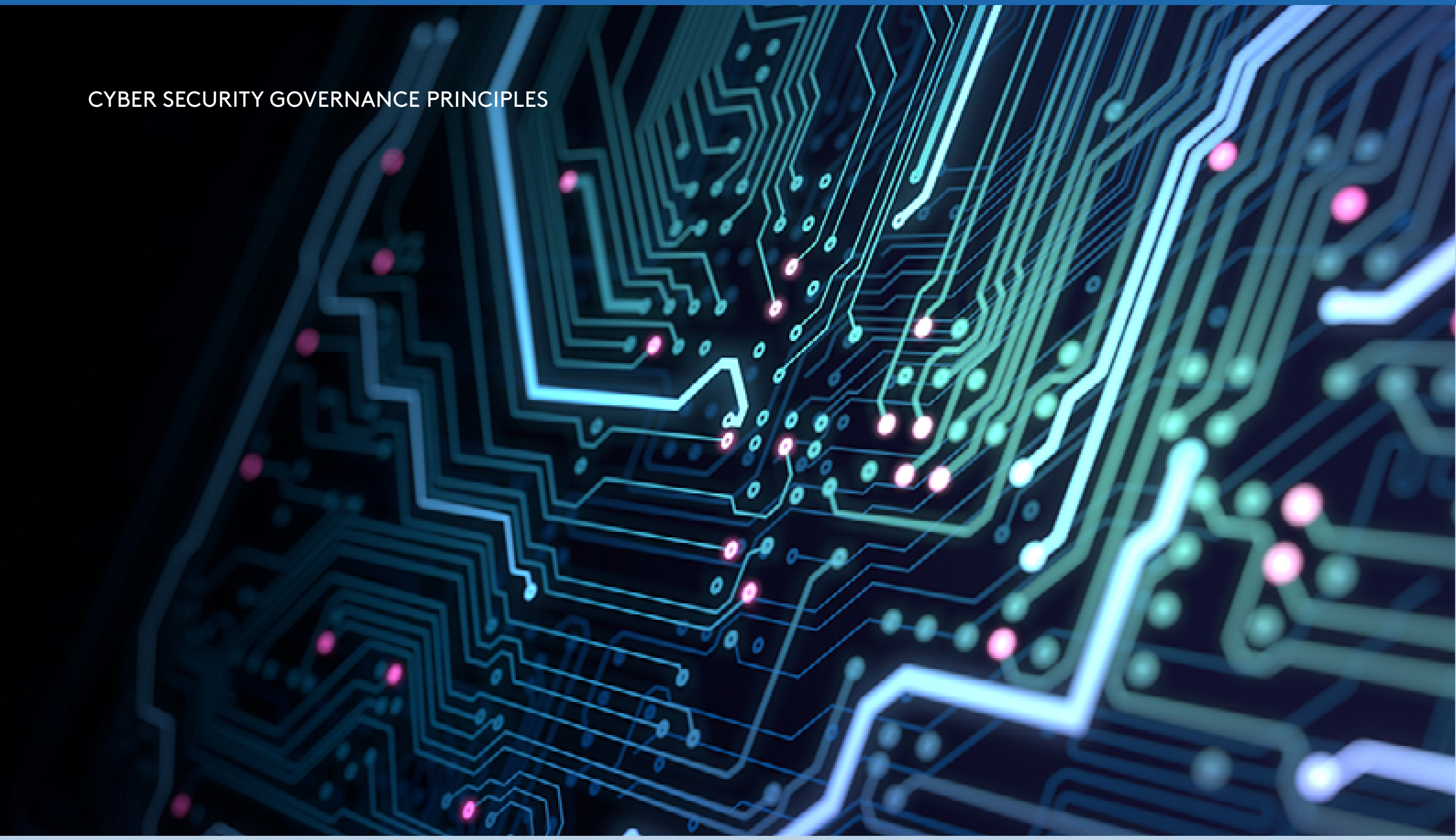
Directors should proactively prepare and plan for a significant cyber incident

Simulation exercises and scenario testing are key tools for the board and senior management to understand roles and responsibilities

A clear and transparent approach to communications with all key stakeholders in a significant cyber incident is critical in mitigating reputational damage and allowing for an effective recovery

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. Who has internal responsibility for the management and protection of our key digital assets and data?
4. Where, and with whom, are our key digital assets and data located?

Cyber risk management

5. Is cyber risk specifically identified in the organisation's risk management framework?
6. How regularly does management present to the board or risk committee on the effectiveness of cyber risk controls?

Cyber resilient culture

7. Is cyber security training mandatory across the organisation and is it differentiated by area or role?
8. How is the effectiveness of training measured?

Cyber incident planning

9. Do we have a Cyber Incident Response Plan, including a comprehensive communications strategy, informed by simulation exercises and testing?
10. Can we access external support if necessary to assist with a significant cyber security incident?

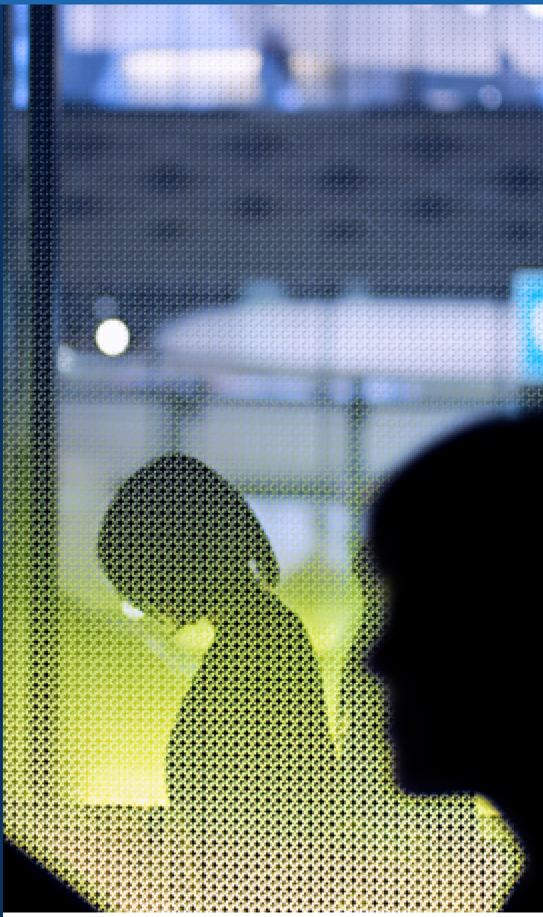
Terminology

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 terminology of cyber security, consistent with the threat itself, evolves at a rapid pace. The Australian Cyber Security Centre (ACSC) 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**.

Cyber Security	• An overarching term that captures the steps, measures and processes used to protect and defend 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 organsation
Cyber Threat	• Any attack or event, or potential attack or event, that may harm an organisation's information systems and infrastructure • Cyber threat includes attempts by external parties to breach an organisation's cyber defences
Cyber Incident	• An unauthorised cyber security event, or a series of such events, that has the potential to compromise an organisation's business operations • Cyber incidents cover the spectrum of events from accidental data losses, such as an employee misplacing a USB, to criminal attacks, issue motivated groups and state sponsored actors
Digital	• Steps or processes taken by organisations to generate and store data via internet facing systems • Data generated via internet facing systems 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 businesses place more of their key assets and systems in internet facing systems, with all organisations susceptible to attack. The cyber threat environment is incredibly dynamic and boards needing to remain responsive to the threat and the cyber resilience of the organisations they govern.

Cyber incidents can have a significant and at times 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 individual hacker gaining access to data or an employee misplacing a USB. 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 the **Toll Case Study in Principle 5**.

It is unsurprising 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 are a 'living document' which will be periodically reviewed to reflect the evolving threat and regulatory landscape.

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 experiences and invites feedback by email to **policy@aicd.com.au**

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.

Threat environment

Threat actors in cyber security can be individuals, 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 actors 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 cyber-criminal 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 in **Appendix A**.

AUSTRALIAN TRENDS (2020/21)

- More than 67,500 cybercrime reports – one every eight minutes
- Losses from cybercrime exceeded $33 billion
- Almost 500 reported ransomware attacks
- 25 per cent of cyber incidents targeted Australia's critical infrastructure

Source: ACSC Annual Cyber Threat Report 2020-21

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. According to the ACSC, a quarter of reported cyber incidents in 2020-21 were associated with Australia's critical infrastructure or essential services. The health care, food distribution, financial services and energy sectors are key targets domestically and internationally.

Threat to NFPs and SMEs

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 topic.

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.

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 and NFP
- These steps are collated in a checklist at **Appendix D**

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**).

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 ensuring 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

Directors of entities that hold an Australian Financial Services License (**AFSL**) are also subject to general and specific obligations under Corporations Act. A recent decision of the Federal Court of Australia, 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.

Duty to advise the market where there is an effect on a company's share price

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. Below is a high-level summary of key cyber regulatory frameworks. A summary of certain industry specific obligations is provided at **Appendix C**, including Australian Prudential Regulation Authority (**APRA**) prudential requirements relevant to the governance and management of cyber security risk.

PRIVACY ACT

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

Two key regimes under the Privacy Act 1988 (the **Privacy Act**) that directors should be aware of are:

1. Notifiable Data Breaches (**NDB**) scheme – requiring an organisation to notify affected individuals and the Office of the Australian Information Commissioner (**OAIC**) as soon as practicable of a material data breach

Australian Privacy Principle 11 – Security of Personal Information (**APP 11**) – requiring an organisation to take active measures to ensure the security of personal information it holds

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 an incident.

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

ACSC STRATEGIES TO MITIGATE CYBER SECURITY INCIDENTS (INCL ESSENTIAL EIGHT)

The ACSC, a part of the Australian Signals directorate, has published **37 Strategies** to Mitigate Cyber Security Incidents. The strategies can be implemented by organisations of all sizes as part of regular cyber hygiene practices and are divided across three primary objectives – preventing attacks, limiting attack impact and data availability. A component of these strategies is the Essential Eight Maturity Model, which is often referenced or referred to as a baseline benchmark or maturity model for Australian organisations to meet.

ASIC V RI ADVICE GROUP PTY LTD

In 2021, the Australian Securities and Investments Commission (**ASIC**) commenced its first enforcement action against AFSL holder, RI Advice Group Pty Ltd (**RI Advice**), for breaches arising from a failure to have adequate cyber security policies, systems and resources.

A number of weaknesses were identified in the management of cyber risks across the RI Advice network, including a) outdated antivirus software; b) no filtering or quarantining of emails; c) no backup systems in place or backups being performed; and d) poor password practices (e.g. sharing of passwords between employees and use of default passwords).

In May 2022, the matter settled between ASIC and RI Advice and the Federal Court noting in its judgment that that RI Advice had contravened its AFSL obligations under the Corporations Act. The Court's reasoning highlighted that while it is not possible to reduce cyber risk to zero, RI Advice was expected, not only to have identified the cyber risks and implemented measures to address them, but to ensure that its systems remained fit for purpose over time to keep pace with the escalating risk.

ASIC in commentary on the case noted that it serves as a timely reminder for company directors about cybersecurity risk oversight, including that an organisation's risk management framework adequately addresses cyber security risk, and that controls are implemented to protect key assets and enhance cyber resilience.

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 on the cyber resilience of an organisation 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. However, directors should gain some comfort in understanding how their organisation is prepared to respond in the event of a cyber incident.

While it is not the role of the board to directly manage cyber risk, it is the board that has 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 comprehensive 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.

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 evolving 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 be reviewed regularly to confirm that roles and responsibilities are clear, especially with respect to evolving risks such as cyber security.

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, and 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 is fostering a cyber resilient culture within the organisation and modelling effective cyber practices (discussed at **Principle 4**). Every director should take responsibility to enhance their own skills and knowledge on cyber security.

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 oversight of cyber security
- Collect data where possible on the effectiveness of cyber risk practices

ROLE OF MANAGEMENT

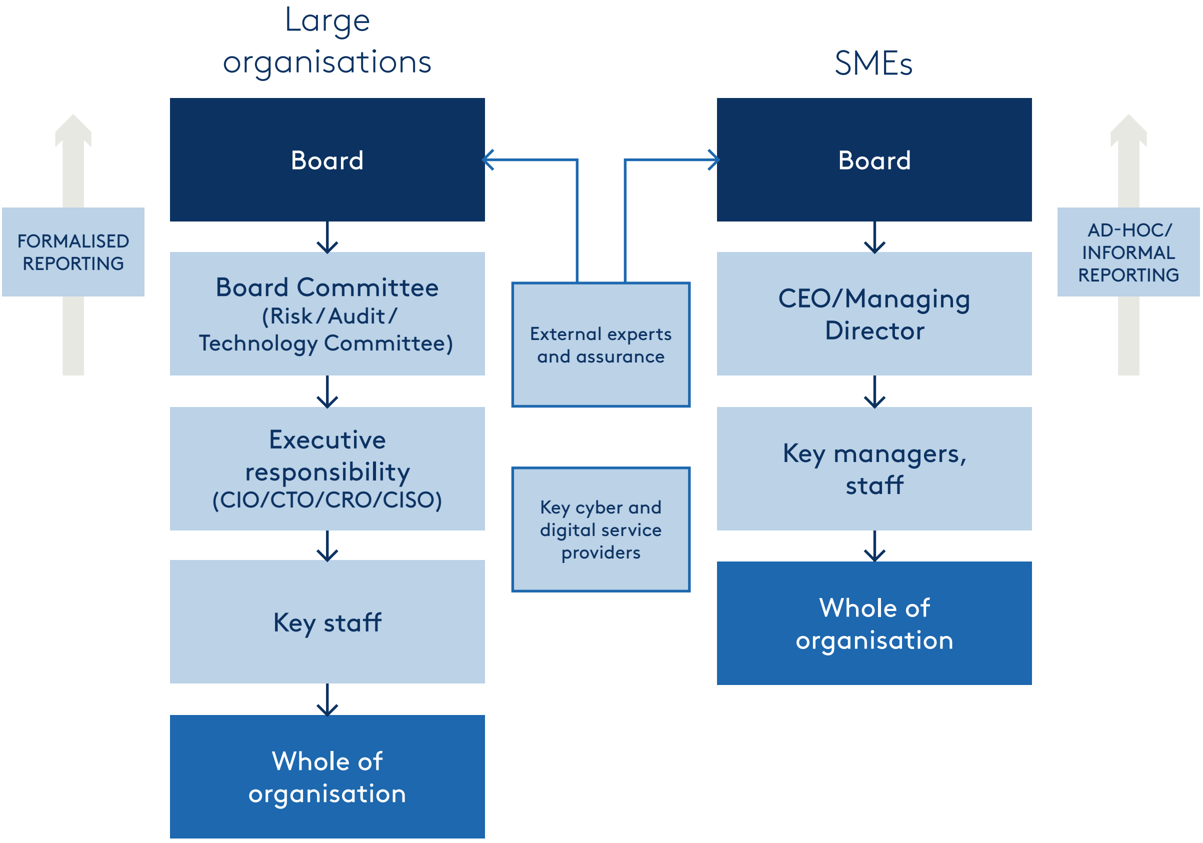
There is no strict rule on where responsibility for cyber security leadership should sit at the management level. Ideally, management responsibility for cyber security must ultimately lie with the person who best understands cyber security, the threat landscape and the organisation's strategy and approach to mitigating risk.

At large organisations, 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 the accountable executive and business unit delegation, cyber security should be considered a shared enterprise risk with responsibility across the full executive team.

At larger organisations, responsibilities are cascaded from management through the organisation to particular individuals. In these circumstances, individual cyber responsibilities should be documented in position descriptions or role statements. Depending on the nature of the business 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.

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.


Large organisations
SMEs
FORMALISED REPORTING
Board
Board Committee (Risk/Audit/ Technology Committee)
Executive responsibility (CIO/CTO/CRO/CISO)
Key staff
Whole of organisation
External experts and assurance
Key cyber and digital service providers
Board
CEO/Managing Director
Key managers, staff
Whole of organisation
AD-HOC/ INFORMAL REPORTING

SHARED RESPONSIBILITIES

A challenge at many organisations is that core cyber security roles and responsibilities may not be located in one business area or team. 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 assist staff better understand where responsibility for cyber sits across an organisation. Additionally, an informal working group of key staff that meet regularly to discuss cyber risks and developments may be an effective on-going 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 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 responsibility in enhancing the cyber resilience of the organisation. This requires a whole of organisation approach to being vigilant to cyber threats, undertaking training and education as well as ensuring there is a cyber incident response plan and that key defences, such as software updates and password security, are 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). 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 to directors.

At larger organisations, information may be presented as a dashboard or heatmap 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.

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

BOX 1.3 COMMON BOARD REPORTING METRICS

- 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 assessment, 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, ACSC alerts and intelligence shared by other organisations, and response to threats

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.

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.[1]

[1] Please see the AICD Director Tool: Directors' right to seek external professional advice (available here), for further information on a director obtaining external advice.

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, International Standards Organisation). 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.

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 respond to 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.

BOX 1.4 GOVERNANCE RED FLAGS

1. Cyber security not featuring periodically on board agendas
2. The board not annually reviewing skills to ensure that directors have an appropriate understanding of cyber 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

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, including 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 that covers from creation to destruction?
- **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?

The role of insurance

Organisations often obtain cyber insurance that can provide a measure of protection in the event of losses from a critical cyber incident. While cyber insurance may be necessary for certain organisations, the often high cost and restricted or tailored coverage of a particular policy means that a board should carefully consider if it is appropriate and/or value for money for their organisation.

In addition to financial compensation, a key motivation 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.

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.

There is a limited pool of providers of cyber insurance in Australia and the often-tailored nature of policies means they can be relatively high cost and may have specific conditions or exclusions of particular cyber incidents (e.g. act of war). As there are no standard terms and conditions for cyber policies, 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 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.

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 multi-factor authentication and comprehensive cyber security training, the attacker was able to gain access to their 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 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's and letters were issued promptly advising them of the possibility their personal information was accessed. Assistance was provided, included standing up the 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,Chair of Spirit Super, Director of Tasmanian Development Board, AICD, Propel Funeral Partners and President Elect of the Institute of Actuaries Australia.

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 a core component of understanding and enhancing cyber capability
3. A robust cyber strategy will account for the importance, and potential risks, associated with key third party suppliers

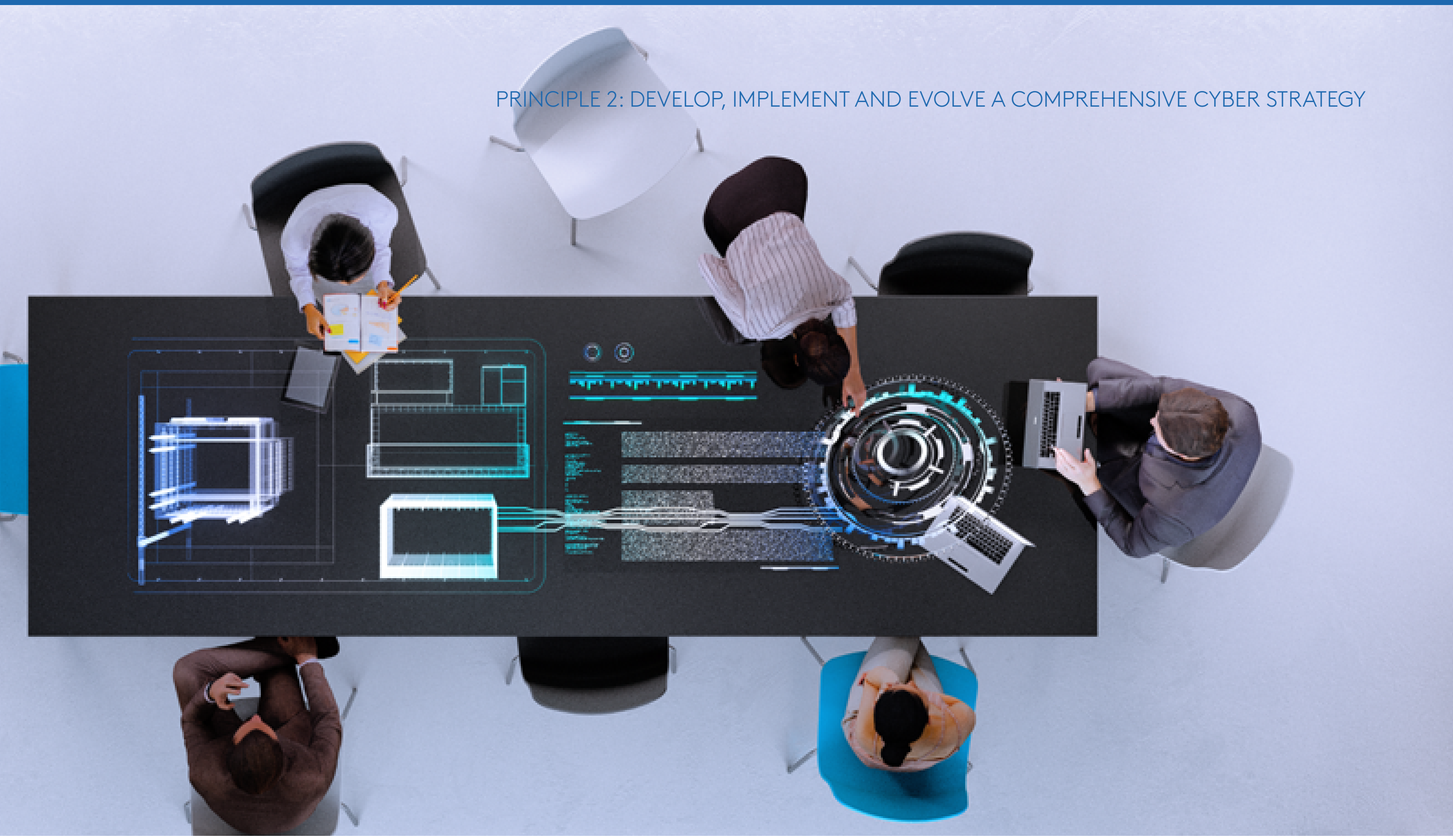
Assessing and enhancing internal capability

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 business; 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 at **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 the Box 2.1. The discussion of these elements is covered in different sections of the Principles – the relevant principles are highlighted in the box.

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



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 (**Principles 2** and **3**)
3. **Assess and enhance:** Understand internal cyber capability, create a plan to enhance capability and promote a cyber resilient culture (**Principles 2** and **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**)

For many SMEs and NFPs, a lengthy cyber strategy is unlikely to be necessary and may act as a barrier to nimble responses to cyber threats. However, for smaller businesses in industries such as healthcare or those that provide services to larger organisations, a documented cyber strategy will often be required. For these businesses 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.

KEY DIGITAL ASSETS AND DATA

Each organisation will have a set of key digital assets that if damaged or lost in a significant cyber incident would represent a significant threat to its ongoing business operations.

For organisations of all sizes the key digital assets, or 'crown jewels', are most commonly critical customer and employee related data, and the technology infrastructure that facilitates doing 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.

A core component of developing a cyber strategy is meticulously identifying the organisation's key digital assets and data documenting the answers to the questions in Box 2.2.

A board should have visibility over these key elements and receive regular updates from management as part of ongoing evaluation processes (see below). This assessment will assist directors to understand where cyber vulnerabilities may exist and will be a key input into risk management processes – discussed in **Principle 3**.

BOX 2.2 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 suppliers 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 GOVERNANCE – KNOW YOUR OBLIGATIONS

Storing large amounts of sensitive customer and organisational data, beyond a legislative requirement, creates a significant risk to customers, and the organisation, as it serves as a valuable target for cyber criminals looking to steal and use that information.

To ensure effective data governance, directors should also understand the extent of personal customer or employee data that is being stored and clearly understand the legislative or regulatory reasons for doing so. All directors should expect of management, on an annual basis, to provide a 'map' of sensitive data that 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 reason for holding this data.

To minimise the risk of data theft or loss, organisations should only collect and store the minimum amount of personal information that is legally 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 keep some identity documents (such as requirements in satisfaction of the telecommunications metadata obligations) and in this case, directors need to be satisfied that data obtained for a legislative obligation is both secure (as required by law) but that data has also not been stored for 'other reasons' in the organisation.

Importantly, many organisations fail to securely delete or destroy sensitive customer or organisational data once systems are replaced or the data is no longer required. This data (if not securely destroyed and on hardware) can often be readily accessed by third parties. Therefore, lifecycle management of all data must be part of any organisation's cyber security strategy and should include secure destruction of all sensitive data.

All sensitive data should be stored in an encrypted and secure manner, and access to such data strictly monitored.

A regular 'spring clean' of all data collected and stored is an effective risk control as part of a broader data management strategy.

BOX 2.3 GOVERNANCE RED FLAGS

1. Lack of formal documentation of the organisation's approach to cyber security
2. Limited understanding of location of key digital assets, 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, protected and deleted

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 to 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 used, 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.

Common frameworks or maturity models that are utilised in benchmarking exercises can include:

1. ACSC **Strategies to Mitigate Cyber Security Incidents**, including the Essential Eight Maturity Model
2. International Standards Organisations (ISO) standards under the **ISO 27000 series**
3. National Institute of Standards and Technology's (NIST) **cybersecurity framework and/or Zero Trust Architecture**

ENHANCING CAPABILITY

A cyber strategy often encompasses steps an organisation will take over a certain period to enhance its cyber capabilities.

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. Doing so would not only enhance cyber capability and resilience, but also have broader business benefits, such as improving reputation amongst stakeholders and maintaining a competitive advantage.

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 2.4 lists a series of practical enhancements focused on smaller organisations drawn from ACSC guidance, however these are relevant to all organisations.

Key third party suppliers

It is equally vital that directors have an understanding of the cyber security capabilities of key third party suppliers who support or manage the organisation's key assets and data.

Increasingly, organisations of all sizes utilise external providers to provide core business services and process and store key data. For example, the software and IT infrastructure of cloud providers are commonly used to facilitate payment and invoice processing, internal payroll, accounting services, customer databases and word-processing software.

In general, utilising a reputable cloud provider will provide greater cyber protections than if the organisation were to manage these functions in-house. However, poor internal cyber practices (e.g. weak password settings or lack of multi-factor authentication) when utilising the provider's services can expose the organisation to potentially significant cyber incidents. Additionally, providers can themselves suffer significant cyber incidents that impact their customers so conducting due diligence on key external providers is critical.

A board should have sufficient visibility of the key third party suppliers, what key digital assets and data they manage or host and what risk controls are in place and importantly, a direct communications channel if they need to notify the organisation of a data breach or issue. Directors should have confidence that management, and the organisation more broadly, has the appropriate internal capabilities and risk-management processes in place to appoint and monitor key external providers. This includes understanding the extent of an organisation's dependence on a provider's service, what data a provider may hold or have access to, the jurisdiction of not just the provider but where they will store the organisation's data, and any vulnerabilities associated with the arrangements that may exist.

At 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 from 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 there should be in place to provide confidence.

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 SMEs AND NFPs – PRACTICAL CYBER CAPABILITY ENHANCEMENTS

1. Utilise the ACSC Cyber Security Assessment Tool to identify the cyber security strengths of the organisation and understand areas for improvement
2. Assess whether utilising reputable external providers will enhance cyber resilience over managing in-house
3. Assess whether there is certain data (e.g. employee or customer data) that does not need to be collected
4. Establish an Access Control System to determine who should have access to what
5. Regularly repeat cyber security training and awareness amongst all employees
6. Promote strong email hygiene (e.g. avoid suspicious email addresses and requests for login or bank details)

(Source: Drawn from ACSC Small Business Cyber Security Guide)

Case Study 2: 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 key digital assets, according to director Catherine Brenner FAICD.

Key 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 paper 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, both by which providers and in which locations 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

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, technology developments and the organisation's capabilities

Cyber-risk appetite

Cyber-risk appetite is, in broad terms, the risk that 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 (i.e. 'crown jewels') 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, an 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.

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.

BOX 3.1 QUESTIONS FOR DIRECTORS TO ASK

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

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, it is central to sound risk governance that directors understand 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 ACSC'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 in mitigating 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 already embedded risk frameworks is 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.

Avoid

- Avoiding cyber risks through ceasing or eliminating certain activities
- For example, avoiding the collection and storage of unecessary customer data

Mitigate

- Reducing cyber risks by implementing internal processes or utilising external service providers
- For example, implementing multi-factor password authentication, ensuring patching and anti-virus software is up to date and educating all staff on what cyber threats to look out for on a daily basis

Transfer

- Transfering, in part or fully, specific elements of cyber risk to external third parties
- Outsourcing systems and functions to third party providers may alleviate an organisation having specific IT infrastructure and systems

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, by themselves it may be challenging for directors 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 on cyber incidents should have directors on notice to engage regularly with management to understand what inputs are informing the level of risk assessment.

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 to 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 3.2 SMEs AND NFPs – RISK CONTROLS

1. Patch and update applications and anti-virus software
2. Configure Microsoft Office macro settings (e.g. only allow macros from trusted sourced)
3. User application hardening – limit interaction between internet applications and business systems
4. Limit or restrict access to social media and external email accounts
5. Restrict use of USBs or external hard drives
6. Restrict operating system and software administrative privileges
7. Implement multi-factor authentication
8. Maintain offline backups of key data
9. Ensure that departing employees and volunteers no longer have access to systems and passwords

BOX 3.3 GOVERNANCE RED FLAGS

1. Cyber risk 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 roles

Case Study 3: Constantly evolving risk management 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 key assets (or 'crown jewels') which could be most impacted by a cyber event.
- **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

KEY POINTS

1. A truly cyber resilient culture begins at the board and must flow through the organisation
2. Regular, engaging and relevant training is a key method 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 in a manner that builds awareness

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 has a central role to play in promoting and demonstrating a cyber security mindset. Governance decisions, and the oversight of cyber risk management, should seek to 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. Frequently significant cyber incidents have an element of human error (e.g. an employee opening a malicious email) and 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 outlined below.

Behaviour and language

- Ongoing cyber awareness training is completed by all employees, including by directors
- Embedding a common and accessible language when talking about cyber security
- Being open and honest about cyber risks to the organisation and encouraging all staff to play their role in promoting cyber resilience
- Cyber training and phishing exercises promote a culture of continuous learning rather than criticising employees for poor understanding

Governance

- Clearly defining key roles and responsibilities for cyber security management
- 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)

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
- Rewarding conduct such as transparency and early reporting of cyber breaches (or attempted breaches such as phishing)

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 the board through reporting should have visibility of training performance, including differences between business areas.

In larger organisations, it may be appropriate that certain business functions or key personnel that have greater exposure to key digital assets, systems and infrastructure receive more in-depth training and more frequently. External training providers can assist with technical 'deep dives' where appropriate for specific cohorts of staff.

Cyber awareness training and technical 'deep dives' should not be limited to staff, with directors and senior executives undertaking similar cyber security training and upskilling.

BOX 4.1 QUESTIONS FOR DIRECTORS TO ASK

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

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 ACSC alerts to stay across emerging cyber threats

In addition to training, best practice at larger organisations is for directors and senior executives to have additional technical controls and security settings associated with use of systems (e.g. email) and devices.

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 cyber security or digital skills. In such cases, having a director with deeper knowledge may provide the full board with additional insight, although it is critical that remaining board members do not abdicate responsibility for cyber security to that one individual.

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 incidents.

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 and the ACSC in the event of a cyber incident.

Collaboration

Directors can also instill an outward and proactive focus on the cyber threat landscape by encouraging management to participate in information sharing and collaboration with regulators 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 **ACSC Partnership Program** and Joint Cyber Security Centres.

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 4.3 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 IT staff to manage)
4. There is a culture of 'exceptions' or workarounds for board and management with respect to cyber hygiene and resilience

Case Study 4: Resilience testing is key to promoting a culture of cyber resilience

Experienced director Anne Templeman-Jones FAICD has found that testing is central to promoting a culture of cyber resilience across an organisation. Ms Templeman-Jones' key observations as a director participating in resilience testing are:

1. 'To pay or not to pay' isn't the biggest issue nor guarantee your data is returned with the encryption key and operating environment is restored. The speed at which you can restore the operating environment and access to data is critical for avoiding business failure.
2. Seek legal advice on paying a ransom prior to an event, so that you are well informed of Australian law, director's obligations and laws in other jurisdictions in which you or your customers may operate. You will need to have this advice refreshed should an incident occur and before you make a decision.
3. A cyber strategy must be designed to protect, respond and reactivate. This requires a framework that is tested through regular controlled and uncontrolled outages. Penetration tests and white box exercises (be they by management or third parties) are excellent methods to learn how to be prepared to respond. Internal Audit can also play a role in identifying weaknesses in the control environment and opportunities for improvement.
4. To create a cyber security mindset, the board and management need to know what data and systems are valuable, what types of cyber crises they may need to manage should the data be stolen or systems compromised, and can operations be restored in the event of an attack:
   - Data – know what it is, where it is and its value;
   - System resilience and the ability to restore operations – has management tried a shut down and full restore from a backup? What is the alternative if your platform is also compromised;
   - What is the stakeholder communication strategy – for example which law enforcement agencies need to be contacted, what backup plans might you have with other providers to assist customers?
5. The board should participate as observers during a ransomware exercise and a committee of the board be delegated to work with management to consider information as it comes to light. These may be aspects such as business and customer impact, regulator communications, and any required disclosure. The committee might consist of the CEO/MD, Chair of the Board, Chair of the Audit and Risk Committee and the Group Counsel.
6. The fastest route to restoration in the event of a significant cyber security event is having secure backups, an operating platform alternative upon which to restore and one that has been tested and re-tested.
7. Some director responsibilities cannot be delegated during a significant cyber security incident:
   - in respect of any contractual arrangement with third parties brought in to assist and the decisions they might make in terms of a course of action – consideration should be given to whether this does this give rise to questions of being a shadow director?

Anne Templeman-Jones FAICD is the Chair of Blackmores Ltd, director of Commonwealth Bank of Australia, Worley Ltd, Trifork AG and the CSCRC

Principle 5: Plan for a significant cyber security incident

KEY POINTS

1. All organisations are susceptible to a significant cyber incident and directors should proactively plan for an incident
2. Simulation exercises and scenario testing are key tools for the board and senior management to understand and refine respective roles and responsibilities
3. A clear and transparent approach to communications with all 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.

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 shape the narrative, who their external incident responders will be, and which experts will be critical in shaping the 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.

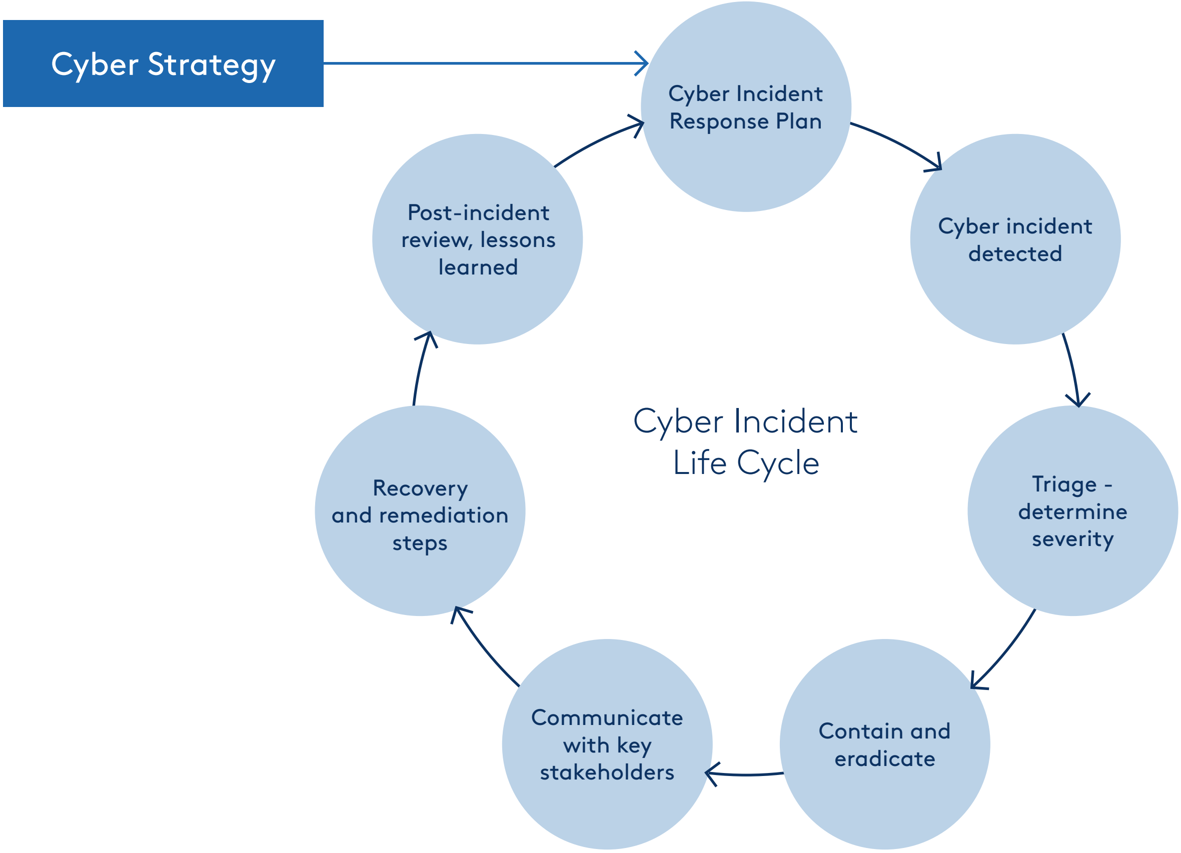
CYBER INCIDENT RESPONSE PLAN

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

Key elements of a Response Plan include:

1. **Responsibilities:** The Response Plan should set out what business functions and key personnel will be responsible for implementing key steps in the plan, including the board. Primary responsibility for enacting the Response Plan is at the operational level, rather than the board, and could include a cross-organisational response team of staff from IT, communications, legal, a representative from the senior executive leadership team, as well as a nominated director. It should also include any third-party external experts who could assist in the event of an incident.
2. **Resources:** What resources those responsible with responding to the incident will draw upon – for example, 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 advisors, legal advisors, cyber insurer support, communications support).
3. **Triage and immediate response:** Steps to identify that a cyber incident is occurring and to assess the severity, including impact on business operations, reputation and key stakeholders (e.g. customer or employee data, suppliers/vendors) and whether any external criminal reporting, insurance notification or regulatory notification/market disclosure obligations may be triggered. Serious consideration should be given to enlisting external support at this time, such as from cyber incident response experts and/or government agencies such as the ACSC.
4. **Containment and eradication:** Strategies for limiting the scope of the cyber incident will differ by the nature of the incident. Steps for containing and eradicating an attack may include taking affected systems offline or isolating unaffected systems to prevent spread of malware.
5. **Communication:** Specific communication channels for staff and impacted customers, including engagement with law enforcement agencies, government, regulators, media, and other affected parties (e.g. those whose data may have been compromised) as well as the broader public. It should be clear who will be responsible for communicating with which stakeholders. Cyber incidents tend to be fast moving and very dynamic. While the incident itself that can be damaging, how an organisation handles the incident can be just as damaging to their ongoing reputation.
6. **Recovery:** 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.


Cyber Strategy
Cyber Incident Response Plan
Cyber incident detected
Triage - determine severity
Contain and eradicate
Communicate with key stakeholders
Recovery and remediation steps
Post-incident review, lessons learned
Cyber Incident Life Cycle

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 with key staff aware of it and 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 key digital assets (or 'crown jewels') of the organisation.

Maintaining hard copies of cyber incident response plan documents – and other documents – 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, its personnel and assets, a range of templates are available, such as the **Victorian Government Incident Response Plan Template**, and the **ACSC Cyber Incident Response Plan Guidance and Template**.

Response

Simulation exercises and testing are key tools in preparing directors, and the broader organisation, to respond effectively to a significant cyber incident.

Many organisations prepare for a cyber incident by having third-party providers test and practice their systems with simulation exercises. This can help assess whether the processes in place under the Response Plan are appropriate, and provide the opportunity to fine-tune approaches. These 'rehearsals; allow directors to become familiar with their oversight responsibilities and/or identify areas for improvement while working through the scenario with management and experts.

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. Can we access external support if necessary to assist with response?

BOX 5.2 SMEs AND NFPs – PLAN AND RESPOND

1. Prepare an incident 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 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.

Organisations can undergo a simulated cyber incident to test the robustness of its Response Plan, with a particular focus on the key steps as 'Triage and immediate response', 'Communication', and 'Recovery'. The board should be closely involved in these exercises, with a focus on understanding the distinct responsibilities of management and the board.

Simulation exercises can take a range of forms. For smaller organisations, it may be appropriate to just discuss or run a step-by-step walk through of the Response Plan. For larger organisations, it may be appropriate to run a full coordinated response exercise where external providers conduct a cyber incident simulation and assess an organisation's response and recovery effort

Exercises could cover:

- Real-time analyses of the simulation incident and the impacts (with the response team not being pre-briefed on the details);
- Dealing with changing scenarios (e.g. an escalation in the severity of the data compromised in a ransomware attack);
- Testing business continuity if key systems go down; and
- Preparing external and internal communications (preferably based off pre-prepared materials such as draft FAQs and media releases with standard messaging pre-prepared which can be used for first release to customers, media and impacted stakeholders).

Once the simulation exercise is complete, it is critical to reflect on the outcomes, how teams responded and update the Response Plan to ensure key learnings are embedded.

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. This can range from not clearly communicating the key facts of the incident, including how the organisation stored and protected key data.

While ultimately 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 regulators, customers and staff. It is vitally important that an organisation communicates as quickly and transparently as possible with key stakeholders (most acutely 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. In some cases, it may be appropriate to acknowledge that the direct cause of the incident and/or impact to business operations and stakeholders may not yet be known, and to update 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 that 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.

ACSC – REPORTCYBER

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

Reporting can be done via the ACSC website's **ReportCyber portal**.

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

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 acutely customers) are advised quickly.

BOX 5.3 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

Directors of ASX listed organisations should also bear in mind their continuous disclosure obligations under the ASX Listing Rules and Corporations Act. Directors will need to 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 – failure to do so may trigger a regulatory response and/or create class action risk. 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.

The Response Plan should be clear on responsibilities for real time managing and approving of communications, including the role of the board, and who will engage with regulators and law enforcement bodies or make statements to the media. Depending on the organisation and the incident, notification requirements may include the OAIC under the Notifiable Data Breaches scheme in the Privacy Act and the ACSC under the SOCI Act.

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.

For directors, a key role in the recovery phase is to assess where improvements may be required to an organisation's risk management controls and cyber strategy. For larger organisations, a post-incident review may assist in identifying lessons learned and ultimately promote a cyber resilience culture. Key questions or issues that would be covered in a post-incident review are highlighted in Box 5.4.

As highlighted in the case study below, an organisation that learns from a cyber incident is in a far stronger position to prevent future incidences.

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?
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. Were the Plan steps, responsibilities and procedures followed? Did the steps mitigate the impact of the incident?
5. Was the board appropriately briefed about the incident and had sufficient oversight and visibility of management actions?
6. What improvements could be made to communication plans?

Remediation

Although an organisation that is a victim of an attack may feel aggrieved that they have had data stolen or leaked, they should not lose sight of who has been most compromised by the breach. The organisation's response must be crafted with those most impacted front of mind.

Where a major cyber incident has occurred and especially where it involves the loss of sensitive personal data, the organisation should decide what support and/or compensation should be offered to those impacted. For some customers, even the thought of having their personal data exposed is enough to cause anxiety, stress and an overwhelming sense of powerlessness. Where the organisation identifies it has vulnerable customers (e.g. victims of domestic violence) that have been impacted it should consider providing additional targeted support.

Where the organisation identifies it has vulnerable customers (e.g. victims of domestic violence) that have been impacted it should consider providing additional targeted support.

At a minimum, support for all customers might take the form of advising them of what recommended steps they should take to mitigate the impact of the lost data (for example identity theft risk) and where they can go to access more expert advice or support (e.g. credit monitoring services or IDCare).

It is better practice though, in a situation where people have been significantly exposed by a cyber breach, for the compromised organisation to offer to pay compensation (financial or in-kind) and/or provide reimbursement for any out-of-pocket expenses incurred in seeking to mitigate their actual or potential loss.

Case Study 5: Major cyber attack on 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, 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 attack highlighted to companies and directors the potential for significant damage that a successful ransomware attack 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".

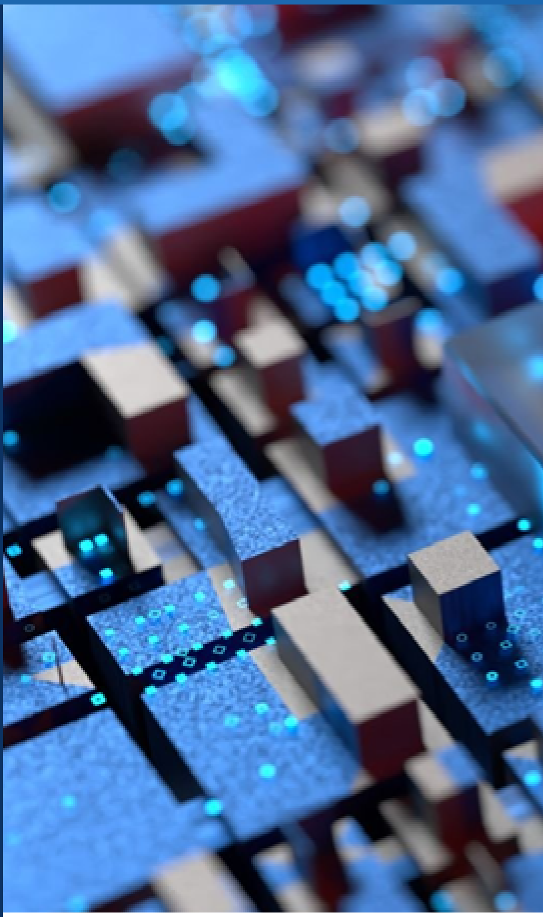
He said for all those reasons, directors should seek independent oversight on a regular basis, comparing cyber assurance to an auditor's review of financials.

"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 incident was 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 AO is the Chair of Telstra, Brambles and the Australian National Maritime Museum

Appendix A: Cyber extortion -Ransomware and data theft



In 2021 the ACSC identified ransomware as the most serious of the cybercrime threats facing Australia due to its high financial and operational cost and other disruptive impacts to victims and the broader Australian community. As highlighted in Case Study 5, such is the impact of ransomware that it can imperil the ongoing solvency of an organisation.

Ransomware and data theft

Data theft involves criminals accessing an organisation's systems and extracting key data.

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.

In recent times, as companies have moved to protect themselves against ransomware attacks, including by ensuring they have adequate back-ups (as one example), the extortion model has changed to include data extortion, with the threat of disclosure or the sale of data on the dark web.

LEGALITY OF RANSOMWARE PAYMENTS IN AUSTRALIA

Australia does not currently have any laws that explicitly prohibit the payment of ransom demands. However, the ACSC has clear advice for organisations not to pay a ransom, as amongst 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).

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

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 threat actor will not retain a copy of the data.

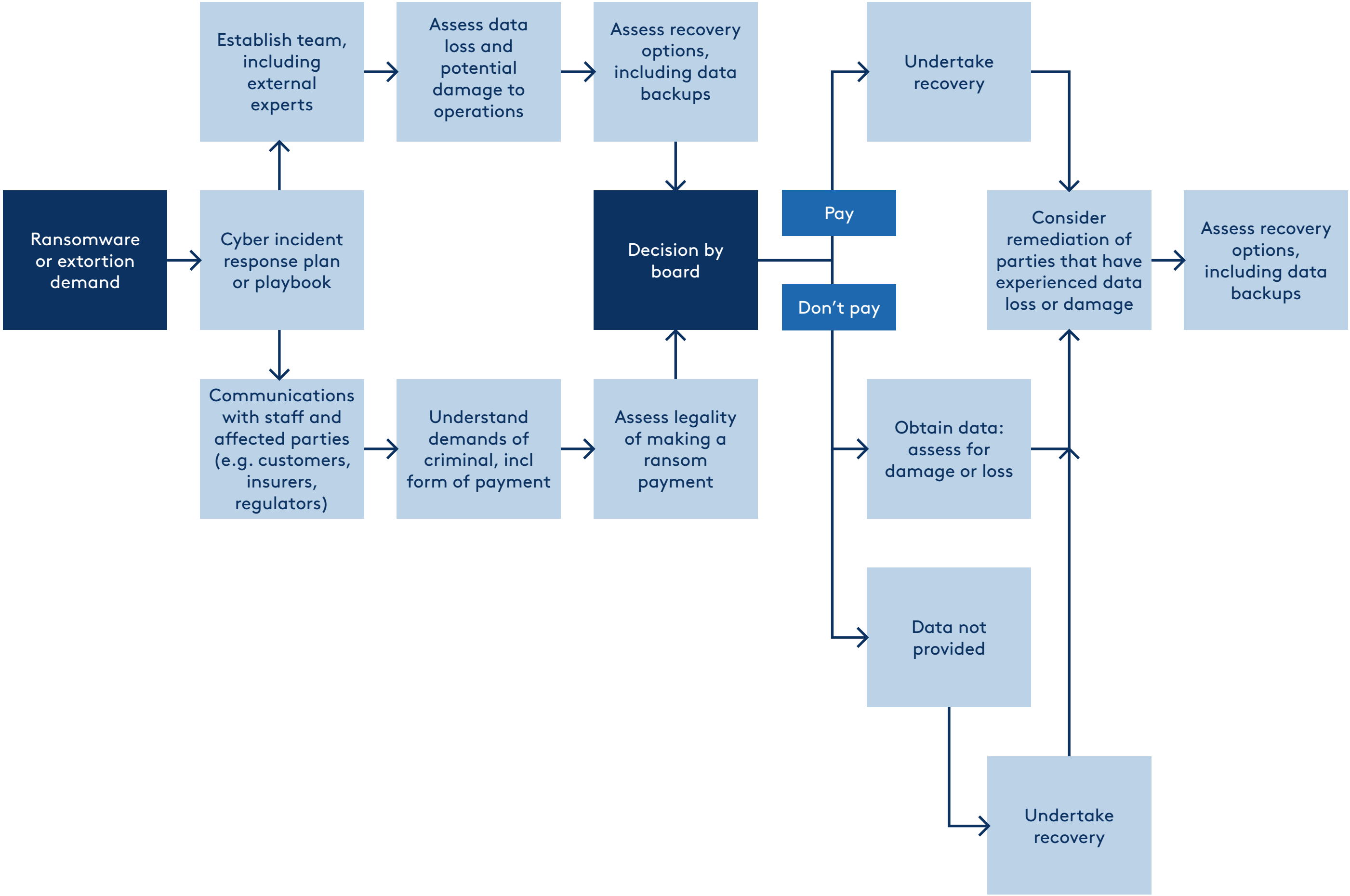
The effectiveness of an organisation's response to an extortion event involving ransomware and/or data theft will depend on how prepared both management and the immediate response team are for such an incident. Developing a cyber incident response plan and the board undertaking simulations (including 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 very messy 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 will often be obligations to notify/regulators and impacted individuals within a specified time frame.

The below decision tree 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


Ransomware or extortion demand
Cyber incident response plan or playbook
Establish team, including external experts
Assess data loss and potential damage to operations
Assess recovery options, including data backups
Communications with staff and affected parties (e.g. customers, insurers, regulators)
Understand demands of criminal, incl form of payment
Assess legality of making a ransom payment
Decision by board
Pay
Don't pay
Undertake recovery
Consider remediation of parties that have experienced data loss or damage
Assess recovery options, including data backups
Obtain data: assess for damage or loss
Data not provided
Undertake recovery

Note: The decision tree presents a linear and binary set of events and decisions of one particular form of 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. ACSC, including:

  i. Cyber security for small and medium businesses

  ii. Cyber security for large organisations and infrastructure

  iii. Strategies to Mitigate Cyber Security Incidents, including the Essential Eight Maturity Model Cyber Incident Response Plan

  iv. ACSC Partnership Program

  v. ReportCyber

  vi. Alerts

b. Cyber and Infrastructure Security Centre

c. ASIC, including:

  i. Cyber resilience good practices

  ii. REP 716 Cyber resilience of firms in Australia's financial markets: 2020–21

  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. Insight article (November 2021): Improving cyber resilience: the role boards have to play

e. OAIC, including

  iv. Australian Privacy Principles guidelines: Chapter 11: APP 11 — Security of personal information

  v. Notifiable Data Breaches

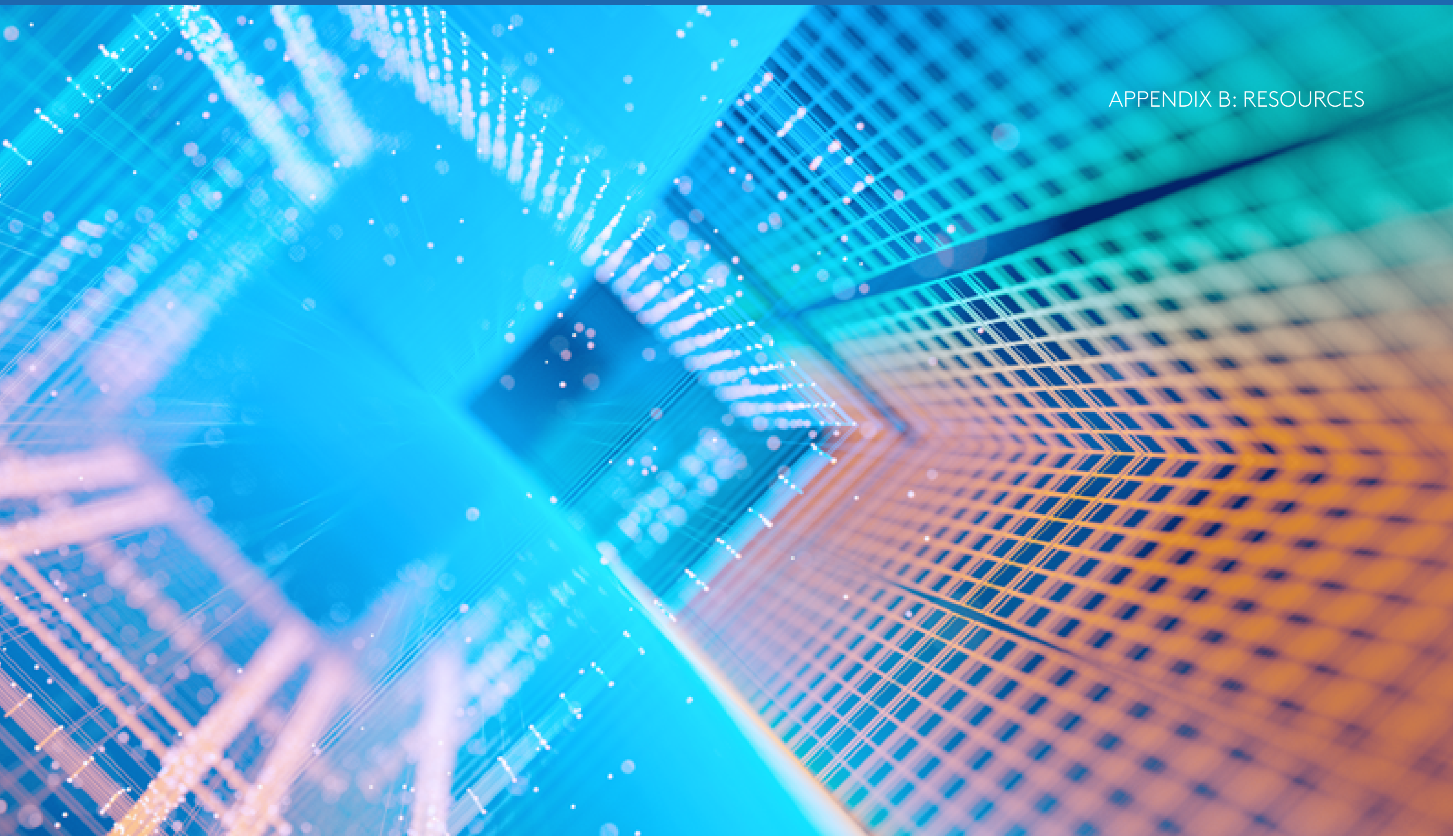
  vi. CDR Privacy Guidelines

  vii. My Health Record

f. IDCARE

g. Australian Energy Sector Cyber Security Framework

h. Council of Small Business Organisations of Australia: 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. Director tools (member only):

  i. **Information technology guidance**

  ii. **Managing a data breach: Ten oversight questions for directors**

  iii. **Data and privacy governance**

a. AICD and Australian Information Security Association research (June 2022): **Boards and Cyber Resilience Study: Insights into director views and current board practices**

4. Research and reports

a. CSCRC:

  i. **Smaller but Stronger: Lifting SME Cyber Security in South Australia (2022)**

  ii. **Case Studies**

  iii. **Underwritten or Oversold? How cyber insurance can hinder (or help) cyber security in Australia**

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)

f. ASX: **ASX 100 Cyber Health Check Report** (2017)

Appendix C: Industry requirements and standards

APRA Prudential Standards: CPS 234 Information Security (CPS 234), CPS 220 Risk Management (CPS 220) and proposed CPS 230 Operational Risk Management (CPS 230)

CPS 234 aims to ensure APRA-regulated entities takes measures to be resilient against information security incidents, including cyberattacks, by maintaining an information security capability commensurate with information security vulnerabilities and threats. CPS 234 states "the board of an APRA-regulated entity is ultimately responsible for ensuring that the entity maintains its information security".

A key objective of CPS 234 is to minimise the likelihood and impact of information security incidents on the confidentiality, integrity or availability of information assets, including information assets managed by related parties or third parties.

Separately, APRA requires comprehensive risk management practices under CPS 220 that are relevant to how an organisation manages cyber risk, including a board approved risk appetite statement that covers material risks. Lastly, APRA has proposed a new prudential standard, CPS 230, which will expand existing outsourcing and business continuity requirements.[2] CPS 230 will require more comprehensive approaches to managing and overseeing material service providers, including those providing key IT and digital infrastructure and services.

[2] CPS 230 was released for consultation in July 2022. At that time it was expected to be finalised in early 2023.

Consumer Data Right (CDR)

The CDR, under the ***Competition and Consumer Act 2010*** (CCA), provides consumers with improved access to, and control over, their data. CDR is being implemented in a phased approach sector-by-sector, beginning with the banking sector, before being extended to other sectors including energy and telecommunications.

Implementation of the CDR is the joint responsibility of the Australian Competition and Consumer Commission (**ACCC**) and the OAIC. The security and integrity of the CDR regime is maintained by 13 privacy safeguards, contained in the ***Competition and Consumer Act 2010*** (Cth) and supplemented by the Consumer Data Rules, which is enforced by the OAIC.

My Health Records Act 2012

The My Health Record system, established by the ***My Health Records Act 2012*** (Cth), is designed to facilitate access by the healthcare recipient and treating healthcare providers, to a summary of health information about a healthcare recipient. The system requires that an organisation take reasonable steps to protect healthcare identifiers from misuse and loss, and unauthorised access, modification or disclosure.

The supporting My Health Records Rules sets out the security requirements that participating organisations must comply with to be eligible to be registered and to remain registered under the My Health Record system. The system also requires a participating organisation to notify the OAIC of any data breaches.

ASIC Market Integrity Rules

ASIC Market Integrity Rules (**the Rules**) apply to networks (e.g. ASX) and participants (e.g. securities trading firms). Under changes that will commence in March 2023 the Rules will seek greater technological and operational resilience through requiring:

- business continuity plans that respond to major events that have the potential to cause significant disruptions to operations or materially impact their services, such as a significant cyber security event;
- the board or senior management must have overall oversight of business continuity plans;
- adequate arrangements to identify, assess, manage and monitor risks to 'ensure the resilience, reliability, integrity and security of [their] Critical Business Services
- adequate arrangements and controls in place to ensure confidentiality, integrity and protection of information. This includes recovery backup systems.

Australian Energy Sector Cyber Security Framework

The Australian Energy Sector Cyber Security Framework (**AESCF**) is an energy sector industry framework that has been developed by Australian Energy Market Operator, industry participants and governance agencies, including ACSC. The AESCF is designed as a tool to assess cyber maturity and promote uplift in capability and cyber resilience. The AESCF leverages existing international standards frameworks, including NIST, ISO 27001 and the US Department of Energy's Electricity Subsector Cybersecurity Capability Maturity Model.

Appendix D: SME and NFP Director Checklist

1. Set clear roles and responsibilities

- Document where possible who has responsiblity 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 overseeing cyber security
- Collect data where possible on the effectiveness of cyber risk practices

2. Develop, implement and evolve a comprehensive cyber strategy

- Utilise the ACSC Cyber Security Assessment Tool to identify the cyber security strengths of the organisation and understand areas for improvement
- Assess whether utilising reputable external providers will enhance cyber resilience over managing in-house
- Assess whether there is certain data (e.g. employee or customer data) that does not need to be collected
- Establish an Access Control System to determine who should have access to what
- Regularly repeat cyber securily training and awareness amongst all employees
- Promote strong email hygiene

3. Embed cyber security in existing risk management practices

- Patch and update applications and anti-virus software
- Configure Microsoft Office macro settings (e.g. only macros from trusted locations enabled)
- 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 offline backups of key data
- Ensure that departing employees or volunteers no longer have access to systems and passwords

4. Promote a culture of cyber resilience

- Mandatory training and phishing testing for all employees and volunteers where appropriate
- Pick a staff member to be a 'cyber security leader' to promote strong cyber practices and respond to questions from other staff
- Subscribe to ACSC alerts to stay across emerging cyber threats

5. Plan for a significant cyber security incident

- Prepare an incident response plan utilsing 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 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

SME AND NFP RESOURCES

1. ACSC: **Cyber security for small and medium businesses**
2. ACSC 24/7 Hotline on 1300 CYBER1 (1300 292 371)
3. Council of Small Business Organisations of Australia: **Cyber Security Resources**
4. CSCRC: Smaller but Stronger: **Lifting SME Cyber Security in South Australia**

Appendix E: Glossary

ACSC has an extensive online glossary of cyber security relevant terms available **here**.

ACSC	Australian Cyber Security Centre
AFSL	Australian Financial Services License
APRA	Australian Prudential Regulation Authority
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 businesses or individuals
Essential Eight	The eight essential mitigation strategies that the ACSC recommends organisations implement as a baseline to make it much harder for adversaries to compromise their systems
IDCARE	Australia and New Zealand non-government identity & cyber support service
ISO 27001	International Standard Organisation 27001 Information Security Management
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
Multi-factor authentication	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 renders data or systems unusable until the victim makes a payment
SME	Small-medium enterprise
SOCI Act	Security of Critical Infrastructure Act 2018
White box exercise	A form of penetration testing carried out by an ethical hacker who has full access to the system they are carrying the simulated attack on.

Acknowledgements

The AICD and CSCRC would like to thank the following directors who gave generously of their time and provided insights into best practice in the governance of cyber security, including the case studies included in these Principles:

- Kathleen Bailey-Lord FAICD, Director of QBE Insurance, Alinta Energy, Melbourne Water and Datacom
- Catherine Brenner FAICD, Chair of Australian Payments Plus, Director of Scentre Group, Emmi and The George Institute for Global Health
- Melinda Conrad FAICD, Director of ASX Limited, Ampol Australia, Stockland, Penten and The Centre for Independent Studies
- Naomi Edwards FAICD, Chair of Spirit Super, Director of Tasmanian Development Board, AICD and Propel Funeral Partners
- John M. Green FAICD, Chair of UOW Global Enterprises, Director of Challenger and the CSCRC
- John Mullen AO, Chair of Telstra, Chair of Brambles and Chair of the Australian National Maritime Museum
- Anne Templeman-Jones FAICD, Chair of Blackmores, Director of Commonwealth Bank of Australia, Worley, Trifork AG and the CSCRC

About the AICD

The AICD 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 the not-for-profit sectors.

About the CSCRC

The CSCRC is dedicated to fostering the next generation of Australian cyber security talent, developing innovative projects to strengthen our nation’s cyber security capabilities. We build effective collaborations between industry, government and researchers, creating real-world solutions for pressing cyber-related problems.

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 excludes 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

CCT328_23

JOIN OUR SOCIAL COMMUNITY

aicd.com.au