Australian Institute of Company Directors

CYBER SECURITY COOPERATIVE RESEARCH CENTRE

Ashurst

Governing Through a Cyber Crisis

CYBER INCIDENT RESPONSE AND RECOVERY FOR AUSTRALIAN DIRECTORS

March 2024

Table of Contents

Minister's foreword

Cyber security is not just good practice; it's good business. A clear understanding of how to manage cyber risks is essential for Australian businesses embracing the digital economy. As cyber threats grow at an unprecedented pace, government and business leaders need to do more to defend Australia from cyber attacks.

In 2023, the Australian Government released the ***2023-2030 Cyber Security Strategy***. Under the strategy, we outlined six 'cyber shields' to protect Australian citizens and businesses. Our strategy is about government and industry stepping up to the plate on cyber security.

Business leaders, boards and directors have important obligations to protect their organisations and customers from cyber risks. Australians rightly expect businesses to take cyber security seriously.

The explosion of cyber incidents over the past two years has shown that we cannot be complacent on cyber. All Australian organisations need to embrace better cyber governance from the board down. Government, business, not-for-profits and community leaders need to work together to make Australia a hard target and ensure we can bounce back quickly.

In consultation on the strategy, we heard that for many people the expectations of cyber governance are unclear. As I spoke with business leaders across the country, I saw that more could be done to help businesses understand what good cyber security looks like.

That's why clarifying cyber obligations is a centrepiece of our strategy. Action 5 of the strategy is to provide clear guidance to industry, including clarifying expectations of corporate cyber governance.

I am therefore delighted to see the Australian Institute of Company Directors, the Cyber Security Cooperative Research Centre and Ashurst partnering to publish ***Governing Through a Cyber Crisis: Cyber Incident Response and Recovery for Australian Directors***. This new guidance builds on the ***AICD CSCRC Cyber Security Governance Principles*** released in 2022, which provided a clear and practical framework for organisations to build stronger cyber resilience.

This guidebook directly supports Action 5 of the strategy by providing detailed guidance to corporate leaders on cyber preparation, response and recovery. I commend this guidance to Australian organisations of all sizes and encourage leaders to embed these principles into how they do business.

Business leaders continually identify ransomware as one of the most destructive cyber threats to Australian organisations. The Government's advice on ransom payments is clear – never pay a ransom. There is no guarantee you will regain access to your information, nor prevent it from being sold or leaked online. You may also be targeted by another attack.

The Government is committed to working closely with industry to build our national cyber shields. Together, we can achieve our goal of making Australia a world leading cyber secure nation by 2030.

Hon Clare O'Neil MP

Minister for Home Affairs and Minister for Cyber Security

AICD & CSCRC foreword

Over the last two years, the profound consequences of serious cyber incidents have impacted every part of the Australian community. Systems have been compromised, deeply personal data has been stolen, commercially sensitive information has been exposed and, more than ever before, cyber security is an area of concern for all Australians. There is a justifiable community expectation that organisations will have strong cyber defences, and that they will respond to serious cyber incidents urgently, effectively, and with as much transparency as possible.

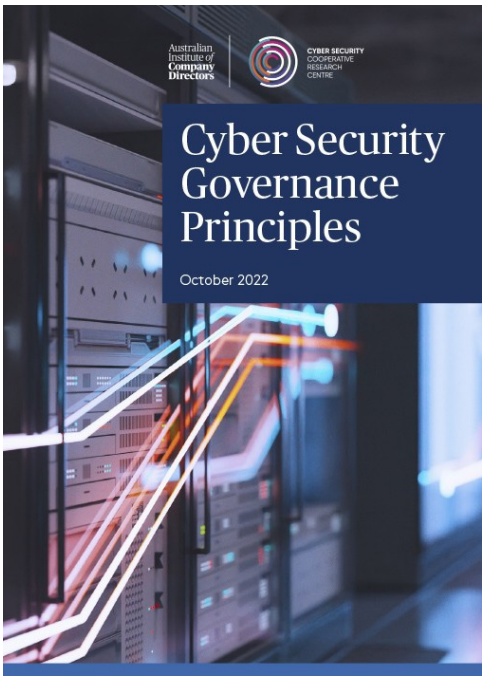
Unsurprisingly, this growing awareness of cyber risks has had a significant impact on the way Australian boards oversee cyber risk-management within their organisations. On television news bulletins, across newspaper headlines and in mainstream public discourse, we have learnt how incredibly destructive a significant cyber incident can be to customers, employees, the business operations of an organisation, its financial position and its reputation, as well as the legal and regulatory risks it faces. Cyber security is a top priority for the community and therefore must be a top priority for boards.

In October 2022, we released the **AICD CSCRC Cyber Security Governance Principles**[1] (the Principles), the first better practice guide for Australian directors when considering cyber security risks. But we quickly realised more was needed – guidance to help boards and directors better prepare for, respond to and recover from a significant cyber incident. This guidance builds on the foundations laid by the Principles and represents the commitment of the AICD and CSCRC, supported by Ashurst, to equip directors from all organisations – big and small – with practical steps to help navigate through a cyber crisis.

Like any other serious business risk, managing cyber risks involves much preparation. This guidance outlines how boards can comprehensively prepare for a cyber crisis through oversight of practices, processes and controls, data governance, testing and simulation. It also provides pragmatic advice to boards about the realities of a cyber incident – the uncertainties and extreme pressure – that they will face, and how to govern through complexity and flux. Importantly, it highlights the centrality of effective communications in a cyber crisis and the vital role it plays in retaining and rebuilding reputation.

We would like to thank all those who contributed to this guidance for their time and thoughtful insights. As a living document, this guidance will continue to be updated to reflect regulatory and legislative change, as well as any significant events that may impact upon cyber crisis preparation, response and recovery. We hope you will find it useful.

Mark Rigotti, MD & CEO AICD &
Rachael Falk, CEO CSCRC



1 https://www.aicd.com.au/content/dam/aicd/pdf/tools-resources/director-tools/board/cyber-security-governance-principles-web3.pdf

Executive summary

Role of the board during a cyber crisis

Boards need to be confident that their organisation is ready for cyber incidents. Thorough and comprehensive planning for significant cyber incidents is key.

Boards should be prepared to become actively involved in a cyber crisis, have oversight of, and support, management's key decisions and responses.

From the outset, boards need to contemplate the long tail of potential post-incident risks, including regulatory, operational and reputational.

Readiness

KEY POINTS

Effective cyber crisis response starts with a current and comprehensive cyber incident response plan that is regularly tested and updated.

Clearly defined roles and responsibilities, including the role of the board and any board committees, are key to effective decision-making during a cyber crisis.

A thorough communications strategy is central to how an organisation manages external and internal stakeholders during a cyber crisis.

A rigorous cyber incident response training and testing program that simulates crisis conditions is a key preparedness tool for the board and management.

KEY QUESTIONS

1. Are roles and responsibilities comprehensively documented, including the role of the Chair and specific directors in the event of a significant incident?
2. Are the processes for key decision-making and external support detailed in the response plan?
3. Do we have a comprehensive approach and plan to communicating with internal and external stakeholders, including responsibilities for notifying and engaging with regulators and approving market disclosures?
4. Do we understand how insurance would operate in the event of an incident and the support the insurer can/cannot provide?
5. Do we regularly scenario test or conduct a simulation on our response plan? How often do we review the response plan and update it to ensure it reflects organisational changes and the current threat environment?

RED FLAGS

1. The board and senior management have not undertaken regular scenario testing or incident simulations to test the cyber incident response plan.
2. The organisation indicated there are no gaps in current cyber readiness.
3. Likely scenarios and consequences are undocumented with lessons from simulations not being captured or actioned.
4. It is not clear how communications with key stakeholders, including customers, will be managed in the event of a critical incident.
5. It is not clear who the organisation will engage to provide support during a critical cyber incident.

Response

KEY POINTS

The dynamic and fluid nature of a cyber crisis means the board should provide agile and timely support and oversight of management decision-making.

For larger organisations, consider establishing a Cyber Incident Sub-Committee of the board that can provide effective and agile governance during the response phase of a cyber crisis.

Consistent, timely, accurate and transparent communications with key stakeholders, such as customers and employees, is critical and plays an important role in mitigating reputational damage.

Expert external advice plays a critical role in supporting boards to effectively oversee decision-making during the response phase.

Have oversight of regulators reporting obligations, and ongoing liaison with regulatory, the ACSC and the National Cyber Coordinator.

For larger organisations, consider establishing a remediation and post-incident review team in parallel to the response team.

KEY QUESTIONS

1. Do we need to establish a sub-committee of the board to oversee management's actions during the response phase and speed-up decision-making?
2. Do we understand our legal and contractual obligations to make notifications (to whom, when and of what)? Do we have a set of priorities for the most-urgent to least-urgent notifications?
3. Who has primary responsibility for making those notifications? Has legal advice been sought on those notifications and their content?
4. Are we satisfied that the resources available to the management team to respond to the incident are appropriate given the scale and complexity of the organisation and the nature of the incident?
5. What key third-party providers are we relying on to provide support during the response phase? What is the nature of this support?

RED FLAGS

1. A significant delay in discovering the incident and understanding the impact on systems, data and key stakeholders, including employees and customers.
2. Confusing or contradictory information reported to the board and/or communicated to employees, customers and key regulators and government agencies.
3. Key elements of the cyber incident response plan not being followed; for instance, a lack of information sharing between teams, or a lack of focus on customers.
4. Failing to utilise the expertise of external advisers and cyber security professionals, including in relation to approaches to crisis management and communications, regulatory notifications and forensics.

Recovery

KEY POINTS

Oversee steps to secure systems and data are appropriate, including the implementation of any immediate or short-term investment in cyber security.

Understand the impact of the cyber crisis on employee well-being and take steps to support employees impacted by the cyber crisis.

The board should oversee a comprehensive post-incident review, which includes utilising external advice, where appropriate.

KEY QUESTIONS

1. Are there immediate security measures that can be implemented?
2. Has the board sought independent advice on the actions taken and the current level of security?
3. Does the board understand the potential risk of harm that impacted individuals face because of data loss? What steps have been taken to adequately mitigate this risk, and what additional steps can be taken?
4. Is the cost, pace and scale of recovery commensurate with the expectations of your customers, government, regulators, and other key stakeholders?
5. Does the board have oversight of ongoing regulators' investigations and requests for information?

RED FLAGS

1. A limited investigation that focuses on fixing immediate issues without identifying the underlying root causes and vulnerabilities.
2. Limited transparency to key stakeholders on the nature of the incident and how it is being remediated.
3. Accountability not apportioned fairly – failures being blamed on one or two individuals.
4. Not documenting and disseminating the lessons learned from the incident across the organisation, including how to approach crisis management.
5. No plan for supporting staff and recognising their contribution.

Remediation

KEY POINTS

Require remediation plans that are customer focused, well resourced and swiftly implemented.

Oversee continuing effective communication and support for employees, customers and third parties who may have been impacted or potentially harmed by the incident.

Oversee remediation, compensation and complaints-handling processes to customers where appropriate.

Responsibly share knowledge and insights gained from the crisis with other organisations.

KEY QUESTIONS

1. Does the board have oversight of likely potential claims which may arise out of the particular incident? Has a strategy been developed to handle each type of claim?
2. Are there sufficient resources and funds available to remediate at the appropriate scale and pace?
3. Has the board reviewed and approved updates to the cyber risk framework, risk appetite statements and incident response plans? Is there a continuation of the simulation and testing program scheduled?
4. Does the board have appropriate oversight over the key customer and employee issues that may require remediation?
5. How would our planned approach to remediation be viewed externally?
6. Has the board agreed, with appropriate legal advice, what lessons can be openly shared with key stakeholders?

RED FLAGS

1. Limited or no genuine attempt to recognise the impact on individual customers and provide them with appropriate support.
2. Management downplaying the severity of the incident or resisting further focus on improving cyber security.
3. No clear strategy or plan for rebuilding the organisation's reputation.
4. Limited information from management about the legal risks and external investigations resulting from the incident.

Recommendations for SME and NFP directors

The ACSC has extensive resources to support smaller organisations available here[1].

Readiness

- Document core elements of a response plan, including:
  - Who will be responsible in leading the response to a cyber crisis?
  - What are the key systems essential to the operations of the SME and NFP?
  - Do we hold highly sensitive or critical data, for example an NFP holding the personal information of clients/beneficiaries?
  - Where are our backups located and are they secure?
  - What will be our approach to communications, including responsibilities for communications and regulatory reporting?
  - What external sources of assistance and expertise can we call on?

Response

- Seek assistance from trusted sources.
- Report the incident to the ACSC.
- Inform key stakeholders including employees, customers, and partners in a transparent, accurate and timely manner.
- Restore systems, critical operations and data from backups where possible. Prioritise recovering essential functions.
- Reset all passwords for affected accounts, including employee, customer, service and administrator accounts.
- Implement strong password policies with multi-factor authentication.

Recovery

- Where possible invest in cyber security enhancements, such as storing key data and systems with reputable cloud providers or migrating key functions to SaaS providers.
- Support impacted employees and volunteers.
- Train employees and volunteers on cyber security awareness and practical controls, including cyber hygiene and awareness of scams.

Remediation

- Where possible provide assistance to impacted individuals, including financial support to replace documents.
- Utilise templates, social media, FAQs on a website, or a dedicated customer telephone line to assist in triaging and responding to customer issues and complaints.
- Continue to communicate honestly, clearly and empathetically with impacted stakeholders.
- Demonstrate cyber enhancements to key stakeholders.
- Consider the range of appropriate remediation options that might be available to those impacted.

1. https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/publications/cyber-incident-response-plan

Introduction

WHAT IS A CYBER CRISIS?

Boards have a key governance role to play in being aware of the cyber threat landscape, prioritising cyber resilience at their organisations and developing capabilities for the oversight of cyber risk and effective responses to cyber crises.

A cyber crisis for an organisation occurs when an IT system fails, becomes unavailable or is breached, resulting in serious interruption to an organisation's operations and functions – that often leads to the access, theft or release of information or data and even the inability to operate the business or the organisation's assets and people being placed at risk. In a cyber crisis, normal business processes are insufficient or unavailable and crisis management mechanisms need to be immediately deployed.

An organisational cyber crisis can result from many factors including, but not limited to, a cyber-attack, theft of data, system failure, human error and/or insider threat.

In a world underpinned by digital systems, cyber crises at an organisational level are becoming more prevalent and attract significant attention from regulators, shareholders, customers and the public.

It is essential directors of all organisations – large and small – take very seriously the significant the significant operational and reputational risks from a critical cyber incident.

PROMINENT 2023 ORGANISATIONAL CYBER CRISES

- Latitude Financial: cyber attack (ransomware) and data breach of personal customer data;
- HWL Ebsworth: cyber attack (ransomware) and theft of personal data and client information;
- MOVEit data breach: Exposed large volumes of data from more than 200 organisations including governments, large and small companies that used the file transfer service;
- Dymocks: Customer personal data breach through a third-party provider;
- DP World: Cyber-attack impacting operations at national ports;
- Clinical Australian Labs: Data breach, including sensitive health data;
- St Vincent's Health: Cyber attack with data theft.

DYNAMIC CYBER THREAT LANDSCAPE

As a result of developing technologies, globally interconnected industries and an unstable geopolitical climate, the cyber-threat landscape is constantly evolving and becoming more complex. In particular, threat actors continue to develop more-innovative ways to access and exfiltrate critical and sensitive data, as well as disrupt-and-disable business operations.

The Australian Government's 2023-2030 Australian Cyber Security Strategy[2] states that:

> "cyber attacks are accelerating faster than ever before... Malicious activity targeting Australians through cyberspace continues to grow at an unprecedented rate, with cyber criminals and state-sponsored actors routinely targeting our networks and data... As malicious actors grow in number, they are also taking advantage of more advanced tools."

The cyber threat landscape comprises a diverse range of threat actors and attack types. Cyber threats may include ransomware, supply chain vulnerabilities, human error, insider threats, business email compromises, phishing, malware or denial of service attacks. These threats present significant risks to many key organisational assets, including confidential and personal information, business operating systems, trade secrets, intellectual property and financial accounts.

Given this dynamic environment, it is vital for directors to understand the evolving nature of the cyber threat landscape and how it relates to their organisation. Failing to do so could result in:

- loss of operations and business;
- financial loss;
- risk of harm (financial and non-financial) to individuals whose personal data or sensitive information has been exposed;
- loss of trust and reputational harm; and
- legal exposure (both for organisations and, in some circumstances, directors in their personal capacity).

This guidance is a 'living document' which will be periodically reviewed to reflect the evolving threat and regulatory landscape. This guidance does not constitute legal advice and is produced as guidance only.

The AICD, CSCRC and Ashurst recommend organisations seek independent advice regarding legal, regulatory and technical cyber security matters.

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

2. https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf

CYBER REGULATORY ENVIRONMENT

Australia's cyber regulatory environment has evolved significantly over the past several years, clearly signalling the expectation of government and regulators that organisations take active steps to mitigate against cyber risks.

The Cyber and Infrastructure Security Centre (**CISC**), part of the Department of Home Affairs, has published a key reference document, ***Overview of Cyber Security Obligations for Corporate Leaders*** (available here[3]).

The CISC resource breaks the obligations down into preparedness, reporting and responding requirements. Crucially, it provides a snapshot of key regulatory frameworks, including the *Privacy Act 1988* (**Privacy Act**), *Security of Critical Infrastructure Act 2018* (**SOCI Act**) and APRA prudential requirements. This publication is a key starting point for directors in understanding the cyber security related regulatory obligations their organisations may face. Appendix A provides a list of key Commonwealth regulatory obligations relevant to the governance of cyber security risk.

In addition to broad regulatory frameworks, such as the Privacy Act, directors should also be alive to specific obligations that vary by industry, sector or state jurisdiction. For example, the telecommunications, defence and energy sectors have specific risk-management obligations that should be accounted for in considering cyber security resilience and risk controls. Further, there are state-based reporting requirements for state-owned bodies and often organisations providing certain products and services to the state government.

Organisations with operations and assets overseas will also need to be cognisant of cyber and reporting obligations in each relevant jurisdiction.

CYBER SECURITY OBLIGATIONS UNDER CONTRACT

In addition to any obligations under applicable cyber-related legislation or regulation, organisations need to be mindful of any obligations they have agreed under contract and their service level agreements (SLAs). Where organisations breach these obligations, and SLAs there could be recourse under the contract. Notably, privacy and confidentiality obligations are commonly the subject of indemnities in commercial contracts that may not be limited by a liability cap.

3. https://www.cisc.gov.au/resources-subsite/Documents/overview-cyber-security-obligations-corporate-leaders.pdf

Reform on the horizon

The Federal Government's ***2023-2030 Australian Cyber Security Strategy*** (**the strategy** – published in November 2023) sets out an ambitious reform agenda. It is important for all boards to monitor these changes as they will have implications for all organisations' cyber security settings.

Proposed reforms are to be co-designed with industry and include:

- a reporting framework for ransom demands and/or payments in the event of a ransomware incident;
- a "limited use" obligation in relation to how the Australian Signals Directorate (**ASD**) and National Cyber Coordinator can use information voluntarily provided by a business during a critical cyber incident;
- a Cyber Incident Review Board to conduct "no-fault" incident reviews;
- Amendments to the SOCI Act in relation to:
  - Data storage systems and defining business critical data
  - Government powers to manage the consequence of cyber attacks
  - Simplified information-sharing framework for government and industry
  - Review and remedy powers for critical infrastructure risk-management plans
  - Folding in existing telecommunications sector risk-management requirements.

The strategy also outlines how the government is exploring options to incorporate stronger cyber security obligations into 'all hazards' obligations for aviation, maritime and offshore facility regulated entities.

KEY TAKEAWAYS FOR THE BOARD TO PREPARE FOR REGULATORY REFORM ARE:

Prepare now – don't wait for legislation to commence to understand and develop additional compliance measures.

Check your privacy governance – organisations will be expected to have adequate systems and procedures in place once any reforms are enacted.

Adopt an 'all hazards' risk approach – identify hazards that may impact critical infrastructure assets, implementing measures to minimise and prevent incidents.

PROPOSED REFORM OF THE PRIVACY ACT

Separate to the strategy, ambitious reform of the Privacy Act is also in train. In October 2023, the government committed to pursuing almost all of the 116 proposals of the extensive Privacy Act Review.

If legislated in full or in part, these reforms would represent a major shift in how organisations collect, manage and dispose of personal information in Australia. They would also bring Australia closer in alignment with the European Union's General Data Protection Regulation (**GDPR**), creating a more prescriptive and demanding privacy regime in Australia.

Key proposals that will be subject to further consultation include:

- Removal of the small business exemption (currently $3 million p.a. for most businesses);
- Targeted amendments to Australian Privacy Principles 11 – Protection of personal information; and
- A new 'fair and reasonable' test for the use of personal information.

1. Overview: role of the board in a cyber crisis

KEY POINTS

1. Boards need to be confident their organisation is cyber ready. The benchmark is thorough and comprehensive planning for significant cyber incidents and business continuity.
2. Boards should be prepared to become actively involved in a cyber crisis.
3. Boards need to contemplate, from the outset, the long tail of potential post-incident risks, including regulatory, operational and reputational.

The board has a key role in overseeing the decisions of an organisation's management team during a cyber crisis. This role is consistent with a director's broader responsibility to oversee the management of cyber and information security risk and ensure business continuity.

> "Never assume you are immune."
>
> — Senior Chair of ASX-listed company

WHAT MAKES A CYBER CRISIS CHALLENGING FOR THE BOARD?

Many organisations successfully respond to minor cyber incidents, including cyber attacks, every day without involving the board beyond the normal course of proper governance reporting. However, there are key features of a significant cyber incident or crisis that demand a more direct board role. These challenges are detailed in the accompanying **Figure 1**.

BOARDS NEED TO BE CONFIDENT THEIR ORGANISATION IS PREPARED

The expectation of regulators, customers, employees and the general community is that all organisations will have a range of cyber security response plans and resources in place, appropriate to their scale, complexity and level of risk.

The board's role is to oversee thorough and comprehensive planning for significant cyber security incidents. Response plans should be rigorously tested at all levels – from operations and management through to leadership and the board.

In the wake of high-profile cyber incidents in Australia, there has been increased regulatory scrutiny in relation to the effectiveness of cyber risk-management and its oversight. Australian Security and investment Commission (**ASIC**) Chair, Joe Longo, has stated that "organisations must take an active approach to evaluating and managing third-party cyber risk", and that "failure to ensure adequate measures are in place exposes directors to potential enforcement action by ASIC based on the directors not acting with reasonable care and diligence".

Similarly, John Lonsdale, Chair of the Australian Prudential Regulation Authority (**APRA**), has stated that "many entities are still struggling with foundational issues: ensuring third-party controls are effective, making sure that systematic security control testing is in place, and regularly testing incident response plans".

FIGURE 1: KEY CHALLENGES

Significant pressure on business continuity, disaster recovery and cyber response planning

Many organisations are underprepared for the scale of a significant cyber incident where multiple (or all) systems are impacted, business operations are severely disrupted and recovery and rebuild can take weeks or months.

Operating in a vacuum of information for a sustained period of time

Critical decisions that will impact customers, employees and reputation need to be made in an absence of certainty with baseline information changing rapidly.

Stakeholder demands

The scale of stakeholder management can be overwhelming. State and federal government agencies, customers, shareholders, suppliers, the media and employees, will all want to know what has caused the incident, the impact and whether the business is secure.

For listed companies, meeting market disclosure requirements, particularly in an information vacuum, can be challenging.

Employee welfare and fatigue

Fatigue suffered by those responding to a cyber incident has a measurable impact one performance and recovery.

Managing "downstream" risk

Some decisions organisations make in the early days of a significant cyber incident will have long-term implications and impact the risk of ongoing legal action and reputational damage.

BOARDS NEED TO TAKE A MORE-ACTIVE ROLE

Management should anticipate the need to notify and update the board in the early stages of a significant cyber incident. The board should look to convene an out-of-session board meeting, or a sub-committee meeting, on short notice. In providing governance and support for the executive team, boards will need to determine what evidence they require to satisfy themselves that regulatory, contractual and insurer notifications have been appropriately made. They also need to have confidence the organisation has access to appropriate expertise and resources to contain the incident, recover systems and data and manage impacts on employees, customers, third parties and their reputation.

CHALLENGES FOR SME AND NFP ORGANISATIONS

SME and NFP organisations face unique challenges in significant cyber incidents. These include:

- Limited financial and human resources to deploy to cyber crisis response and recovery;
- A reliance on third-party IT providers and software developers for key business functions and support, which may not have the proper expertise or resources to respond effectively;
- Cash flow and immediate financial impacts triggered by the sudden, and sustained, operational outage;
- Expertise, time and resourcing difficulties in managing and responding to high-volume customer and stakeholder communication requirements.

Examples of where directors may need to become more actively involved in cyber crisis response include:

- Support and oversight of management's key decision-making and responses;
- Consider a board sub-committee for cyber crises (refer to Governance Structures in section 3 for more detail);
- Oversight of engagement with key stakeholders, including government, key shareholders, customers and critical third parties (particularly, but not exclusively, for SME organisations);
- Support the management team's communications and media strategy;
- Approve out of cycle/extraordinary budget items;
- Make a decision, with appropriate advice, regarding a ransom demand;
- Ensure the organisation is taking actions to limit the risk of harm to any impacted individuals;
- Assessing and supporting the executive to identify and manage "downstream" risks to the organisation, including litigation, investigation and reputational risks; and
- Helping organisations navigate business continuity issues.[1]

Directors may also require direct access to specialist advisors in a cyber crisis.

1 The AICD guidance on business continuity can be found here: https://www.aicd.com.au/good-governance/organisational-strategy/long-term-strategic-plan/business-continuity-9-key-areas-of-focus-for-your-board.html

ONGOING BOARD OVERSIGHT OF THE 'LONG TAIL' OF POST-INCIDENT RISK

The consequences of cyber crises can be varied and long term. They will result in:

- the need for ongoing engagement with regulators and responding to regulatory investigations;
- litigation and class actions;
- supporting customers and employees who have been impacted by a data breach or an operational outage;
- ensuring systems are secure from secondary attacks; and,
- implementing an appropriate security uplift program, based on an appropriate root-cause analysis.

Boards will need to review their cyber risk appetite and determine the appropriate speed, allocated resources and investment in cyber security, following an incident. Boards also often take an active role in ensuring there is a strategy in place to manage reputational risk or potential loss of both revenue and market share and, for listed companies, recover from any impacts the incident may have had on share price.

2. Readiness

> As a board you need to step back ... you need to start thinking about the issue at a broader level"
>
> — Senior Chair of ASX-listed company

KEY POINTS

1. Effective cyber crisis response starts with a current and comprehensive cyber incident response plan that is regularly tested and updated.
2. Clearly defined roles and responsibilities, including the role of the board and any board committees, are key to effective decision-making during a cyber crisis.
3. A thorough communications strategy – tested and refined during cyber scenario planning and with clear spokesperson authorisation, and a focus on customers – is central to how an organisation manages external and internal stakeholders during a cyber crisis.
4. A rigorous training and testing program for cyber incident responses, which simulates crisis conditions, is a key tool in helping boards and management prepare to effectively respond to them.
5. Organisations should also recognise the national security overlay of the cyber threat environment. In particular, they may become a target for a state-sponsored actor wishing to harm Australia's interests through disrupting a key part of the economy or financial system.

STRONG CYBER RISK GOVERNANCE FOUNDATIONS

It is the board's responsibility to oversee the management of cyber risk; boards need to be prepared to scrutinise, analyse, support and advise management in response to an incident. They should have appropriate oversight over the organisation and enough insight into its preparedness to assist management to quickly and effectively respond

The board should promote a risk-based approach, rather than a narrow compliance-based approach, to cyber resilience. Cyber risk-management should be integrated into an organisation's objectives and risk-management framework, dealt with as a wider organisational risk, not just an IT risk. An organisation's cyber risk policies and processes must sit seamlessly with the business continuity and crisis policies and processes.

To build strong cyber governance foundations, there must be a clear understanding at all levels that cyber security is the responsibility of all employees. The board has a key role in a setting a tone from the top in promoting a strong cyber culture, leading by example and investing time and energy into making cyber a top priority. This includes the board participating in scenario testing and simulations.

FOUNDATIONS OF CYBER RISK GOVERNANCE

- Clear roles and responsibilities
- Understanding key digital and physical assets
- Effective cyber risk-management and controls
- Data governance framework
- Tested incident response plan

Know your digital and physical assets

Identifying the digital assets and data held by an organisation, including being able to identify and map critical systems and data, is an essential step in cyber readiness. During a significant cyber incident, knowledge of digital and physical assets is vital, supporting containment and enabling decisions to be made more quickly.

Certain legislation also places obligations on particular organisations around documentation and maintaining the inventories of specific assets. For instance, the SOCI Act requires captured entities to have oversight of critical digital and physical assets.

Boards cannot have assurance their digital perimeter is secure unless there is an appropriate and full account of all digital assets. This includes assets that may be obsolete or no longer supported.

Therefore, it is vital that an inventory of digital assets, which vendor supports them, their level of criticality and their interdependencies be mapped. This assists the board and management to develop a clear risk-based approach to managing cyber threats. This is not a straightforward exercise and may require a specific program to be undertaken. Unfortunately, many companies are unsure of the digital and data assets that they hold, and where they hold them.

Data governance framework

Data underpins the operations of almost every organisation and is often the 'crown jewels' or most-valuable asset. However, as recent data breaches have clearly illustrated, data is also valuable to cyber criminals. Therefore, a documented data-governance framework applying across the organisation to manage the security, storage and disposal of data is essential.

The most-effective way to approach this complex exercise is to undertake a comprehensive review of organisational data. Key to this is standardisation of data definitions, establishment of data registers and inventories, and identification of key data assets and their owners. Any personal or sensitive information should be included in the governance framework, with data asset owners assigned for all personal data and highly sensitive data.

The core elements of a data governance framework are outlined in the accompanying Figure 2.

Boards and management need an appropriate understanding of the potential risk of holding certain personal data, even if it seems low risk. For example, a compromise of just names and addresses of vulnerable individuals can be high risk.

Accordingly, key data and digital assets should be clearly mapped in cyber incident response plans, including identifying individuals with access to these assets. This will assist the board to quickly assess whether sensitive data has been impacted and will facilitate a more rapid response.

FIGURE 2: CORE ELEMENTS OF A DATA GOVERNANCE FRAMEWORK

Clear Policies and procedures

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

Accountability

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

Data classification

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

Internal controls and security

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

Data quality

Data should be reviewed and updated regularly, including periodic destruction and data cleansing, to ensure it remains relevant and retainable in light of changing laws, regulations and business needs.

Regular review and updating

Data should be reviewed and updated regularly to ensure it remains relevant and retainable in light of changing laws, regulations and business needs.

Cyber risk-management and controls

Cyber resilience requires an organisation to have strong risk-management frameworks and embedded practices that implement effective governance arrangements, control frameworks and effective testing and review regimes. These are detailed further in the AICD CSCRC Cyber Security Governance Principles (available here[4]).

There is an onus on boards to oversee adequate investment in an organisation's cyber risk controls, supported by internal and external assurance and effective board reporting. A valuable resource to assist directors is ASD's Questions to Ask About Cyber Security[5].

Cyber security vulnerabilities are often publicly identified but remain unpatched for extended periods.[2] Organisations should also focus on standardising and rationalising the control environment to reduce residual risks. For further information on implementing patching in your organisation visit ASD's Guidelines for System Management[6].

For larger and more complex organisations control testing should be undertaken by independent cyber experts with a mandate to objectively challenge the design and appropriateness of controls, identify gaps and highlight areas requiring investment and uplift. Control testing reports should be made available to the board.

To gain a better undertaking of cyber security controls, it is advisable that boards undertake regular training, education and subscribe to latest advisories and via the Home Affairs Trusted Information and Sharing Network and the ASD Partnership Program[7].

Supply chain risk

Supply chain attacks are increasingly being used by cyber threat actors. An organisation's supply chain forms part of its attack surface, placing the confidentiality of data and systems at risk. As organisations increasingly rely upon vendors and managed service providers for critical data and software services, the need to evaluate and actively manage third-party cyber risk increases.

Therefore, an organisation's cyber risk posture should account for the importance, and potential risks, associated with key third-party suppliers. The board should engage with the leadership team that adequate measures are in place to manage and continually reassess third-party cyber risk.

ACSC SMALL BUSINESS GUIDANCE

The ACSC has extensive guidance to assist smaller organisations to improve their cyber risk-management and build cyber resilience.

This guidance can be found in the Small Business Cyber Security Guide and the Small Business Cyber Security Checklist. Key recommendations include:

- Implement multi-factor authentication;
- Use strong passwords or passphrases;
- Update software and use security software;
- Maintain and update backups; and
- Secure network and external services and harden the organisation's website.

In addition, the ACSC recommends implementing Maturity Level One of the Essential Eight.

> "Achieving sufficient assurance of information security controls operated by third-party service providers is a common challenge. This is a concern as more and more entities are relying on service providers to manage critical systems."
>
> — APRA, 2023[3]

2 Australian Signals Directorate, 2022 Top Routinely Exploited Vulnerabilities, available here[8].
3 https://www.apra.gov.au/news-and-publications/cyber-security-stocktake-exposes-gaps
4 https://www.aicd.com.au/risk-management/framework/cyber-security/cyber-security-governance-principles.html
5 https://www.cyber.gov.au/resources-business-and-government/governance-and-user-education/governance/questions-boards-ask-about-cyber-security
6 https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-system-management
7 https://www.cisc.gov.au/how-we-support-industry/partnership-and-collaboration/trusted-information-sharing-network#:~:text=TISN%20is%20an%20Australian%20Government,supply%20chain%20entities
8 https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/2022-top-routinely-exploited-vulnerabilities

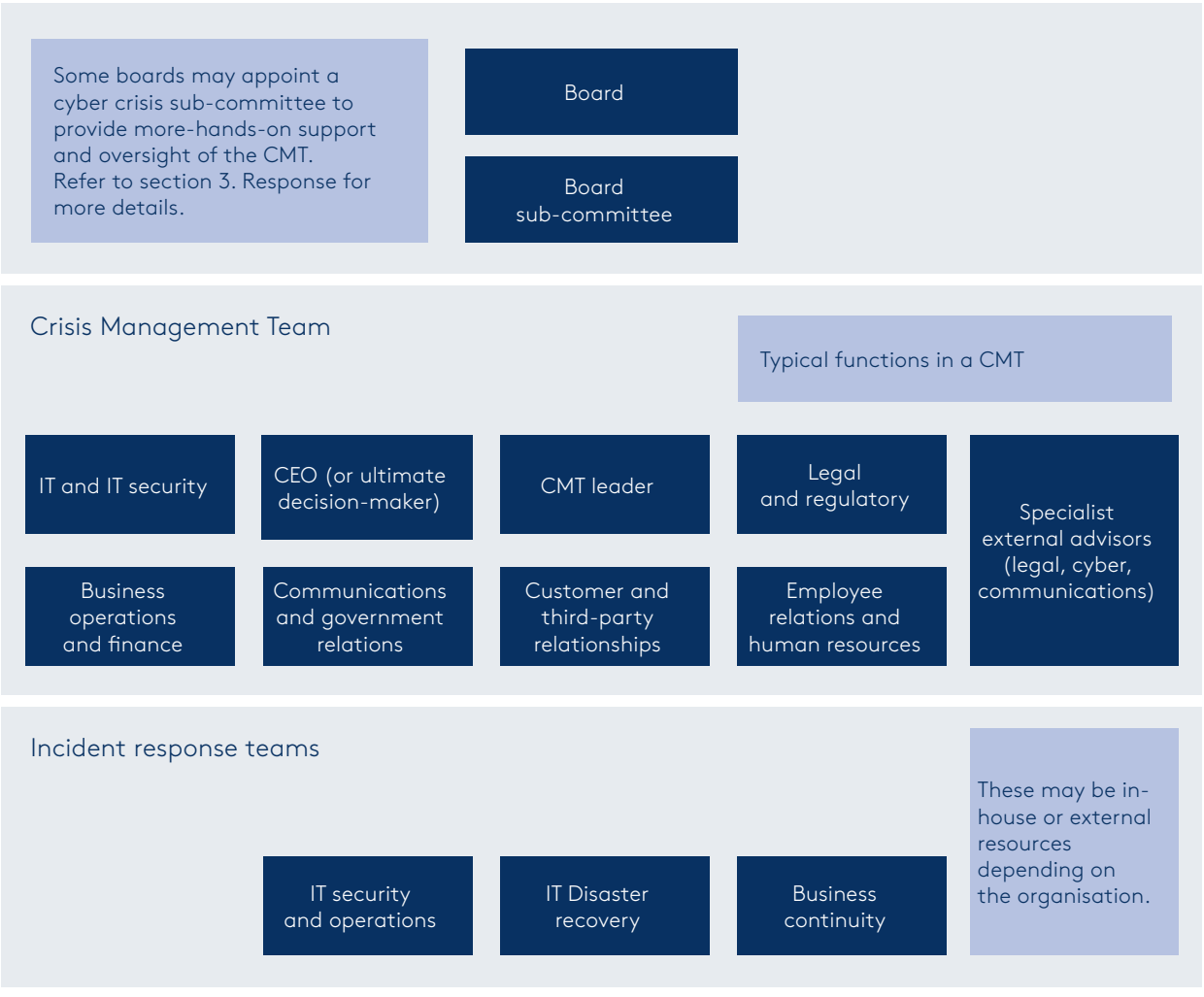
CLARITY OF ROLES AND RESPONSIBILITIES

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

A typical structure for a crisis management team is in the diagram below:

ESTABLISHING A CRISIS MANAGEMENT TEAM

For larger organisations, establishing a standing crisis management team (**CMT**) is good practice. The CMT has responsibility for developing and executing the response and recovery from any crisis incident. It will typically include the CEO as the primary decision-maker, a CMT leader who guides the team through response processes and protocols, functional leaders with responsibility for separate workstreams, and subject matter experts or specialists. Larger organisations may have several layers of crisis and incident response teams, while smaller organisations will have members who are often responsible for multiple areas of response.



CYBER INCIDENT RESPONSE PLAN

Mounting an effective response to a significant cyber incident is complex. There can be many unknowns, many moving pieces and it will likely evolve at a rapid pace.

This means that the board must be confident the organisation is adequately prepared for a range of possible scenarios and different threat actors. This experience can only be gained through having a well-tested cyber incident response plan (**response plan**) in place.

For larger organisations, this will involve a hierarchy of integrated operational and executive-level response plans, but all organisations should consider the key elements of a comprehensive response plan set out below. Appendix B contains detail on supporting plans for large businesses.

To be effective, a response plan should also be aligned with existing business continuity and crisis communication plans and procedures. Organisations may also consider developing a standalone ransom response plan.

What does a comprehensive cyber response plan entail?

While the scale and complexity of cyber readiness planning will be unique to the size and complexity of each organisation, boards should look to assess the appropriateness of eight key elements (in the table below) when developing, reviewing and updating a cyber response plan (or suite of response plans, depending on the complexity of your organisation).

SME AND NFP GUIDANCE: READINESS

- Document core elements of a response plan, including:
  - Who will be responsible in leading the response to a cyber crisis? How will that team communicate amongst each other if systems go down?
  - What are the key systems that are essential to the operations of the SME and NFP?
  - How will the organisation operate and communicate if all systems go offline for an extended period?
  - Do we hold highly sensitive or critical data, for example an NFP holding client/beneficiary personal information?
  - Where are our backups located and are they secure?
  - What will be our approach to communications, including responsibilities for communications?
  - What external sources of assistance and expertise can we call on? Have we already met them?

The ACSC has extensive resources to support smaller organisations, including a template response plan and readiness checklist, available **here**[1].

1. https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/publications/cyber-incident-response-plan

KEY ELEMENTS OF A RESPONSE PLAN

1	**Business continuity and disaster recovery** Are there adequate arrangements in place, including backups, to restore data and systems in the event of an incident? Have we considered continuity arrangements in a "worst-case scenario" where we are unable to recover critical operations or data in a timely manner, or where a significant number of systems are impacted simultaneously?
2	**Stakeholder management and communications** Have we identified our stakeholders, including employees, unions, regulators, government minsters, agencies and departments, shareholders, customers and clients and the media? Do we know who is responsible for engaging with them? Do we have key messages and holding statements for a range of cyber attack scenarios?
3	**Customer complaints and support** Have we identified the potential impacts on customers in a data breach or outage and planned for how we can support and communicate with customers? Do we have an appropriate plan and resources to handle customer queries and complaints?
4	**Data privacy and breach response** Do we have an adequate understanding of the personal and sensitive data we hold and where it is? Do we have a thorough plan that identifies when we would notify individuals and what support and advice we would provide to limit the risk of financial and non-financial harm?
5	**Third-party service providers and experts** Do we know whom we would call in the event of an incident? If we are relying on our IT provider(s), do they have adequate resources to support us? Have we conducted due diligence on any providers as part of our insurance panel arrangements? Do we know whom we would use for legal advice, crisis communications, IT forensics, ransom negotiation and crisis-management support?
6	**Regulator response and investigation** Have we clearly identified our regulatory reporting obligations and timeframes? Do we have adequate resources and expertise to anticipate and respond to regulators' questions and investigations? Do we know where to get extra resources should we need to divert staff to responding to the incident and/or regulators' inquiries? NOTE: the Federal Government has recently published a guide to cyber regulatory obligations[1].
7	**Playbooks and decision guidance** Do we have operational and technical plans in place for foreseeable cyber incidents, including system outages, ransomware attacks, DDOS attacks, data theft, third-party compromise and credential compromise attacks? Do we have guidance for critical decisions, such as ransom payments?
8	**Training and simulations** Do we have a program of training and testing that includes whole-of-organisation simulations as well as focused, team-based training to uplift specific skills and experience? Do we train and simulate for a range of scenarios, aligned to our cyber risk registers, as well as emerging cyber risk scenarios? Do we update plans and training based on lessons from real incidents in from across industry?

1. https://www.cisc.gov.au/resources-subsite/Documents/overview-cyber-security-obligations-corporate-leaders.pdf

TRAINING AND TESTING

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

A program of training and testing should include:

1. **Regular technical and physical penetration testing.** For more-mature organisations, penetration testing ('pen testing') should also include testing based on the assumption of compromise (both technical and physical) (e.g. allowing testers entry to an IT environment to determine how secure it is beyond the perimeter). Boards should be briefed on the scope and results of penetration testing, including understanding what controls and systems are tested and the remediation timetable in relation to high-risk vulnerabilities. Boards should note the remediation timetable in open action items for follow-up at each board meeting and consider the need to retest post remediation.

Ransomware or data extortion event

Insider attack

Third-party/key supplier data breach

Critical system or software failure

Cyber fraud (e.g. business email compromise)

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

3. **Testing an organisation's response through simulations:** Simulation exercises are a key tool for the board, senior management team and operational teams to test their knowledge of plans and processes and their roles and responsibilities during an incident. They differ from desktop exercises in that their purpose is to test people, processes and plans.

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

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

It may be worth doing simulation exercises where key executives or directors are unavailable to ensure that there is not an over-reliance on individuals.

ENGAGING EXTERNAL SUPPORT

In the event of a significant cyber incident, early consideration should be given to engaging external support, and in many cases support should be in place well before a cyber incident as part of robust planning.

External support within Government that should be engaged includes the Australian Signals Directorate, the Cyber Security Response Coordination Unit within the National Office for Cyber Security and, if appropriate, the Australian Federal Police.

Larger organisations should also plan to engage:

- external legal support;
- crisis management expertise to support the crisis management team;
- a third-party forensic investigator, IT consultants or incident responders with cyber capabilities;
- a public relations consultant to manage the media and communications; and
- in the event of a ransomware incident, a ransom negotiator and cyber risk consultant.

To enhance cyber preparedness and reduce cyber risk, organisations may also consider engaging external support and specialist advice as part of preparing for and preventing cyber crises before they occur.

The role of external advisors

Many directors who have experienced significant cyber incidents have spoken about the importance of the board and executive team having direct access to external advisors and specialists. Where possible, as part of the board's readiness planning, it is important that it has met with the experts it would call upon in the event of an incident.

Cyber response plans should clearly address the engagement of third-party experts, including the names and contact details of the experts to be engaged. It is important to remember the role of an external advisor is to provide advice and guidance – they cannot and should not be making decisions on behalf of the company.

If the organisation has cyber insurance, the insurer may need to approve external advisers. If the organisation's preferred external advisers are not already approved by insurers, approval to use those advisers and the rates recoverable should be negotiated with insurers before a cyber incident arises.

SMEs AND NFPs – ACCESS TO ASSISTANCE

SMEs that hold a cyber insurance policy can often access expert assistance via the insurer's nominated panel of experts in the event of significant cyber incident. Organisations should review their policy, understand whom they may have available to assist, and consider whether the panel of available providers is appropriate for their specific circumstances.

The Australian Cyber Security Centre also has extensive resources and guidance for SMEs to support technical cyber response and to advise them where to get help (available **here**[1]).

READINESS: GOVERNANCE RED FLAGS

1. The board and senior management have not undertaken scenario testing or incident simulations to test the response plan.
2. The organisation indicated there are no gaps in current cyber readiness.
3. Likely scenarios and consequences are undocumented with lessons from simulations not being captured.
4. It is unclear how communications with key stakeholders will be managed in the event of a critical incident.
5. It is not clear whom the organisation will engage to provide support during a critical cyber incident.

1. https://www.cyber.gov.au/report-and-recover/where-get-help

Role of insurance

Cyber insurance can protect against the financial costs and losses of a cyber incident.

Various types of policies can respond to a cyber incident, including cyber insurance, professional indemnity insurance, business interruption insurance and directors' and officers' liability insurance.

The organisation should undertake a review of its insurance cover to test and assess its insured and uninsured risks. It may be possible to typically insure uninsured risks if this is desirable. The board and senior management team must understand the insurance cover and conditions available to the organisation for cyber incidents, which will include notification and insurer consent requirements.

Even if a decision is made not to purchase insurance, the exercise of exploring potential coverage can reveal potential weaknesses. In particular, insurer questionnaires can highlight common vulnerabilities and help organisations to benchmark their readiness.

READINESS: KEY QUESTIONS FOR DIRECTORS

1. Are roles and responsibilities comprehensively documented, including the role of the Chair and specific directors in the event of a significant incident?
2. Are the processes for key decision-making and external support detailed in the response plan?
3. Do we have a comprehensive approach and plan to communicating with internal and external stakeholders, including responsibilities for notifying and engaging with regulators and approving market disclosures?
4. Do we understand how insurance would operate in the event of an incident and the support the insurer can/cannot provide?
5. Do we regularly scenario test or conduct a simulation on our response plan? How often do we review the response plan and update it to ensure it reflects organisational changes and the current threat environment?

3. Response

KEY POINTS

1. The dynamic and fluid nature of a cyber crisis means the board should provide agile and timely support and oversight of management decision-making.
2. For larger organisations, establishing a Cyber Incident Sub-Committee of the board is good practice in providing effective and agile governance during the response phase of a cyber crisis in helping the board to effectively oversee decision-making.
3. Consistent, timely and transparent communications with key stakeholders, such as customers and employees, is critical in the response phase and plays an important role in mitigating reputational damage.
4. Expert external advice plays a critical role in the board effectively overseeing decision-making during the response phase.
5. For larger organisations, consider establishing a remediation and post-incident review team in parallel to the response team.

> "When you're a chair, you've just got to drop everything and be there."
>
> — Senior Chair, ASX-listed company

IMMEDIATE RESPONSE

The board has an important role to play in overseeing the decisions of management during the immediate response phase of a significant cyber incident.

Directors should expect a critical cyber incident to rapidly evolve with decision-making based on imperfect information. Early indicators of the incident are often incorrect and underestimated, including the number of impacted individuals, the type and volume of data compromised and the recovery timeframe. Directors should adopt a dynamic and adapting mindset to this environment.

The board's role includes ensuring the safety of employees and customers has been prioritised, management has the necessary support to respond to the incident and that key elements of the response plan have been initiated.

Central issues the board should consider include:

- Whether the organisation has triggered the appropriate response plans and has a robust cadence of meetings, updates and tracking action items. For listed companies, the continuous disclosure sub-committee should also be convened.
- Affected areas of the organisation have been identified and an understanding of the impacts on business operations, employees and customers has been established.
- Testing the accuracy of information that forms the basis of critical decisions and communications, noting the fact base is likely to change rapidly over the first few days.
- The potential sensitivity of data which may have been impacted has been assessed, as well as any information available confirming whether there has been a data breach.
- Immediate regulatory notifications or continuous disclosure obligations have been considered and actioned – these should be clearly articulated in the response plans.
- Whether key third-party providers are prioritising and assisting on the incident.
- Identifying what resources (internal and external) are available to support (including from your insurance panel).
- Initial assessment of the severity of the incident and its likely impact on the organisation, customers and key stakeholders is underway.
- Ensuring insurers are notified and insurer consents have been obtained, where required.
- Drafting communications to employees, customers and third parties is underway.

TRIAGE – INCIDENT RESPONSE CHECKLIST

- ✓ What is our understanding of the cyber incident?
- ✓ Is there an imminent or actual threat to the safety of our staff and continuing business operations?
- ✓ Who knows about the cyber incident internally and externally?
- ✓ Who needs to know about the cyber incident internally and/or externally?
- ✓ How sensitive is the information that may have been compromised?
- ✓ What additional information do we need? Where can we get this information and are there any risks?
- ✓ What are our mandatory and voluntary regulatory and government notifications?
- ✓ Have we received any complaints or media enquiries?

> "When a cyber crisis occurs you know you have to act fast but until it happens to your organisation you don't realise how fast."
>
> — Senior Chair, ASX-listed company and NFP

GOVERNANCE STRUCTURES

The board

While management, or the CMT at larger/more-complex organisations, will maintain responsibility for the response to the crisis until it is contained, the board must ensure it receives regular updates. The executives leading the response must be clear on which decisions must be escalated to the board for approval.

The board will play a critical role in reviewing and challenging the assumptions made by the whole board. Therefore, directors must be satisfied they are receiving adequate updates and documentation, with direct access to internal and external experts as required, to allow them to fulfil their oversight obligations.

The board must also be comfortable that the regular operations of the organisation are being given adequate attention despite the unfolding crisis.

SME AND NFP GUIDANCE: RESPONSE

- Seek assistance from trusted sources.
- Report the incident to the ACSC.
- Inform key stakeholders, including partners, in a transparent and timely manner.
- Restore systems, critical operations and data from backups, where possible. Prioritise recovering essential functions.
- Reset all passwords for affected accounts, including employee, customer, service and administrator accounts.

Cyber Incident Sub-Committee

Larger organisations may have a separate Cyber Incident Sub-Committee (**sub-committee**) comprising two or three board members which can be convened at short notice to provide agile support to management during a cyber crisis. The sub-committee can also be used to report regularly to the whole board.

The sub-committee can, with appropriate delegations, act as the key point of information for the whole board, facilitating timely decision-making and providing support to management during a cyber incident.

The sub-committee can assist with:

- effective and fast decision-making, including approving spending decisions;
- strategic-level oversight of the incident response and availability of adequate resources and specialist expertise;
- reviewing regular updates on internal and external investigations;
- overseeing stakeholder communications; and
- providing oversight of management's post-incident planning and review.

The sub-committee should employ a strategic approach and longer-term view by anticipating outcomes and consequences of management's decisions. It can also help to anticipate any potential strategic and reputational risks and manage key stakeholder relationships throughout the cyber incident.

Of course, having a subcommittee does not mean that all other directors are absolved of their duties. All members of the board must be satisfied in the organisation's response". We should also say that the mandate of the sub-committee should be clear, and ideally agreed as part of the readiness planning of the organisation, rather than hastily convened on an ad hoc basis during an incident.

BOARD REPORTING DURING AN INCIDENT

During a cyber crisis, it is vital that there is comprehensive and clear reporting to the board. This provides the board with appropriate oversight of the incident response. Although a desire for reporting and greater information should be balanced with the understanding that management will be under significant pressure and focused on responding to the incident.

Board papers should be prepared and presented on key actions being undertaken and progress against targets, including on any critical issues, emerging and current risks and how they are being managed within the organisation's risk-management framework.

It is important to acknowledge that senior management will be working under extreme pressure, so extensive board papers will not always be necessary, with verbal briefings and updates via email also adequate. The Company Secretary should contemporaneously record and accurately document the discussions undertaken and any decisions made by the board and circulate them promptly. It is good practice for a paper to be subsequently prepared on the items reported to the board outside of the meeting cycle.

The importance of check and challenge

The board should have a clear understanding of what is being reported and the impact on the organisation, regulatory obligations and customers and be able to demonstrate they have queried and raised issues with senior management and the CMT, rather than just relying on, or accepting, information at face value. It is particularly important that the board checks and challenges what is being reported if the subject matter is highly technical and difficult to understand. The board should openly question the technical experts and request a 'plain English' explanation if they do not fully understand the subject matter.

Early indicators of the impact of an incident are often wrong and underestimated. This includes issues such as the number of impacted individuals, the type of data compromised and the recovery timeframe for operations to return to normal.

Organisations should recognise that a major cyber incident can prompt a range of emotional responses from impacted customers and/or stakeholders. Communications should be sensitive to such sentiment and not be seen as the organisation seeking to avoid responsibility or downplaying the harm caused.

STAKEHOLDER COMMUNICATIONS

A key responsibility of the board during the response phase is overseeing communications with the key stakeholders of the organisation. The key stakeholders should be documented in the response plan and would typically include shareholders, employees, customers, suppliers, government regulators and agencies.

The response plans should clearly identify all key stakeholders in order of priority, along with their direct contact details and the person allocated with responsibility to make contact. Larger organisations should also have an integrated Communications Plan.

Organisations need to be deliberate about selecting the most appropriate spokesperson. Typically in order to show appropriate accountability and senior executive focus, the CEO would be the primary public spokesperson on a cyber incident

The board and individual directors, particularly the chair, may play a role in engaging with more-important stakeholders, such as regulators or key customers. A clear and comprehensive approach to communications during a significant cyber incident is critical (link to page 44 of the AICD CSCRC ***Cyber Security Governance Principles***).

> "Be really clear about who your critical stakeholders are, how you communicate with them and who communicates with them."
>
> — Senior Chair, ASX-listed company

The importance of timeliness, accuracy and transparency

An organisation should aim to communicate as efficiently, accurately and transparently as possible, within the context of the risks that might arise. This includes, where possible, articulating what went wrong, how it will be fixed and how the organisation will assist impacted customers and stakeholders. Demonstrating actions your customers and employees can take may contribute to minimising down-stream reputational, legal and regulatory risk.

When considering what and when to communicate, the board and management will need to assess and balance:

- The importance of communicating early, but avoiding any ***unnecessary*** angst or stress with customers, the public and community;
- The need to communicate what has gone wrong, in a vacuum of information or with incomplete information, and the need to avoid speculation, noting that the fact base is highly likely to change;
- The correct or most-effective sequencing of communications to regulators, government agencies, the media, customers and employees;
- Legal and security considerations and the importance of managing down-stream investigations and/or not compromising any police investigations; and
- the appropriate medium and platforms to communicate to impacted and/or interested stakeholders – e.g. email and/or SMS notifications, website FAQs, social media posts, media releases.

It may be prudent to remind staff of the organisation's media and social media policies to prevent employees creating confusion or misleading stakeholders through public commentary.

Clear principles

It is important that clear principles are agreed at the outset to ensure all communications and messaging are consistent. The response plan (or integrated Communications Plan) should identify these principles. For example, it could be agreed the key guiding principle for all communications is the need for an organisation to act in the best interests of its customers and employees and to mitigate potential risk of harm to victims. Ideally, template communications prepared in advance of the incident can be adapted appropriately.

While communications will ultimately be the responsibility of senior management, the board should be closely engaged given the potential impact on corporate reputation and stakeholder relationships.

Internal communications

In some cases, there will be no, or limited, access to corporate systems (including email and phone) during the incident. In these circumstances, alternative communication methods will need to be established as a matter of urgency. The response plan should address the steps to be taken if this scenario arises.

It is important that hard copies of the response plan(s) and a key contacts list (including contact details for the board, CMT, key internal and external response staff, key stakeholders) are kept in all office locations.

It is also critical that the response leaders and board have pre-determined who will be contacted out of hours and how board members will also receive relevant plans in hard copy (which should be updated and reviewed regularly). External board portals can also play a role.

Market disclosure for ASX-listed entities

Continuous disclosure obligations under the Corporations Act and ASX Listing Rules in Australia require listed companies to immediately disclose any information they become aware of that a reasonable person would expect to have a material effect on the price or value of their securities.

Boards should be cognisant that materiality in the early days of a cyber incident may be challenging to determine with any certainty.

When this obligation is triggered during a cyber incident, it is likely that limited information will be known about the impact of the incident. This information can also change quickly, making it difficult to determine what information to disclose and when to disclose it. However, failing to do so could lead to legal and reputational issues.

Difficult judgment calls may be required as to whether an announcement should be lodged, which is why key consideration must be given to the circumstances for undertaking a trading halt.

The board should consider convening the continuous disclosure committee and whether to initiate a trading-halt plan. Boards will also need to determine the triggers and thresholds for updating any announcements. Given the complexity of managing disclosure legal obligations during a major cyber incident, and liability risks, external legal advice should typically be sought" to the end.

KEY CONSIDERATIONS: UNDERTAKING A TRADING HALT

An organisation's Trading Halt Plan should:

1. include the circumstances in which a trading halt will be sought and have a draft trading halt application prepared. The trading halt should also be available in hard copy in case the organisation's systems cannot be accessed during the incident;
2. agree the circumstances in which a voluntary suspension will be sought, and the proposed length of time of the voluntary suspension;
3. set out the protocol for out-of-hours contact with the organisation's listing officer, including their contact details; and
4. consider the impact of the organisation's securities being suspended for an extended period, including the impact this may have on the organisation's ability to rely on the cleansing notice regime for future securities issues.

Media management

The reputational damage arising from poor communications during an incident can be more damaging than the incident itself. It may be appropriate to brief an external media consultant or public relations firm to assist, depending upon the size of the organisation and the potential reputational damage which could be sustained.

Boards and management should expect all public facing statements and internal documents will be provided to regulators and used in any subsequent litigation, including shareholder class actions. Therefore, it is vital that all public statements are consistent with the true position of the company at a particular time during the incident. Management should also be aware that public communications and media statements may influence the actions of a threat actor; for instance, in a ransomware incident. Similarly, all media interviews and media articles can be used in litigation, so incorrect statements should be amended as soon as possible.

The response plan should cover responsibility for monitoring media coverage of the incident and reporting back to the board.

REGULATORY REPORTING AND NOTIFICATION OBLIGATIONS

During a critical cyber incident many organisations, both large and small, are likely to have mandatory reporting and notification obligations at Commonwealth and state levels. The organisation will also receive a high volume of requests for information and updates from a range of key stakeholders including regulators, commercial third-party suppliers, partners and impacted individuals.

The nature and type of the reporting and notification obligations will differ based on the size and complexity of the organisation, its industry and the nature of the cyber incident (e.g. whether it entails a data breach). A comprehensive response plan should include the different reporting obligations in the event of an incident and when each reporting obligation might be triggered – this is a complex task and takes considerable effort to be done thoroughly.

A board should oversee and have visibility of regulatory reporting and notification obligations and ensure they are being met. Key reporting frameworks a board should have knowledge of include the Notifiable Data Breaches scheme under the Privacy Act, reporting obligations under the SOCI Act (if applicable) and separate reporting/notification requirements for listed entities who may need to notify the ASX and financial services entities regulated by APRA and ASIC.

ASD provides guidance and best practice cyber security advice and assistance to government, organisations, critical infrastructure and the community. Visit cyber.gov.au for the latest advice and guidance.

Even when reporting is not mandatory, individuals and organisations of all sizes are encouraged to report cyber incidents to ReportCyber. This helps build a strong understanding of the national cyber threat picture, and informs future ASD cyber security guidance, tools and services.

CYBER.GOV.AU – REPORTING PORTAL

The ACSC website provides a valuable reporting resource with a list of all regulatory reporting obligations and a link to each reporting portal.

This effectively steps a user through the reporting processes based on industry and other regulatory reporting obligations.

In addition, the ACSC 24-hour Cyber Security Hotline (**1300 CYBER1 (1300 292 371**) is a key source of advice for individuals, business and subject matter experts.

> “Make the best judgement you can with the information you have in front of you.”
>
> — **Senior Chair, ASX-listed company**

ROLE OF GOVERNMENT – SUPPORT AND ASSISTANCE

The Australian Cyber Security Centre (ACSC) and Australian Signals Directorate (ASD)

The ASD/ACSC **can provide technical advice and assistance**[1], supporting organisations in their incident response efforts. Organisations are encouraged to report incidents and share technical information with the ACSC as early as possible. Australian businesses and organisations are encouraged to join the **ASD Cyber Security Partnership Program**[2]. Partners receive the latest cyber security insights and access to the experience, skills and capability of thousands of Australian organisations to collectively lift cyber resilience across the nation. Advice and assistance may include information on incident containment and providing contacts with other government entities that may be able to support response and support for impacted individuals.

The National Cyber Security Coordinator

The National Cyber Security Coordinator (**the Coordinator**) and the National Office of Cyber Security (**NOCS**), manage the whole-of-government response to major cyber incidents. This includes bringing together all relevant Commonwealth, state and territory agencies to align and coordinate the support provided to organisations managing the consequences of cyber incidents.

By establishing working groups with a range of stakeholders and the impacted entity, the NOCS can support impacted entities to efficiently distribute information across government and support streamlined information requests and briefings as well as assist in understanding and managing the consequences of the incident.

INFORMATION REQUESTS FROM ACSC AND THE NATIONAL CYBER SECURITY COORDINATOR

Organisations might be requested to provide the following information to the ACSC and/or the National Cyber Security Coordinator:

- Logs and memory dumps;
- Network traffic data;
- Indicators of compromise;
- Samples of malware;
- The number of potential or suspected individuals impacted by the incident;
- The types of government-issued identity documents that may have been accessed or stolen;
- Details regarding the impact on vulnerable individuals and/or communities;
- The anticipated timeframe for recovery; and
- Copies of any ransom notes or contact from a threat actor.

Organisations should seek independent legal advice when sharing information with any third-party, but should be encouraged to share technical details with the ACSC as quickly as possible.

1 https://www.cyber.gov.au/report-and-recover/how-asdacsc-can-help-during-cyber-security-incident
2 https://www.cyber.gov.au/resources-business-and-government/partner-hub

LEGAL ADVICE AND SUPPORT

Timely and comprehensive legal advice will often be critical to a board and organisation effectively responding to a cyber crisis. Legal advisers can provide assistance to the organisation in navigating mandatory disclosure obligations, regulatory requirements, disclosure under existing contractual relationships, retention of evidence, method of engaging third parties, preservation of privilege and the legality of paying a ransom.

For some larger, complex organisations it may be appropriate to engage expert advice during the development of a response plan to avoid uncertainty during the immediate response phase.

The board itself can benefit from having specific legal advice to ensure it is meeting its obligations. This advice can be an important source of assurance for the board in a complex and rapidly changing environment.

There may be a tension between the desire to restore the organisation's systems and revert to BAU as quickly as possible, and the need to preserve evidence relating to the cyber incident. The board should test with management whether the preservation of evidence is being prioritised if future litigation or regulatory proceedings are reasonably anticipated.

ROLE OF KEY THIRD PARTIES

Assistance and support

Areas where third-party providers can assist during the response and immediate recovery period, include:

- Incident detection: Many software providers have built-in security features that can detect suspicious activity and notify the organisation of an attack or potential attack. This rapid notification can be crucial in containing the attack before it causes more damage.
- Threat analysis: Once an attack is detected, the software provider can help to identify the type of attack, the attacker's methods, and the affected systems.
- Isolation and containment: The provider may be able to assist in isolating the affected systems to prevent the attack from spreading to other parts of your network. This may involve shutting down certain systems or applications.
- Eradication: The provider may assist in taking steps to expel the attacker from systems.
- Recovery: A provider may be able to support in recovering data and restoring systems from backup.
- System repair and restoration: The software provider may in some cases be able to assist with repairing or restoring damaged systems.

The board should understand the dependency on these external providers and how they are assisting the management team and the organisation in responding to the cyber crisis. It may be appropriate for the organisation to authorise the third-party to work and share information with the ASD as a part of a collaborative effort to respond to the incident.

In an incident specialist advisers can provide an important frank, independent assessment of how the organisation is responding. It may be appropriate for the board to meet with advisors without management present.

RESPONSE: GOVERNANCE RED FLAGS

1. A significant delay in discovering the incident and understanding the impact on systems and key stakeholders, including staff and customers.
2. Confusing or contradictory information reported to the board and/or communicated to staff, customers and key regulators and government agencies.
3. Key elements of the Response Plan not being followed, for instance a lack of collaboration and information sharing between different departments or teams.
4. Failing to utilise the expertise of external advisers and cyber security professionals including regarding approach to communications.

Contractual implications

A significant cyber incident will impact operations and the ability to access data and systems. This commonly leads to circumstances where organisations are unable to fulfil their contractual obligations.

Organisations may also be required to notify contractual counterparties of the incident within a specific timeframe, and third parties may have a contractual right to attend the organisation's premises for auditing purposes. If the organisation has a contract with a Commonwealth or state agency/department there are often specific contractual notification obligations that should be understood in advance.

Organisations should also be prepared for the fact that third parties are likely to immediately disconnect from their systems as soon as they are notified of the incident and will remain disconnected until the incident has been contained and systems restored. This may impact the organisation's ability to operate and should be contemplated in the response plans. The response plans should include a list of all notifications required under existing contractual arrangements, including any specified timeframes and whether an incident could enliven force majeure clauses.

KEY QUESTIONS FOR DIRECTORS

1. Do we need to establish a sub-committee of the board to oversee management's actions during the response phase and speed-up decision-making?
2. Do we understand our legal and contractual obligations to make notifications (to whom, when and of what)? Do we have a set of priorities for the most-urgent to least-urgent notifications?
3. Who has primary responsibility for making those notifications? Has legal advice been sought on those notifications and their content?
4. Are we satisfied that the resources available to the management team to respond to the incident are appropriate given the scale and complexity of the organisation and the nature of the incident?
5. What key third-party providers are we relying on to provide support during the response phase? What is the nature of this support?

4. Critical response scenario: A data and system extortion crisis

In this section, we focus on the role of the board in respect of a response to a particular type of cyber crisis – a data extortion event.

What is an extortion crisis?

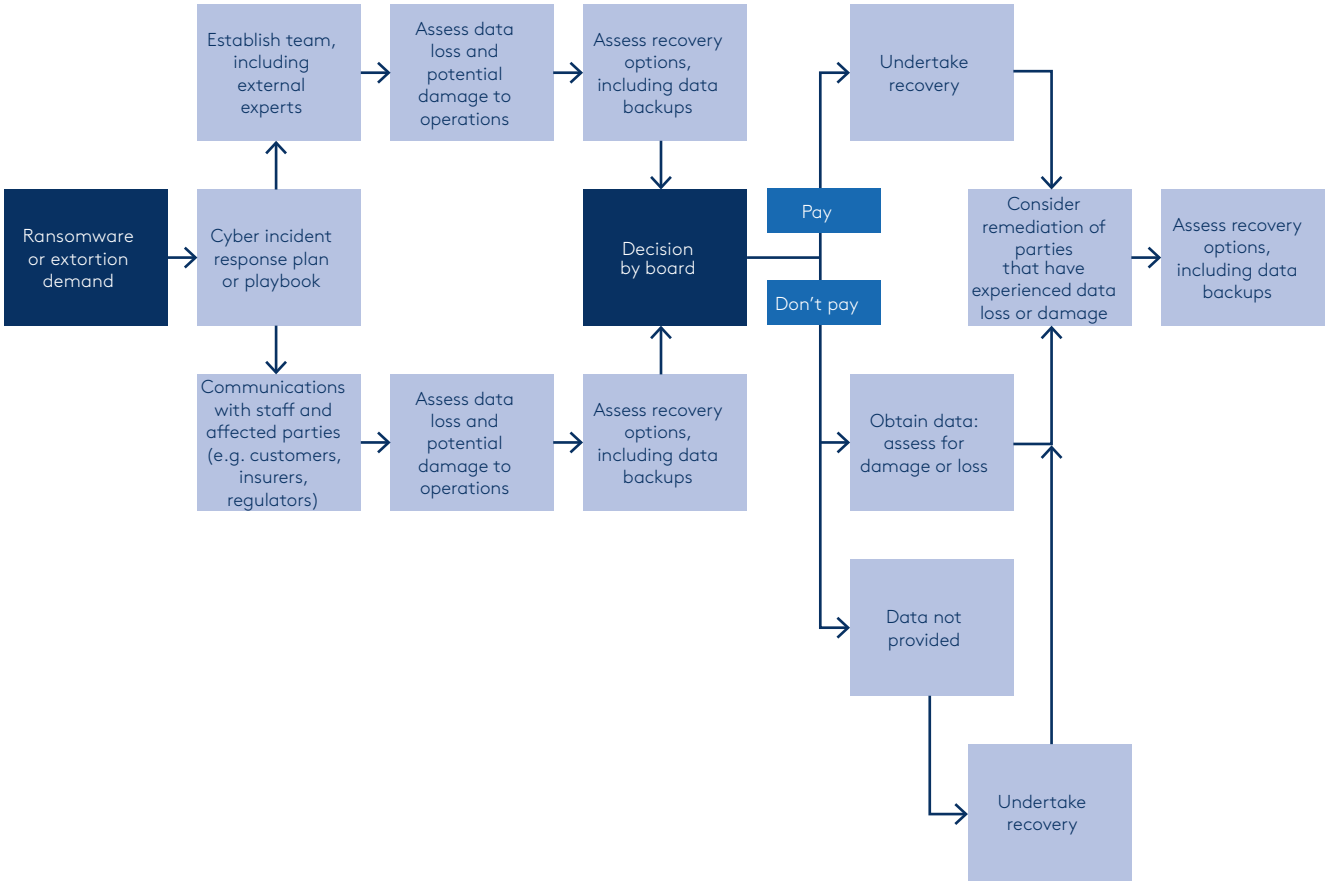
An extortion crisis (commonly also referred to as ransomware) involves a threat actor making a ransom demand following a cyber crisis, usually on the basis the threat actor 'promises' not to release the organisation's data, or returns access to key systems, when payment is made.

According to the 2023-2030 Australian Cyber Security Strategy, "the ransomware business model is fuelled by payments made to cybercriminals, with cryptocurrency transactions enabling malicious actors to anonymously profit from extortion claims. Paying a ransom does **not** guarantee that sensitive data will be recovered. It also makes Australia a more attractive target for criminal groups.

While organisations will need to undertake their own assessment, boards should note the Government's firm policy position on ransom payments, which is not to pay.

The accompanying decision tree is taken from the AICD CSCRC Cyber Security Governance Principles.

Decision tree



Key roles, responsibilities and objectives

In the event of an extortion event, there are two critical decisions a board will need to have visibility over: whether or not to make contact with the threat actor and whether to pay the ransom.

It is important that there is clarity around who has the authority to make critical decisions, and who should have visibility of them. The decision-making process and delegated authority should be clearly set out in the organisation's cyber response plan.

It is crucial for the board to understand the objectives for contacting a threat actor or paying a ransom. The objectives should be documented and based on the best possible information and analysis, recognising there can be significant time pressure and uncertainty.

Once the objectives underlying the critical decision have been considered, the board will need to make a risk-based decision considering all relevant factors.

A summary of key responsibilities is set out in the following table and should be read alongside legal and government policy considerations, below). In particular, in making these decisions directors should be guided by a clear-eyed assessment of what is in the best interests of the organisation.

EXAMPLE - MAKING CONTACT WITH THE THREAT ACTOR

What are the **key objectives** of making contact with the threat actor?

- To seek more information about the attack and/or the scale of any data theft.
- To determine the likely identity of the threat actor.
- To determine the "integrity" of the threat actor – how likely it is that they will delete stolen data and/or that their decryption keys will accelerate recovery of encrypted systems.
- To delay the threat actor from uploading, publicising or selling data or details about the attack.

ROLE	RESPONSIBILITIES
Board	Ultimately responsible for whether to engage with the threat actor and whether to pay a ransom or for ensuring a clear delegation-of-payment decision. Some board members may also be called upon to brief, and receive confidential briefings from, government and law enforcement, including the ACSC, ASD, National Office of Cyber Security and AFP.
Senior management/ Crisis Management Team (CMT)	Key responsibilities include: a) Ongoing management of the crisis and ensuring the senior management team and the board have access to appropriate external experts. b) Undertaking the assessment, for board approval, and providing input into the decision of whether to pay a ransom. c) Ensuring the implementation of activities and communications that limit the impact and risk of harm to the organisations and impacted individuals. d) Briefing senior regulators, ACSC, ASD, National Office of Cyber Security and law enforcement stakeholders.
Finance	Responsible for facilitating the payment of a ransom demand, with appropriate legal advice and board approvals.
Legal & Risk	Responsible for providing legal advice to the board and CMT on ransomware payment decisions, including: a) The legality of a ransom payment (including the consideration of sanctions, anti-money laundering and counter terrorism financing obligations). b) Law enforcement (AFP and state) liaison. c) Advising on potential sanctions, anti-money laundering, counter terrorism and other criminal offenses. d) The use of Legal Professional Privilege when engaging third-party advisors, particularly advisors who may be called upon to report on the root cause(s) of a ransomware attack or write a post-incident review. e) The coverage of any relevant insurance policies. f) Harm reduction decisions and actions in the event of a breach of personal data.
Operations (including IT and security)	Responsible for assessing the impact on critical systems and data and determining the likelihood of recovery within an acceptable timeframe. Also, for providing viable alternatives for recovery and assessing the likelihood that payment of a ransom might accelerate recovery.
External advisors	External advisors are critical in any ransom decision-making. a) External legal counsel can advise on the legality of ransom payments and the risks of legal enforcement action. b) Specialist ransom negotiators can advise on: – the likely identity (typically the affiliations) of the threat actors and their method and track record, including reliability in returning data or system access; – the process of purchasing crypto currency; and – assist with law enforcement liaison. Law enforcement are continually updating their own databases of encryption keys that can be provided to assist organisations in their recovery from certain ransomware attacks.

DECISION-MAKING ON THE PAYMENT OF A RANSOM

The decision to pay or not to pay a ransom is complex and should be the responsibility of the board. This role should be clearly documented in the response plan.

Ransom payment does not guarantee the return, destruction or security of stolen data and systems. Payment also does not guarantee the threat actor will provide the decryption key to enable the full restoration of the organisation's systems. It's uncommon for an organisation to have their systems fully restored after a significant cyber incident, even if a ransom is paid.

Board reporting or information flow from management and internal/external experts is crucial in the decision-making process. While timing and urgency may limit written board reports, a risk-based approach to making the decision to pay a ransom will ensure consideration is made only in the most extreme risk circumstances.

A risk-based approach considers factors including the potential impact or harm on employees and customers if data or systems are not retrieved. It also accounts for any mitigants against identified risks. A board should also be aware that irrespective of whether a ransom is paid or not, the threat actor will likely have made a copy of the stolen data. This means it still could be on-sold or used in other ways by other threat actors, including state-sponsored actors.

BOARD REPORTING AND INFORMATION FLOW IN A RANSOMWARE EVENT

- **Situation update:** What is the known impact on systems and key data?
- **The threat actor:** What is known about the identity and history of the threat actor? Can appropriate due diligence be conducted to satisfy sanctions, anti-money laundering and counter terrorism financing obligations?
- **Critical asset impact analysis:** What is the impact on critical assets and the likely recovery time? How does this impact customers? What are the current restoration options and the likelihood of success?
- **Risk assessment:** What are the risks of making a payment? Including legal, reputation, national security and operational? Do the benefits of paying (if any) significantly outweigh the risks of paying and the alternative means of mitigating risks while not paying?

Legal considerations and government policy

The legality of making a ransomware payment is unclear.

Although there is no express prohibition on payment of ransoms in Australia, certain laws mean in some circumstances payment of a ransom may be illegal – such as the ***Anti-Money Laundering and Counter-Terrorism Financing Act 2006*** (Cth), ***Autonomous Sanctions Act 2011*** and the ***Criminal Code Act 1995*** (Cth).

Making or facilitating a ransom payment to a person or entity subject to a sanction would be a contravention of sanctions law and could expose businesses to criminal penalties. Guidance on Australia's cyber sanctions regime can be found on the Department of Foreign Affairs and Trade's **website**[1].

Under such laws, directors may be personally and/or criminally liable if they make the decision to pay. The potential consequences relating to directors of paying a ransom in the specific circumstance, should be included in legal advice.

As previously noted, the Government's advice is also clear – in the event of a ransomware attack the ransom should not be paid.

As part of the strategy, the Government has committed to work with industry to design a no-fault, no-liability ransomware reporting obligation. Separately, it has committed to provide guidance to industry on how to prepare for and deal with ransom demands.

EXAMPLE – RISK ASSESSMENT OF THE PAYMENT OF A RANSOM

When assessing whether to pay a ransom, boards should consider:

- The level of disruption to the organisation, whether critical systems or assets have been attacked and whether the risks can be adequately mitigated;
- The anticipated cost of the incident and recovery time, the sustainability of business continuity arrangements and any likely failure of critical operations;
- Measures to protect data and minimise harm to individuals and third parties whose data may be compromised;
- The recovery of systems and data as quickly as possible, without compromising security;
- The security and stability of any critical infrastructure, and whether a threat to life could arise if the organisation does not engage or pay the ransom;
- The need to preserve evidence for future investigation, noting this may cause delays to the completion of some of the recovery tasks;
- The anticipated impact on customers and stakeholders were the ransom is not paid;
- Who is making the ransomware threat, including understanding sanctions, anti-money laundering or counter-terrorism financing obligations;
- The level of confidence that payment will be effective;
- Potential legal consequences; and
- Reputational impact, including with government.

1 https://www.dfat.gov.au/international-relations/guidance-note-cyber-sanctions

5. Recovery

KEY POINTS

1. Oversee steps to secure systems and data are appropriate, including any immediate or short-term investment in cyber security has been implemented.
2. Understand the impact of the crisis on employee well-being and take steps to support employees impacted by the cyber crisis.
3. The board should oversee a comprehensive post-incident review, including utilising external advice where appropriate.
4. Remain focused on how the incident has impacted customers and how the organisation may need to continue to support customers.

ROLE OF THE BOARD

The recovery phase begins when the crisis has been contained and no longer represents an immediate risk to an organisation's data, systems, people and customers, with systems operating at a level that enables BAU (business as usual) activity to resume.

The role of the board in the recovery phase is to oversee and assist management to secure systems, understanding the impact and what went wrong and returning the organisation to BAU.

> "It is critical that the board doesn't forget the human element, the profound impact on customers and employees."
>
> — Senior director ASX listed-company

A BOARD SHOULD BE SATISFIED THAT THE MANAGEMENT TEAM:	
1	Has taken all reasonable steps to ensure its systems are secure and there is no further threat actor activity in the organisation's systems.
2	Has adequate resources and funds to uplift security controls and systems.
3	Conducts a comprehensive, board-sponsored review of the root causes of the incident that satisfies the board and the anticipated needs of key regulators.
4	Is engaging and communicating in an ongoing manner with all key stakeholders.
5	Has a comprehensive plan and is taking action to continue to mitigate the risk of harm to individuals impacted by any data breach.
6	Has taken appropriate measures to understand and mitigate psychosocial risks associated with fatigue and stress that employees and frontline staff may have experienced during the response phase of the incident.
7	Is identifying the potential risks of downstream regulatory investigation, disputes and class actions.

SECURITY UPLIFT IN THE RECOVERY PHASE

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

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

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

REVERTING TO BAU

As the organisation returns to normal, the board will need to be satisfied key processes or compliance activities which may have fallen by the wayside during the incident are addressed.

In significant incidents where data has been lost, the board will need to be satisfied the organisation has a plan in place to rebuild systems and recover critical data as part of the return to BAU. If lost data included information required for audit, tax and financial accounting, or information to comply with regulatory obligations, the board must have oversight of the data re-build process and, in particular, the quality control and verification processes in place in advance of any audit.

If there are concerns regarding ongoing data integrity, the organisation may need to consider engaging with external auditors.

SME AND NFP GUIDANCE: RECOVERY

- Where possible, invest in cyber security enhancements, such as storing key data and systems with reputable cloud providers or migrating key functions to SaaS providers.
- Support impacted employees and volunteers.
- Enhance employee and volunteer training, such as cyber hygiene practices and awareness of scams.
- Implement strong password policies with multi-factor authentication.

WELLBEING OF STAFF

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

The wellbeing of staff should be a key consideration in the recovery period, with a supportive, team-focused culture central to effective recovery and rebuild. Concrete steps a board could oversee and prompt management to implement include:

- Regular communications and briefings: Keep staff updated on the progress of the recovery process and any new developments.
- Offer emotional support: Acknowledge the emotional impact the attack may have on staff and provide access to resources like Employee Assistance Programs or mental health hotlines.
- Assist with identity theft concerns: If employees' personal data was compromised, offer staff financial support to replace identify documents and identity theft reporting/scanning services.
- Acknowledge and reward efforts: Recognise and thank staff for their resilience and cooperation during this difficult time and acknowledge the emotional toll from the crisis. Consider whether mechanisms such as time in lieu should be offered for relevant staff, and that their efforts feed into performance reviews.

It is also important to encourage a supportive 'no blame' environment during the incident response phase – consequence management can be determined at a later date.

DATA INVESTIGATION

Once the incident has been contained, the organisation will need to investigate the scope of any data breach.

The forensic data analysis process can be long and challenging. Advanced search and identification technology and forensic tools will be used to extract data from the documents suspected of being compromised. The document review team will then identify patterns within the data that would indicate whether individual documents had potentially been compromised. That information can be analysed to generate customised reports and, if necessary, produce correspondence notifying affected individuals of the breach.

If there has been a significant data breach, a framework to respond to customers' complaints will need to be developed, together with a methodology for compensation and reimbursement (see Remediation section). Both require board oversight.

It is important that the recovery and remediation phase is carefully managed, and that early legal advice is sought on how to protect legal professional privilege if litigation is reasonably anticipated. The board will need to determine the level of oversight it requires into the data investigation, board reporting on progress and any remediation processes.

RECOVERY: GOVERNANCE RED FLAGS

1. A limited investigation that focuses on fixing immediate issues without identifying the underlying root causes and vulnerabilities.
2. Limited transparency to key stakeholders on the nature of the incident and how it is being remediated.
3. Accountability not apportioned fairly – failures being blamed on one or two individuals.
4. Not documenting and disseminating the lessons learned from the incident across the organisation, including how to approach crisis management.
5. No plan for supporting staff and recognising their contribution.

THE POST-INCIDENT REVIEW

A full post-incident review should be sponsored by the board with the final report, findings and recommendations considered by the board. At large complex organisations it is good practice for the review to be undertaken by an independent third-party expert.

A key benefit from a comprehensive post-incident review, overseen by the board, is identifying lessons learned from the incident and where the organisation can take active steps to build its cyber resilience. A rigorous review is also a key component of rebuilding reputation and demonstrating to internal and external stakeholders that the board and organisation has learnt from the incident.

For larger organisations, it may be appropriate and possible for the post-incident review team to be activated in parallel to the response team. This accelerates the analysis of root cause and can positively impact remediation activities and the management of regulatory risk. It is important the activities of the post-incident review team do not interfere with the recovery efforts. This may require careful navigation and review of priorities.

The board should understand, and if necessary, seek legal advice on, the limitations of legal professional privilege over any post-incident review reports. Prior to any post incident review taking place, there should be a board level discussion regarding whether the subsequent report should be made public (in full or part). Organisations will need to carefully weigh up stakeholder expectations around transparency with the legal risks that can be triggered by publishing such reports.

The following table details the different reports, with separate and distinct purposes, that may form the basis of an overarching post-incident review.

REPORT OR COMPONENT OF REPORT	TYPICAL TERMS OF REFERENCE
Incident Forensic Post-Incident Report	A review of all available forensic evidence and logs to determine: • How and when the threat actor compromised systems and any indicators that support identification of the threat actor/their affiliation(s) and motivations; • What the indicators of compromise are; • Lateral movement by the threat actor (what tools did the threat actor deploy to move laterally, and what parts of the system did they access?); • The extent and details of data exfiltration (if any); • The extent that the threat actor may have removed forensic evidence of their own activities; and • Evidence of last known activity of the threat actor and indicators they are, no longer present in the system.
Data loss and privacy risk assessment	Based on an assessment of the data in any data breach (either confirmed data loss or assumed data stolen/access): • Determine the risk of financial and non-financial harm to impacted individuals, based on the categories of data stolen; • Assess the effectiveness of the current measures taken to mitigate the risks of harm and identify any gaps or opportunities to further mitigate the risk; • Assess the current privacy policies, procedures and practices against relevant regulatory obligations and best practice; and • Receive prioritised recommendations to improve compliance with privacy regulations and data retention that can be both immediately implemented, and implemented over time.
Cyber risk-management and governance	Understanding risk-control failings: • An assessment of the effectiveness of relevant security controls; • A review of the management and governance of cyber risk, including relevant policies and processes, third-party software and systems; and • Role of third parties in the cyber environment and assess their contribution, if any, to security vulnerability and control weaknesses.
Crisis management response	Consider the performance of the crisis management team, senior executive and board in responding to the incident: • Review the performance of any external experts used to support the incident response; • Analyse the timeliness and effectiveness of organisational response – e.g. technical recovery, remediation of impacted stakeholders; and • Assess stakeholder communications and impact on corporate reputation and relationships.

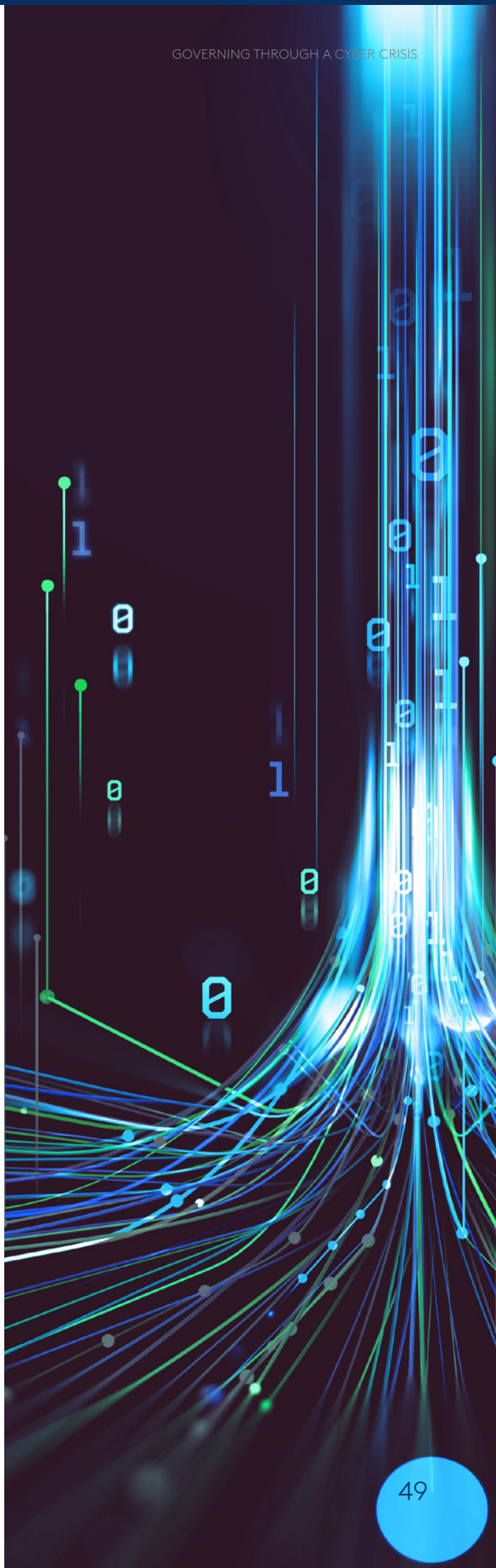
POST-INCIDENT INFORMATION SHARING

The board should review, or delegate the authority to the management team, to release certain information to external agencies and third parties.

Following a cyber incident, there can be significant interest by third parties and government, especially the ACSC and the National Cyber Security Coordinator, in the details of the incident and in the ongoing security of an organisation's systems. Sharing indicators of compromise, technical details of the incident and lessons about response and recovery are important to improving and uplifting the security of all organisations. However, boards and management teams should receive appropriate advice regarding the impact of sharing information on potential regulatory investigations and litigation.

KEY QUESTIONS FOR DIRECTORS

1. Are there immediate security measures that can be implemented?
2. Has the board sought independent advice on the actions taken and the current level of security?
3. Does the board understand the potential risk of harm that impacted individuals face because of data loss? What steps have been taken to adequately mitigate this risk, and what additional steps can be taken?
4. Is the cost, pace and scale of recovery commensurate with the expectations of your customers, government, regulators, and other key stakeholders?
5. Does the board have oversight of ongoing regulators' investigations and requests for information?



6. Remediate

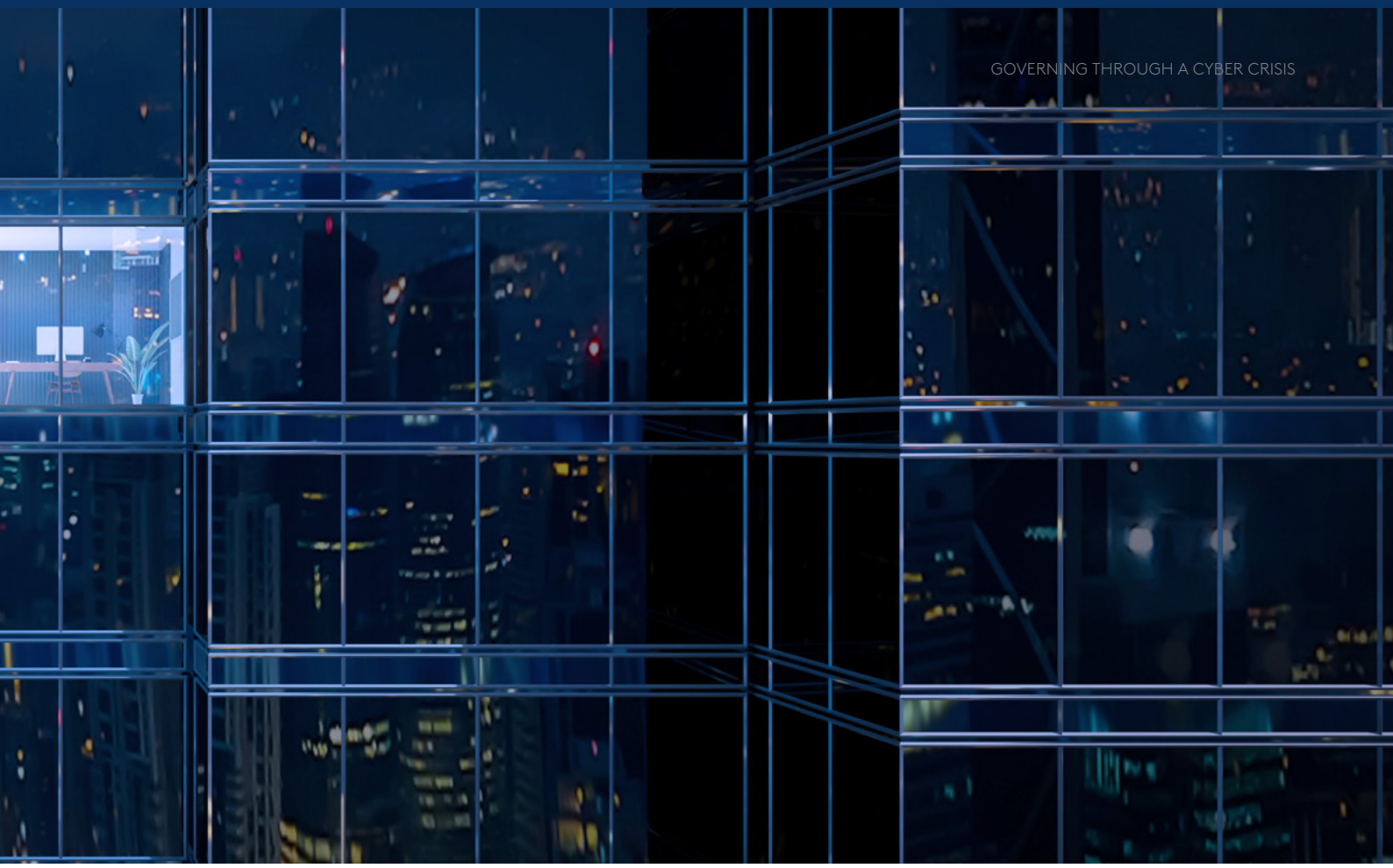
KEY POINTS

1. Support the management team's post-incident response and actions, including that remediation plans are adequately resourced and implemented in a timely manner.
2. Oversee effective communication and support for employees, customers and third parties who may have been impacted or potentially harmed by the incident.
3. Oversee the remediation and compensation to customers, where appropriate.
4. Responsibly share knowledge and insights gained from the crisis with other organisations.

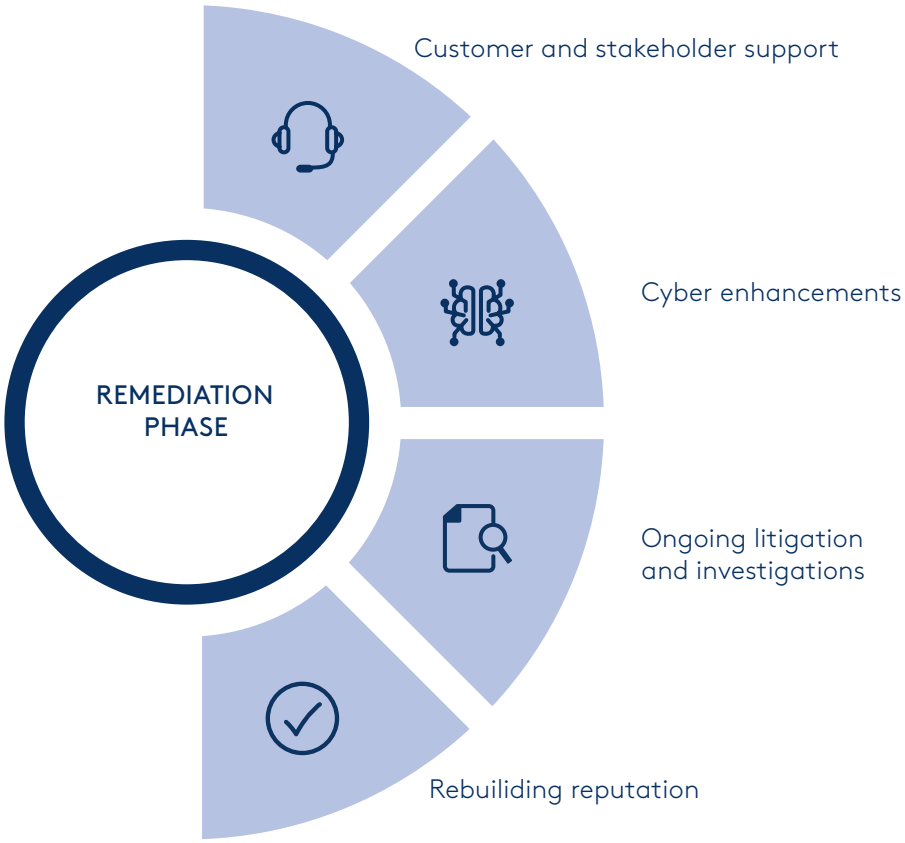
THE ROLE OF THE BOARD

The board has a key role in the long-term remediation phase of a cyber crisis where the organisation is seeking to rebuild trust and reputation and making investments to significantly strengthen its cyber defences.

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



> “Clear, transparent communication is the lifeblood of navigating a cyber incident. It fosters trust, calms anxieties and helps rebuild reputation.”
>
> — Senior director
> ASX listed-company



CUSTOMER REMEDIATION AND COMPENSATION

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

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

- The provision of specific advice and access to resources for individuals whose personal data may have been stolen, including advice that improves their awareness of and ability to detect potential scams, identity theft and fraud, and access to credit monitoring and dark web monitoring, where appropriate.
- Advice to individuals regarding actions they can take to limit their risk of identify theft and fraud following a data breach, including contacting banks and government agencies to ensure additional monitoring can be put in place.
- Advising individuals on any steps the organisation itself has been able to take to limit its risk of harm, including cooperating with regulators and governments.
- Providing advice on the necessity of replacing identity documents, the costs (and any reimbursement) of replacement and the process to replace documents, working closely with relevant government departments.
- Providing access to appropriate counselling or other support services.
- Considering the need to reimburse or compensate impacted individuals or businesses for particular types of harm or damage.

SME AND NFP GUIDANCE: REMEDIATION

1. Where possible, provide assistance to impacted individuals, including financial support to replace documents.
2. Utilise templates, social media, FAQs on a website, or a dedicated customer telephone line to assist in triaging and responding to customers' issues and complaints.
3. Continue to communicate honestly, clearly and empathetically with impacted stakeholders.
4. Demonstrate cyber enhancements to key stakeholders.
5. Consider whether compensation, such as product or service discounts, for impacted customers/clients may assist in rebuilding reputation.

Complaints-handling

Providing accurate information to customers and impacted parties is a part of a robust customer-remediation plan that contributes to rebuilding an organisation's reputation.

The board should oversee the implementation of a complaints-resolution framework that can proactively address a range of loss scenarios, address common complaints and privacy issues, and ensure fairness and consistency in any compensation claims. The framework should empower frontline staff with decision-making authority in most instances. The objective is to achieve a 'first-call' resolution, which enhances efficiency, reduces reputation risks and ensures prompt, positive customer outcomes.

It is also important that the framework covers actions for high-risk and vulnerable customers and, where relevant, can provide specialised care and support. There should be a clear escalation pathway to resolve disputes and high-risk complaints.

Frontline staff may be subject to unacceptable behaviours from impacted customers and the public. Security and support considerations for staff must be a priority.

CYBER SECURITY REMEDIATION AND IMPROVEMENTS

The board should receive detailed recommendations for security improvements as part of the post-incident review process.

The board should oversee the necessary investments and enhancements to the organisation's existing cyber security risk approach, policies and procedures. It is important the organisation's cyber posture is continually strengthened to enable it to defend against future attacks. This may include reviewing the risk appetite statements, board and management reporting, the cyber security risk controls, adherence to applicable cyber security standards and maturity levels, data governance and retention practices, and employee training and awareness.

The board should receive regular (ideally monthly) updates on the progress of implementing these recommendations. It is not unusual for the complete implementation of recommendations in a post-incident report to take 6-12 months to complete, so prioritisation is often required. In exercising appropriate governance over security remediation, the board should review and assess:

- The timeliness of remediating vulnerabilities, especially critical and high-risk vulnerabilities. Regulators and customers will not take kindly to remediation action that is too slow, especially if there is publicly-available guidance from the ACSC about known vulnerabilities.
- The appropriateness of the remediation budget and resources to fill gaps and complete the implementation of all of the recommendations.
- Balancing the prioritisation of recommended actions versus the ongoing cyber BAU activities and any limitations of resourcing and budget.

It may be helpful for the board to approve a set of key principles up-front regarding how customer remediation should work (e.g. all financial loss reimbursed, target resolution timeframes for complaints).

Given the often long-tail impact on reputation, it may be wise for the organisation to adopt a generous approach to customer remediation. This is preferable to an approach that may have some short-term financial savings but contribute to an entrenched negative perception amongst stakeholders.

REBUILDING REPUTATION

Significant cyber incidents can be seen as a breach of customer, employee and community trust, and can cause considerable ongoing reputational damage. The board will need to oversee management's steps to rebuild the organisation's reputation.

Understand your reputation and set objectives

Rebuilding reputation takes time. It starts with building a clear picture of the extent of reputational damage across core constituents.

While the board may engage directly with key shareholders, it is also important that there is an appropriate understanding of the impact on reputation amongst employees and prospective employees, different segments of the customer base, third parties and the media.

Communicate with transparency and authenticity

The community, media and customers are increasingly aware of organisations that attempt to overreach and overpromise in an attempt to remediate a damaged corporate reputation. They expect transparency and authenticity in communications.

It's important that from the outset, communications are customer centric, provide ongoing updates to support impacted parties, and that customers feel empowered to take action to mitigate any risks they may be exposed to. Organisations should be mindful, however, of not attempting to provide a running commentary that may fuel customer anxiety and further damage reputation.

The communication expectations of individual victims of a cyber incident evolve and change over time. For example, it is often appropriate for an organisation in the early stages of an incident to say their information is incomplete and it will take considerable time to verify facts and/or identify the recovery timeframe.

The board plays an important 'check-and-challenge' function, determining that the organisation can deliver on commitments to customers and impacted parties in the weeks and months following a cyber incident. The board should also ensure that communications with all stakeholders are well planned, appropriately frequent, and aligned with the organisation's long-term remediation objectives.

Accept responsibility

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

Accepting responsibility can be demonstrated through a clear public acknowledgement of responsibility, tangible material improvements to the organisation's security program, removing personal data that is not required to be retained, remaining relentlessly customer focused and escalating complaints rapidly.

After a significant cyber incident, the board should be able to point to the measures taken to improve the organisation's cyber resilience.

RESPONSE: GOVERNANCE RED FLAGS

1. Limited or no genuine attempt to recognise the impact on individual customers and provide them with appropriate support.
2. Management downplaying the severity of the incident or resisting further focus on lifting cyber security.
3. No clear strategy or plan for rebuilding the organisation's reputation.
4. Limited information from management about the legal risks and external investigations resulting from the incident.

Sharing lessons learnt

Following a significant incident, there can be intense interest from industry and peers, who want to understand and learn from the experience. Being transparent about the challenges, solutions, resources and strategies that worked and didn't work, and spending time in forums with other boards and management teams is a valuable contribution to improving cyber readiness and response. It will also contribute to enhanced standing with Government, which wishes to see national cyber resilience lifted.

LONG TAIL OF LEGAL ACTIONS AND REGULATORY INVESTIGATIONS

Boards will need to closely monitor and respond to regulatory investigations and litigation following a cyber crisis. The board should receive regular updates and advice on ongoing potential legal risks.

Australia has experienced a significant increase in class actions and regulatory activity stemming from recent high-profile cyber incidents. The potential outcomes following a significant cyber incident will depend upon the size and type of the organisation, whether it is listed and how it is regulated.

For claims that may be made by individuals or contract breach claims, the board should consider its strategy and approach for settlement negotiations, including with insurers, if appropriate.

Directors should be aware the Federal Government has committed, in principle, to introducing a direct right of action for individuals impacted by a privacy breach that will create a new and simpler litigation route. This will significantly increase legal risks and should be factored into organisational approaches to data governance and cyber security strategies.

Potential outcomes following a significant cyber incident

- ASIC investigation and commencement of proceedings alleging that the board failed to implement sufficient cyber risk mitigation or management strategies causing harm to the company thereby breaching directors' duty of care and diligence (s180 Corporations Act) and/or duty to act in good faith in the best interests of the corporation (s181).
- Office of the Australian Information Commissioner (OAIC) investigation and civil penalties or enforceable undertakings.
- Consumer and/or supplier class action alleging loss related to the cyber incident.
- Shareholder class action alleging failure to adequately disclose cyber risk-management practices and/or material details of the cyber incident.
- Investigations by industry specific regulators and conditions imposed on licences (e.g. APRA).
- ACCC investigations for misleading or deceptive conduct under s29(1)(a) or 29(1)(g) of the Australian Consumer Law for false or misleading representations about privacy or cyber security measures.
- Claims for breach of contract by customers.
- Board members and executives being called before a Parliamentary Inquiry or Royal Commission and required to provide written statements or give oral evidence.

If the organisation holds cyber insurance, the board should be aware of the extent to which their policies will cover the costs associated with investigations and subsequent litigation or regulatory actions. For example, the cost of appearing at formal investigations is usually covered under a policy, but the cost of producing documents may not be.

The board should also consider undertaking training for the Chair and CEO in how to prepare for possible inquiries, regulatory action and cross-examinations. This may build on earlier training, in the readiness phase, around preparing for media appearances.

KEY QUESTIONS FOR DIRECTORS

1. Does the board have oversight of likely potential claims which may arise out of the particular incident? Has a strategy been developed to handle each type of claim?
2. Are there sufficient resources and funds available to remediate at the appropriate scale and pace?
3. Has the board reviewed and approved updates to the cyber risk framework, risk appetite statements and incident response plans? Is there a continuation of the simulation and testing program scheduled?
4. Does the board have appropriate oversight over the key customer and employee issues that may require remediation?
5. How would our planned approach to remediation be viewed externally?
6. Has the board agreed, with appropriate legal advice, what lessons can be openly shared with key stakeholders?

7. Annexures

Appendix A: Cyber security regulatory obligations

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

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

Key Commonwealth regulatory frameworks include:

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

Appendix B: Large business response plans

EXECUTIVE AND BOARD-LEVEL PLANS	SUMMARY
Crisis management plan (CMP)	Outlines the key roles and responsibilities across the organisation, defines the crisis management team and supporting teams, how potential crises will be escalated to key decision-makers, and provides useful templates for recording key events and decisions. The CMP must also outline the role of the board and of any board crisis sub-committees.
Cyber Crisis communications plan	Outlines the roles and members of the crisis communications team, defines the authority to release statements to the media, employees and other third parties, and includes pre-prepared statements for the key cyber scenarios identified in risk planning. **A process for customer complaints, support and remediation should also be developed, either as part of a communications plan or a separate planning document.**
Regulatory support and notifications	A plan, or sub-set to other plans, that clearly identifies the regulatory obligations, timeframes and mechanisms to report cyber incidents to Government agencies, State and Commonwealth Ministers. Also identifies avenues for Government support, including the ASD and National Officer of Cyber Security. For publicly listed companies, disclosure obligations and draft disclosure statements should also be included.
Ransom response	Organisations should consider a documented policy on ransom payment and the authority to make decisions in a ransomware attack, including any communication with a threat actor and the decision to pay or not to pay a ransom. A separate, discrete plan should include a risk-based decision-making process that outlines the key considerations, and legal and non-legal risks of any potential payment decision, and demonstrate that any decision to pay is an option of last resort.
CYBER-SPECIFIC PLANS	**DETAIL**
Cyber incident response plan	Defines the role and responsibility for the IT and cyber team (and external specialist resources) in identifying, escalating, containing and recovering from a cyber attack, including playbooks that outline the technical responses required for typical cyber incidents.
Data breach plan	Identifies how potential data breaches will be escalated, the responsible individual(s) for triaging and making an initial assessment, reporting obligations and how the organisation should notify impacted individuals to limit their risk of harm, including, where appropriate, tools and resources to monitor credit and the dark web, and the replacement of identity documents.
Business continuity and disaster recovery plans	These are detailed plans that outline the impact on systems and processes in the event of an outage, ideal recovery time frames and the key actions for interim arrangements, as well as the processes for recovering systems (including from backup).

Appendix C: Resources

1. Government resources

a. ASD/ACSC:
- Questions for Boards to Ask About Cyber Security
- Small Business Cyber Security Guide
- Essential Eight
- Australian Signals Directorate's Cyber Security Partnership Program
- ReportCyber

b. Cyber and Infrastructure Security Centre:
- Overview of Cyber Security Obligations for Corporate Leaders
- General Guidance for Critical Infrastructure Assets
- Mandatory Cyber Incident Reporting

c. Australian Securities and Investments Commission:
- Key questions for an organisation's board of directors
- Cyber resilience good practices

d. Australian Prudential Regulation Authority:
- Improving cyber resilience: the role boards have to play
- Cyber security stocktake exposes gaps
- Prudential Standard CPS 230 Operational Risk Management
- Prudential Standard CPS 234 Information Security
- Prudential Practice Guide CPG 234 Information Security

e. Australian Charities and Not-for-profits Commission
- Governance toolkit: Cyber Security

2. AICD resources

- Course: The Board's Role in Cyber
- Director tools:
  i) Information technology governance
  ii) Managing a data breach: Ten oversight questions for directors
  iii) Data and privacy governance

3. CSCRC resources

- Poison the Well – AI, Data Integrity and Emerging Cyber Threats
- Gamification Impact Case Study
- Research projects

4. International resources

- UK Cyber Security Centre: Cyber Security Toolkit for Boards
- UK draft Cyber Governance Code of Practice
- US Cybersecurity & Infrastructure Security Agency Framework for Improving Critical Infrastructure Cybersecurity
- National Institute of Standards and Technology Cybersecurity Framework

Acknowledgements

The AICD, CSCRC and Ashurst would like to thank the directors, government agencies and companies who gave generously of their time and provided insights into good practice in the cyber incident response and recovery, including:

- Catherine Brenner FAICD, Chair of Australian Payments Plus, Director of Scentre Group, Emmi and The George Institute for Global Health;
- John M. Green FAICD, Chair of UOW Global Enterprises, Director of Challenger and the CSCRC;
- John Mullen AO, Chair of Brambles and Chair of Treasury Wine Estates;
- David Thodey AO, Chair of Xero, Chair of Tyro Payments, Director of Ramsay Health Care.

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.

By identifying, funding and supporting research projects that build Australia's cyber security capacity, strengthening the cyber security of Australian businesses and addressing pressing policy and legislative issues across the cyber spectrum, the CSCRC is a key player in the nation's cyber ecosystem. The CSCRC has two research programs: Critical Infrastructure Security and Cyber Security as a Service.

About Ashurst

Ashurst is a leading global law firm with world class capability, and in-depth understanding of its clients and commitment to providing exceptional standards of service.

Ashurst Risk Advisory is Ashurst's consultancy business, with a 130-strong global team of highly experienced, expert risk consultants. Together with Ashurst Advance, the firm works to deliver a seamless end-to-end service across all the legal, risk and technology aspects of cyber readiness, response, recovery and remediation.

The firm has supported organisations recovering from some of the highest-profile, recent cyber incidents in Australia and the UK. Ashurst leverages this experience to prepare Boards and management teams, giving them confidence they have thorough and comprehensive plans for significant cyber incidents.

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, CSCRC and Ashurst 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, CSCRC and Ashurst 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, CSCRC and Ashurst. All details were accurate at the time of printing. The AICD, CSCRC and Ashurst reserve the right to make changes without notice where necessary.

Copyright

aicd.com.au